Escola de Tecnologias e Arquitetura

GESTÃO DIGITAL DA PROPRIEDADE INTELECTUAL DE CONHECIMENTO CIENTÍFICO E EDUCACIONAL

Joaquim José Gonçalves Marques

Tese especialmente elaborada para obtenção do grau de
Doutor em Ciências e Tecnologias de Informação

Orientador:
Professor Doutor Carlos José Corredoura Serrão,
Professor Auxiliar, ISCTE-IUL

Setembro de 2015

Departamento de Ciências e Tecnologias de Informação

GESTÃO DIGITAL DA PROPRIEDADE INTELECTUAL DE CONHECIMENTO CIENTÍFICO E EDUCACIONAL

Joaquim José Gonçalves Marques

Tese submetida como requisito parcial para obtenção do grau de

Doutor em Ciências e Tecnologias de Informação

Júri:

Doutor Victor Rodriguez-Doncel, Investigador Pós-DOC da Universidade Politécnica de Madrid, Espanha

Doutor Jaime Delgado Merce, Professor Catedrático da Universidade Politécnica de Catalunha, Espanha

Doutor José Carlos Meireles Monteiro Metrolho, Professor Adjunto do Instituto Politécnico de Castelo Branco

Doutor Henrique José da Rocha O'Neill, Professor Associado do Departamento de Marketing, Operações e Gestão Geral do ISCTE-IUL

Doutor Carlos José Corredoura Serrão, Professor Auxiliar do Departamento de Ciências e Tecnologias de Informação do ISCTE- IUL

Setembro 2015

ISCTE IUL
Instituto Universitário de Lisboa

Gestão Digital da Propriedade Intelectual de Conhecimento Científico e Educacional

Joaquim Marques

Setembro

A ti que sempre o sonhaste … “meu velho”

In memoriam

(west Atlantic ocean, new Foundland banks, west Indic ocean, Greenland sea, North sea, Irish sea)

Agradecimentos

Tal como em todas as teses de doutoramento, existiram vários momentos em que o cansaço e o desalento entravam porta adentro provocando o desnorte nesta longa e difícil viagem. Contudo, nos momentos em que tudo parecia perdido, o bom porto de abrigo que a família e amigos proporcionavam davam o alento para continuar e demonstravam que acreditavam que eu ia conseguir.

Agradeço a todos os meus familiares pela confiança e apoio, principalmente á minha esposa, Margarida, aos meus filhos, Zé Pedro e Marta, que sempre me fizeram sentir as forças das minhas raízes e aos meus sogros, que sempre me entusiasmaram.

Agradeço ao meu orientador por todo o apoio e ensinamentos que me transmitiu. Como um arrais que ensina o seu discípulo a navegar, assim foi o Professor Carlos Serrão, umas vezes corrigindo a rota da navegação, outras aparentemente libertando o discípulo para lhe dar a oportunidade de cometer e corrigir os erros. Agradeço a confiança que depositou em mim ao longo de todos estes anos.

Não poderia deixar de agradecer em especial ao Professor José Carlos Metrolho, pelo incentivo e total cooperação demonstrada ao longo destes tempos.

Resumo

O objetivo principal desta tese consiste na definição, projeto e adaptação de uma solução de gestão digital de direitos (*Digital Rights Management* - DRM), capaz de se enquadrar no contexto académico, preservando os direitos básicos dos autores/detentores de conteúdo neste meio e respeitando a linha de direitos sucessórios. A solução proposta, suportada por uma solução DRM aberta, facilmente adaptável e baseada em normas internacionais, está orientada para dar resposta aos requisitos específicos dos detentores de direitos sobre o conteúdo digital partilhado no que respeita ao suporte oferecido à preservação dos seus direitos mais elementares neste contexto: a preservação da integridade do conteúdo e direito de atribuição.

Visando atingir este objetivo foram analisadas várias iniciativas e soluções de DRM, assim como normas internacionais nesta área. Tendo por base a proposta de um modelo de referência, em conjunto com a adaptação de um sistema de DRM "aberto" (designado por ARMS - *Academic Rights Management System*) ao contexto educacional e académico, e considerando a integração das normas MPEG-21, foi possível realizar a validação do licenciamento através de mecanismos de controlo adequados e assim estabelecer o governo de direitos sobre conteúdos no domínio académico, garantindo que os direitos dos autores/detentores são respeitados de acordo com uma linha sucessória. A proposta apresentada, ao aplicar mecanismos de controlo baseados na norma MPEG-21 no processo de emissão de licenças, permite assegurar que os direitos transmitidos são respeitados ao longo da linha sucessória.

Esta tese procura contribuir com várias melhorias na área dos sistemas de DRM usando a norma MPEG-21 com vista à preservação de direitos de Propriedade Intelectual (PI) sobre conteúdos no contexto académico. Além da proposta de um modelo de referência orientado para o contexto académico e de investigação, várias iniciativas e normas internacionais na área do DRM são aqui analisadas sendo definida e proposta uma estrutura de transporte de conteúdos e de direitos associados, baseada na norma internacional ISO/IEC-21000 (MPEG-21) capaz de permitir a sua interpretação pelos atuais sistemas de DRM e a sua transmissão nas atuais infraestruturas de comunicação. Os aspetos de protecção e transmissão do conteúdo e direitos associados são aqui analisados tendo por base casos de estudo típicos do domínio académico, sendo propostos novos mecanismos de controlo de transmissão de direitos com vista a preservar e simplificar o governo dos direitos concessionados ao longo da linha sucessória.

Palavras-chave: Gestão Digital de Direitos (DRM), Propriedade Intelectual, MPEG-21, Proteção e partilha de conteúdos no contexto académico, Preservação e concessão de direitos.

Abstract

Digital technology offers many technological tools that ease the creation, modification and transmission of content introducing many challenges when content owner wants to preserve his intellectual property rights, specialy in the educational and research community. The main goal of this dissertation is the definition and design of a DRM solution able to be adapted to educational and research context offering support to elementar preservation of rights on sharable content like authorship and content integrity. The proposed solution, supported by an open platform easily adaptable to this context and based in recognized international standards like ISO/IEC 21000 standard (MPEG-21), is able to meet specific rights holder's needs in this special context preserving the inheritance rights. Through the implementation of specific mecanisms that controls the license issuance, the proposed solution have the capacity to manage the inherithed rights assuring these are transmited according the conditions defined by the chain of issuers.

This thesis presents several improvements in the area of DRM systems using MPEG-21 in order to preserve intellectual property rights over content in the educational and academic context. In order to achieve this goal, several standards, initiatives and solutions were analised and taken into account, in special the OpenSDRM system and the integration with some parts of ISO/IEC 21000 standard. A reference rights management model is proposed in order to support a DRM solution based in an existing open solution like OpenSDRM, here the emphasis is focused on rights transmission. Having always in mind the MPEG-21standard integration, in special the perspective of rights expression and transmission, a DRM system named ARMS is developed interacting with the Academic Management System (SGA) that supports the main academic activities of educational instituitions. One of the main resulting contributions is the integration of this standard with the ARMS system, enabling the licensing validation of the usage license before its emission. The target is to simplify the license management, preserving the inheritance rights stated by authors and establish a framework to control and govern rights on the educational domain.

Keywords: DRM, Intellectual Property, MPEG-21, Content Protection and sharing in the educational context, Rights preservation, Grant of rights.

Índice

Agradecimentos i

Resumo iii

Abstract v

Índice de Figuras xiii

Índice de Tabelas xvii

Principais Abreviaturas Utilizadas xviii

Parte I 1

Introdução e contextualização da investigação 1

Capítulo 1 3

Âmbito da investigação 3

1 Introdução 3

1.1 Conceitos/Terminologia 5

1.2 Proteção de direitos no contexto académico 6

2 Problema e questões de investigação 9

2.1 A investigação 10

3 Objetivo da investigação 14

4 Contributos 15

5 Estrutura do documento 16

Capítulo 2 19

Gestão de direitos de PI no meio académico e sistemas DRM 19

Resumo 19

1 Introdução 19

2 Ciclo de vida do conteúdo e gestão de direitos 22

2.1 Gestão de direitos de PI no meio educacional e académico 24

2.2 Cenários de gestão de direitos e meio académico 25

3 Gestão digital de direitos 26
3.1 Fundamentos sobre sistemas de gestão digital de direitos 29
3.1.1 Fluxo de conteúdo e de direitos 31
3.1.2 Entidades DRM 34
3.1.2.1 Participantes no DRM 34
3.1.2.2 Componentes de DRM 36
4 Perspetiva estrutural do DRM 40
4.1 DRM: estrutura funcional 40
4.1.1 DRM e ferramentas tecnológicas 44
4.2 DRM: arquitetura 51
4.2.1 DRM: estrutura por camadas 53
4.2.2 DRM: estrutura por serviços 55
5 Aspetos de segurança do DRM 57
5.1 DRM - Vulnerabilidades 58
5.2 DRM - conteúdos e licenças 60
5.2.1 DRM - conteúdo protegido 61
5.2.2 DRM - licenças 61
5.3 Licenciamento em DRM 62
6 Conclusão 63
Capítulo 3 65
Análise de soluções de DRM “abertas” 65
Resumo 65
1 Introdução 65
2 Classificação de sistemas DRM 66
3 Sistemas DRM “abertos” 67
3.1 OpenSDRM 68

3.1.1 Licenciamento no OpenSDRM 74
3.2 Open Mobile Alliance (OMA-DRM) 75
3.2.1 Arquitetura OMA DRM 76
3.3 MIPAMS 81
3.3.1 Protocolos envolvidos 83
3.4 OpenIPMP 84
3.5 DReaM 85
3.6 Marlin 86
4 Resumo das características primárias das soluções 89
5 Conclusão 93
Parte II 95
Proposta de modelo de referência de DRM e integração do OpenSDRM 95
Capítulo 4 97
Proposta de modelo conceptual de referência de DRM para contexto educacional 97
Resumo 97
1 Introdução 97
2 Conteúdos e DRM 99
3 Proposta de modelo 100
3.1 Fluxo de conteúdo e DRM 100
3.2 Entidades e Papéis 102
3.3 Conceptualização do modelo proposto 103
3.3.1 Requisitos dos participantes 107
3.4 Componentes do sistema DRM 108
3.4.1 Interação entre os diferentes componentes de um sistema DRM 110
3.4.2 Proteção do conteúdo e chaves 114
3.5 Estrutura do sistema proposto 117

3.5.1 Requisitos na transferência da licença 122
3.5.2 Funcionalidades do modelo proposto 123
4 Análise das propriedades de segurança na proposta 125
5 Conclusão 128
Capítulo 5 131
Proteção de conteúdos e transmissão de direitos 131
Resumo 131
1 Introdução 131
2 Conteúdos e licenças no DRM: caso de uso 133
2.1 Aquisição de licença 134
2.2 Transferência de conteúdo e licença 135
2.3 Transmissão de direitos entre utilizadores 136
2.3.1 Licença emitida entre utilizadores e assinaturas digitais 139
2.3.1.1 Reencriptação pelo dispositivo 139
2.3.1.2 Reencriptação por *proxy* 141
2.4 Rastreio do licenciamento 145
3 Conclusão 146
Capítulo 6 147
OpenSDRM adaptado ao contexto educacional e académico 147
Resumo 147
1 Introdução 147
2 OpenSDRM – características, funcionalidades e serviços 149
2.1 Aspetos de segurança no OpenSDRM 153
3 MPEG-21, modelo proposto e adaptação do OpenSDRM 155
4 OpenSDRM e a arquitetura orientada por serviços *Web* 157
5 Conclusão 161

Parte III 163

Transmissão de conteúdos e direitos no OpenSDRM adaptado 163

Capítulo 7 165

Proteção do conteúdo recorrendo à norma MPEG-21 165

Resumo 165

1 Introdução 165

2 Representação de objetos digitais usando o MPEG-21 167

2.1 Empacotamento de conteúdos e de licenças 169

2.1.1 Conteúdo desprotegido 169

2.1.2 Conteúdo protegido 174

2.1.2.1 MPEG-21 e a gestão de direitos 174

2.1.2.2 Conteúdos seguros e transmissão 178

2.1.2.3 MPEG-21 e rastreio do licenciamento 188

3 A norma MPEG-21 e o modelo proposto 193

4 Modelo baseado na norma MPEG-21 e OpenSDRM adaptado ao contexto académico 195

4.1 Proteção de conteúdo e empacotamento 195

4.1.1 Descarregamento de conteúdo e respetiva licença 199

4.1.2 Superdistribuição do conteúdo 201

4.2 O Media Player/Wallet 201

5 Conclusão 202

Capítulo 8 203

ARMS – Sistema DRM adaptado ao contexto educacional e académico 203

Resumo 203

1 Introdução 203

2 ARMS 204

2.1 ARMS e utilização de objetos digitais 207
3 Proteção de conteúdo no ARMS 210
3.1 Registo do utilizador 210
3.2 Partilha de conteúdo 211
3.3 Objetos DID_C e DID_L 214
4. Protocolo de preparação, partilha e acesso ao conteúdo 214
4.1 Preparação do conteúdo no ARMS 215
4.2 Partilha e regras de utilização do conteúdo 216
4.2.1 Licença de distribuição 217
4.3 Acesso ao conteúdo 218
5. Ferramentas de suporte MPEG-21 no ARMS 223
6. Conclusão 228
PARTE IV 229
Transmissão de direitos e mecanismos de controlo 229
Capítulo 9 231
MPEG-21 e transmissão de direitos no contexto educacional e académico 231
Resumo 231
1 Introdução 231
2 Controlo sobre a utilização do conteúdo 234
2.1 As licenças e o controlo sobre o uso de conteúdo 235
2.2 Ciclo de vida do conteúdo e licenciamento 237
2.3 Direitos referenciais 241
3 Licenciamento de direitos e etapas da produção 242
3.2 Redistribuição de licenças 245
4 MPEG-21 e transmissão de direitos 245
4.1 MPEG-21 - Dependência de direitos e validação 248

4.2 Validação da licença distribuição por emissão 252
5 Casos de utilização 253
6 Conclusão 261
Capítulo 10 263
Controlo da concessão de direitos entre utilizadores 263
Resumo 263
1 Introdução 263
2 Dependências de direitos e licenciamento 265
3 Controlo sobre direitos transmitidos recorrendo ao MPEG-21 267
3.1 Distribuição de licenças com controlo da delegação de direitos 268
3.2 Validação da distribuição de licença por controlo de delegação de direitos 272
3.2.1 Aplicação de regras de validação 274
4 Processamento de licença 280
5 Conclusão 285
PARTE V 287
Conclusão e Investigação Futura 287
Capítulo 11 289
Conclusões e Contribuição Científica 289
Trabalho futuro 293
Referências Bibliográficas I
Anexo A 1

Índice de Figuras

Figura 1 – Fluxo de conteúdo 7

Figura 2 – Transmissão de conteúdos e direitos num sistema DRM básico 27

Figura 3 – A licença e o conteúdo encriptado e acesso ao conteúdo "em claro". 32

Figura 4 - Fluxo do conteúdo num sistema típico DRM 34

Figura 5 - Interações entre componentes e fluxos DRM 37

Figura 6 - Vertente detentor de direitos: fluxo de conteúdos e direitos 38

Figura 7 - Vertente consumidor: fluxo de conteúdos e direitos 39

Figura 8 - Arquitetura funcional do DRM (adaptado de Iannella, 2001) 41

Figura 9 - Elementos funcionais para a proteção de conteúdo (Mampaey & Villegas, 2012). 44

Figura 10 – Arquitetura típica DRM (adaptado de Rosenblatt, et al., 2004) 52

Figura 11 – Interação entre camadas do DRM (adaptado de Diehl, 2008) 54

Figura 12 – Serviços genéricos da *framework* DRM (Serrão, 2008) 56

Figura 13 – Estratificação dos serviços DRM (adaptado de Grzonkowski, 2010) 57

Figura 14 – Elementos da arquitetura OpenSDRM (Serrão, 2008) 69

Figura 15 – Arquitetura da plataforma OpenSDRM (adaptado de Serrão, 2008) 72

Figura 16 – Elementos externos e OpenSDRM (adaptado de Serrão, 2008) 73

Figura 17 - OpenSDRM Wallet mediação do acesso a licenças (Serrão, et al, 2006c) 74

Figura 18 – Arquitetura funcional de OMA-DRM (adaptado de OMA, 2011d) 80

Figura 19 – Arquitetura da plataforma MIPAMS (Delgado et al., 2005b) 81

Figura 20 - Arquitetura OpenIPMP (Serrão, Marques, Dias, & Delgado, 2006b) 84

Figura 21 – Componentes do objeto licença Marlin (Keoh & Vrielink, 2009) 87

Figura 22 - Componentes e arquitetura Marlin (adaptado de MDC, 2007) 88

Figura 23 – Fluxo de conteúdo 97

Figura 24 – Fluxo de conteúdo desprotegido (aquisição e consumo) 98

Figura 25 – Fluxo de conteúdo protegido 101

Figura 26 - Fluxo de conteúdo 102

Figura 27 – Participantes e processos de segurança DRM (adaptado de Nickolova & Nickolov, 2007)..... 104

Figura 28 – Segurança e elementos participantes no modelo 105

Figura 29 - Processos nucleares na proposta de modelo genérico 106

Figura 30 - Proposta de modelo DRM de referência 106

Figura 31 - Abstração das interações entre componentes de um sistema DRM 110

Figura 32 - Validação do pedido de emissão de licenças..... 113

Figura 33 – Fluxo de conteúdos, direitos e informação, ... 117

Figura 34 – Arquitetura proposta do sistema DRM 119

Figura 35 - Utilização de chaves na proteção de conteúdo e geração de licenças 132

Figura 36 – Cenário de aquisição de licença..... 134

Figura 37 – Aquisição e transferência de conteúdo e licença 135

Figura 38 – Fluxo de informação na obtenção de licenças 136

Figura 39 – Transmissão de licenças entre utilizadores..... 138

Figura 40 – Integração do *proxy* na estrutura proposta..... 143

Figura 41 – Reencriptação por *proxy* 144

Figura 42 – Distribuição de licenças entre utilizadores no meio académico 145

Figura 43 – Arquitetura orientada a serviços do OpenSDRM (Serrão, Dias & Delgado, 2005b) 148

Figura 44 - OpenSDRM e interação com componentes externos (adaptado de Serrão, 2008) 157

Figura 45 - Arquitetura do OpenSDRM adaptado (adaptado de Serrão, 2008). 158

Figura 46 – Integração dos componentes OpenSDRM com os serviços *Web* do SGA 160

Figura 47 – Estrutura MPEG-21 DID para um conteúdo desprotegido..... 172

Figura 48 - Exemplo MPEG-21 DIDL para um conteúdo desprotegido 174

Figura 49 - Estrutura básica da licença MPEG-21..... 175

Figura 50 – Estrutura básica de um documento DID contendo a licença 177
Figura 51 – Estrutura básica dos elementos IPMP 179
Figura 52 - Estrutura do subelemento IPMPGeneralInfoDescriptor 180
Figura 53 - Estrutura do subelemento IPMPInfoDescriptor 180
Figura 54 – Conteúdo PDF protegido e embebido num documento DID 183
Figura 55 – Representação da estrutura de documento DID_C contendo ficheiro protegido. . 184
Figura 56 – Licença e chave protegida embebidas num documento DID 187
Figura 57 – Estrutura do documento DID_L contendo a chave e a licença 188
Figura 58 - O elemento *annotation* e a cadeia sucessória num documento DID 192
Figura 59 – Representação da estrutura do documento DID_L com o elemento *annotation.* .. 193
Figura 60 – Preparação de conteúdo 196
Figura 61 - Definição de direitos 197
Figura 62 – ARMS: empacotamento e proteção do conteúdo 197
Figura 63 - Empacotamento de conteúdo não protegido no ARMS 198
Figura 64 – ARMS e descarregamento de conteúdo e respetiva licença 200
Figura 65 – ARMS e superdistribuição 201
Figura 66 – Compoentes ARMS e principais interações 206
Figura 67 - Patamares de proteção no ARMS 207
Figura 68 – Proteção do conteúdo e criação do documento DID_C 212
Figura 69 - Proteção da cifra de proteção do conteúdo e criação do documento DID_L 213
Figura 70 – Utilização de conteúdo com uma licença válida já armazenada no dispositivo . 220
Figura 71 – Obtenção de conteúdo e do objeto licença armazenado em LIS. 221
Figura 72 – Criação do objeto licença 223
Figura 73 – Interações para autorizar a obtenção da ferramenta IPMP 227
Figura 74 - Transmissão de direitos e ciclo de vida do conteúdo 232
Figura 75 - *Upload* de conteúdos e geração de licenças no contexto académico 237

Figura 76 – Consumo de conteúdo e utilização governada por licença 238

Figura 77 – Licença de distribuição e criação de licenças de utilização 238

Figura 78 - Proteção de conteúdos e geração da licença de distribuição 239

Figura 79 – Processo de definição da licença modelo (adaptado de Kamperman et al., 2007) 240

Figura 80 - Cenário de transmissão de direitos referenciais 241

Figura 81 - Geração de licenças de utilização a partir de licenças modelo 243

Figura 82 – Estrutura básica de uma licença de distribuição 246

Figura 83 – Distribuição de licenças e estrutura básica de licenças MPEG-21 247

Figura 84 - Exemplo de transferência de direitos no meio académico 247

Figura 85 – Emissão de licenças e sua estrutura 248

Figura 86 – Licença de distribuição da Universidade emitida pelo Professor 250

Figura 87 – Licença do utilizador emitida pela Universidade 251

Figura 88 – Licenças de distribuição pai/filho por emissão de direitos 253

Figura 89 – Caso de utilização: licença de distribuição por emissão *versus* licença de utilização 254

Figura 90 – Cenário académico: emissão da licença de distribuição 256

Figura 91 – Cenário académico: distribuição direta de licenças e interação com o SGA 257

Figura 92 – Cenário académico: geração de licenças e distribuição por emissão 258

Figura 93 – Distribuição simples de licenças 265

Figura 94 – Licenciamento por subconcessão 266

Figura 95 – Estrutura básica de licenças com controlo por delegação. 269

Figura 96 – Licenças pai/filho *delegationControl* 270

Figura 97 – Exemplo de licença pai para *conditionUnchanged* 271

Figura 98 - Exemplo de licença filho para *conditionUnchanged* 272

Figura 99 – Licenças pai/filho por controlo de delegação de direitos 273

Figura 100 – Licenciamento com delegação de direitos sem alteração de condições 274

Figura 101 – Cenário de delegação controlada. 276
Figura 102 – Transmissão de direitos e controlo de níveis na delegação 276
Figura 103 – Licença de distribuição da editora 277
Figura 104 - A licença de utilização de aluno 278
Figura 105 – Transmissão de licenças de distribuição e controlo de delegação de direitos .. 280
Figura 106 – Licenciamento: criação e obtenção de licenças 284

Índice de Tabelas

Tabela 1 - Ciclo de vida do conteúdo e questões sobre direitos ……..…… 23
Tabela 2 - Gestão de direitos no meio comercial e académico …..……..……26
Tabela 3 - Sistemas e *standards* de identificação/registo de conteúdos.…….……..46
Tabela 4 - Características fundamentais de soluções abertas de DRM……..…….…..90
Tabela 5 - OpenSDRM, MIPAMS e *standards* …….…….…..…….93
Tabela 6 - OpenSDRM e estrutura funcional DRM …….…….……151
Tabela 7 – OpenSDRM e funcionalidades do modelo proposto…….……152
Tabela 8 – OpenSDRM e serviços……..……152
Tabela 9 – Combinações de conteúdo desprotegido e licenças…….……..170
Tabela 10 - MPEG-21 *schemas* – *prefix* e *namespace*……..176

Principais Abreviaturas Utilizadas

3DES	*Triple Data Encryption Standard*
AES	*Advanced Encryption Standard*
BBC	*Blowfish Block Cipher*
CA	*Certification Authority*
DCF	*DRM Content Format*
DCMI	*Dublin Core Metadata Initiative*
DI	*Digital Item*
DID	*Digital Item Declaration*
DIDL	*Digital Item Declaration Language*
DII	*Digital Item Identification*
DMP	*Digital Media project*
DOI	*Digital Object Identifier*
DRM	*Digital Rights Management*
IPMP	*Intellectual Property Management and Protection*
IPMP	*Intellectual Property Management and Protection*
MAC	*Message Authentication Code*
MPEG	*Moving Picture Experts Group*
MPEG-21	*Multimedia framework (ISO/IEC 21000)*
ODRL	*Open Digital Rights Language*
OMA	*Open Mobile Alliance*
PC	*Personal Computer*
PEL	Privilégio de emissão da licença
PI	Propriedade Intelectual
PKI	*Public Key Infrastructure*
REL	*Rights Expression language*
RDF	*Resource Description Framework*
SAML	*Security Assertion Markup Language*
SOAP	*Simple Object Access Protocol*
SSL	*Secure Socket Layer*
SSO	*Single Sign-On*
TCG	*Trusted Computing Group*
TIC	*Tecnologias da Informação e Comunicação*
TPM	*Trusted Platform Module*
XML	*Extensible Markup Language*
XRML	*Extensible Rights Markup Language*
WSDL	*Web Services Description Language*

Parte I

Introdução e contextualização da investigação

Capítulo 1

Âmbito da investigação

1 Introdução

A utilização da Internet em larga escala, aliada à facilidade de utilização de várias ferramentas proporcionadas pelas Tecnologias de Informação e Comunicação (TIC), tem levado a que cada vez mais conteúdos[1] sejam criados e disponibilizados em formato digital (Miniwatts Marketing Group, 2013; Cooper & Martin, 2006; Sandvine, 2014). A utilização desses conteúdos e a sua distribuição e partilha também tem vindo a aumentar (Mussinelli, 2010), bem como a facilidade com que estes se podem copiar, alterar e distribuir a uma escala sem precedentes, baseada numa "cultura de cópia" generalizada (Karaganis & Renkema, 2013). Tudo isto assenta em três características básicas do conteúdo: são facilmente reproduzíveis sem perda de qualidade, são fáceis de transferir e podem ser facilmente personalizados de acordo com as preferências individuais. Por isso, a facilidade de criação, distribuição e obtenção de conteúdos digitais faz com que haja uma cada vez maior necessidade de criar formas de os proteger relativamente aos direitos de PI (Campidoglio, Frattolillo, & Landolfi, 2009; Collier, Piccariello & Robson, 2004b), controlando a sua distribuição e utilização (Liu, Safavi-Naini, & Sheppard, 2003), ou seja, de utilizar sistemas que permitam a gestão de direitos sobre o conteúdo (Iwakiri & Thanh, 2015).

No mundo atual, altamente digitalizado, a enorme evolução tecnológica na área das TIC nos últimos tempos tem feito surgir novas ameaças aos direitos de PI (Ross, 2013; Sun & Baez, 2009; Favale, 2014). Essa evolução acaba por ser um espelho de dupla face, pois se por um lado permite uma melhoria considerável da sofisticação das funcionalidades do *software* e com isso um aumento considerável da quantidade de conteúdos graças à utilização de novos canais de distribuição mais rápidos e volumosos, essa sofisticação quando associada a uma enorme facilidade de utilização torna possível a fácil manipulação desses conteúdos. Ou seja, as mesmas tecnologias que têm contribuído para a criação e distribuição de conteúdos também

[1] Não sendo fácil dar uma definição de "conteúdo" (Mullan, 2011; Halpin & Kelso, 2009), utilizaremos uma definição onde o termo se refere a "*any processed and packaged digital information, such as digital audio, video, graphics, animation, images, text, or any combinations of these types*" (Subramanya & Yi, 2006).

contribuem para facilitar a proliferação de atentados à PI sobre os mesmos. Em cada quatro bits de tráfego na Internet um deles é correspondente a infrações de direitos de PI sobre conteúdos digitais (Castro, 2011). Por isso, a proteção e gestão desses conteúdos e direitos associados é cada vez mais importante não só pelo valor económico dos mesmos, mas também pela potencial perda de outros direitos de PI que os seus detentores possuem.

A PI refere-se a "*creations of the mind: inventions; literary and artistic works; designs and symbols, names and images used in commerce*" (WIPO, n.d.,a) e é protegida por lei através de patentes, direitos de autor e de marca, permitindo às pessoas ganhar reconhecimento ou um benefício financeiro daquilo que inventam ou criam. No meio académico as principais formas em que a PI se manifesta são nas patentes e direitos de autor (Wang, DeMartini, Wragg, Paramasivam & Barlas, 2005). O direito de autor é um termo legal usado para descrever os direitos que os criadores possuem sobre os seus trabalhos literários ou artísticos e envolvem "*economic rights regarding the work reproduction, distribution, public performance, adaptation and translation and moral rights regarding the right to claim authorship and the right of integrity"* (WIPO, n.d.b) que os titulares possuem relativamente às "criações da mente". Os trabalhos abrangidos por direito de autor podem ser conteúdos de diferentes tipos, desde "books, *music, paintings, sculpture and films, computer programs, databases, advertisements, maps and technical drawings*" (WIPO, n.d.,b)

Apesar de a indústria de conteúdos digitais ter vindo, progressivamente, a utilizar sistemas de Gestão Digital de Direitos (DRM) sobre conteúdos digitais (Ku & Chi, 2004; Liu et al., 2003), no meio académico verifica-se uma reduzida utilização destes sistemas. Uma grande parte dos intervenientes no fornecimento e partilha de conteúdos sente necessidade de proteger os seus direitos (Liu, Wang, Lee & Han, 2007; Collier G. et. al., 2004b), em particular o direito de atribuição (Collier & Robson, 2004; Gadd, Oppenheim & Probets, 2003b), mas o que se verifica é que este tipo de sistemas tem recebido pouca atenção neste domínio. Este facto pode dever-se em parte a fatores sociais como, por exemplo, uma cultura de partilha e divulgação do saber em larga escala baseada na confiança, típica entre os pares no meio académico (McGeveran & Fisher, 2008), mas também pode ser atribuído à orientação das ferramentas atuais que compõem os sistemas de gestão de direitos não estarem especificamente vocacionadas para este contexto.

A PI e o conhecimento são dos principais ativos que é importante preservar na cadeia de valor das instituições académicas e de investigação, pois funcionam como fatores diferenciadores oferecendo vantagens competitivas perante concorrentes na captação de novas oportunidades, de estudantes e de investigadores (Marques & Serrão, 2009; Ross, 2013). A identificação das

áreas de aplicação, assim como os principais intervenientes, os tipos e as camadas de direitos associados, as principais funções e modelos nos quais os sistemas de DRM se podem inserir no contexto académico são as peças chave de todo o processo de preservação dos direitos de PI (Subramanya & Yi, 2006). Contudo, a ausência de um sistema plenamente aceite que permita gerir estes valiosos recursos e os direitos associados, aliado a plataformas inteligentes de gestão de conteúdos capazes de usarem ferramentas e técnicas para expressar, comunicar e partilhar direitos, não têm contribuído para uma expansão fácil do uso e partilha de conteúdos abrangidos por direito de PI tecnologicamente protegidos (Collier & Robson, 2004).

1.1 Conceitos/Terminologia

De forma a evitar ambiguidades com as expressões utilizadas, torna-se conveniente clarificar os termos e expressões utilizadas. Assim, ao longo da tese são de considerar os seguintes termos/expressões básicos no contexto de gestão digital de direitos:

Entidade: Uma entidade é definida como algo ou alguém que possui identidade, por exemplo uma pessoa, um sujeito, instituição, ou aplicação de *software*. Entidade de confiança é aquela que é autorizada a realizar uma ação pois assume-se que é seguro que irá atuar de um modo pré-estabelecido num determinado contexto e relativamente a outra entidade.

Direitos: No contexto dos sistemas de gestão digital de direitos, um direito é um atributo que especifica como as partes envolvidas podem usar um bem ou obra (aceder, visualizar, imprimir, …) e em que condições. A ação que o direito habilita é a permissão de execução (ler, imprimir, …) e pode ser limitada por uma condição (uso num intervalo de tempo, usar se pagar, usar num dispositivo, …).

Conteúdo/recurso[2]: Os termos conteúdo ou recurso são aqui utilizados como sendo o bem/obra digital que é realmente utilizado sem informação descritiva ou proteção associada. A execução de uma ação sobre o conteúdo é designada por consumo do conteúdo.

Termos de utilização: Num sentido lato, os termos de utilização definem as regras que governam as ações que podem ser executadas por uma entidade sobre um recurso. Estas ações representam os direitos que uma entidade pode exercer num determinado contexto ou ambiente. Por isso, as regras de governo do conteúdo são expressas de acordo com o contexto em que o recurso é utilizado.

[2] Assumindo que num sistema de DRM os conteúdos possuem sempre informação descritiva associada, o termo bem/obra e conteúdo/recurso são usados com o mesmo sentido.

Bem/obra: Este termo designa o recurso registado no sistema de DRM sobre os quais recaem direitos e que, por isso, possui implicitamente valor. Um bem/obra pode ser a agregação de vários outros bens/obras e/ou recursos.

Partes: Uma parte é uma pessoa simples, organização, instituição ou grupo de pessoas com papéis definidos na sua atuação. Podem ser considerados os seguintes papéis:

- Dono/Detentor – a parte ou conjunto de partes que detêm direitos sobre um bem/obra. O dono da obra pode conceder qualquer direito sobre esta, inclusivé direitos de distribuição. O autor é a parte que representa o criador do conteúdo sendo por isso o produtor do conteúdo e como tal o detentor do conteúdo original;
- Distribuidor – a parte a quem foi concedida a faculdade de transferir direitos sobre o bem/obra para terceiros. Note-se que, por definição, o distribuidor somente necessita de transferir os direitos;
- Fornecedor – a parte que recebe e prepara os conteúdos para distribuição. Além de receber e preparar o conteúdo, pode também atuar como distribuidor;
- Utilizador final/consumidor - a parte que usa ou consome o bem/obra (visualiza, imprime, reproduz, outro). Utiliza-se por vezes o termo "cliente" no sentido de representar o utilizador/consumidor que usa um dispositivo eletrónico para aceder ao conteúdo.

Nesta tese, o termo "autor" representa o criador do conteúdo e o termo "utilizador/consumidor" representa qualquer pessoa com acesso ao conteúdo. O termo "conteúdo" é daqui em diante usado para dados, informação ou conhecimento dentro do domínio da comunicação eletrónica podendo estes tomar a forma de texto, som, imagem, vídeo…entre outros. O termo "licença" corresponde a um conjunto de dados podendo conter as chaves de proteção/desproteção do conteúdo e os termos que definem as regras de utilização. Por sua vez, as "regras de utilização" especificam como o conteúdo pode ser usado.

1.2 Proteção de direitos no contexto académico

O objetivo de muitos criadores de conteúdos no meio académico é disseminar conhecimento através da partilha de conteúdo o mais alargadamente possível, recebendo em troca o reconhecimento de autoria sempre que o seu trabalho for reutilizado ou referenciado (Collier & Robson, 2004; Ross, 2013). Ou seja, interessa ao autor preservar a sua reputação (Ross, 2013). Mas nem sempre esta intenção é conseguida, pois a atribuição de direito de autoria é efetuada

por normas ético-profissionais de reconhecimento, não validadas automaticamente, não havendo um modo reconhecidamente aceite para efetuar a verificação da aplicação deste direito e de outros relacionados com a PI. Existe assim uma enorme necessidade de adoção de sistemas de gestão de direitos de PI que contribuam para a expansão da partilha e da disseminação de conteúdos baseados em conhecimento no meio académico (Campidoglio et al., 2009).

As infraestruturas tecnológicas das instituições educacionais fornecem segurança e controlo de acesso dentro das suas fronteiras. Mas quando o conteúdo é partilhado este controlo deixa de ser eficaz, no sentido em que a tecnologia usada para exprimir e verificar a aplicação dos termos e condições de utilização associados aos conteúdos deixa de ser persistente ao longo de todo o seu ciclo de vida (Marques & Serrão, 2009; Marques & Serrão, 2012a). Ou seja, torna-se necessário assegurar a gestão adequada de direitos de PI sobre o conteúdo desde a sua criação até ao seu consumo (Figura 1). Possuindo cada participante, o criador, o fornecedor e o utilizador os seus direitos sobre o conteúdo, torna-se necessário assegurar uma eficaz proteção do conteúdos e direitos de PI associados desde o criador até chegar ao utilizador final passando pelo distribuidor (Iannella, 2008).

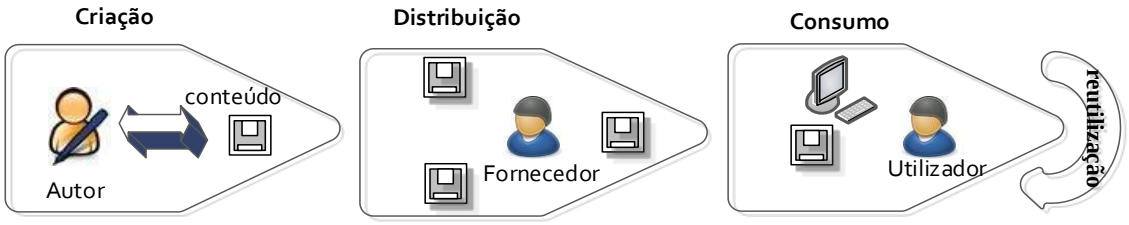


Figura 1 – Fluxo de conteúdo

Não sendo exequível usar sistemas fechados ou proprietários para gerir os direitos de PI associados a uma enorme diversidade de conteúdos proveniente de diversas fontes, torna-se assim necessária a aplicação de sistemas abertos que façam recurso a métodos automatizados para exprimir, transmitir, interpretar e verificar a aplicação de direitos sobre os conteúdos no contexto académico. Os sistemas de DRM baseados em normas internacionalmente reconhecidas são os mais indicados para dar resposta a estas questões (Ku & Chi, 2004; Iannella & Mclean 2002), pois fazem uso de especificações plenamente aceites e conhecidas da comunidade científica onde se pode aplicar tecnologia de vanguarda com vista a proteger o conteúdo, controlar e rastrear a sua distribuição e verificar a vigência dos direitos associados. Apesar da existência de variadas soluções e iniciativas na área do DRM (OMA; Marlin; DMP), estas encontram-se orientadas para a indústria de grande consumo, onde a sua visão está focada em assegurar que os direitos são aplicados e respeitados (Sachan & Kankanhalli, 2012). Torres,

Tous & Delgado (2010) propoêm um sistema de DRM, o IPOS-DS, orientado para o registo, pesquisa e negociação de objetos educacionais (*scholarly objects*) com vista a lidar com potenciais problemas na publicação e distribuição respeitando direitos de PI. Contudo, este sistema é vocacionado para a negociação de conteúdos educacionais com fins comerciais, podendo ser adotado por companhias privadas e sociedades de autores (Torres et al., 2010), cujo fim é essencialmente o retorno finaceiro da exploração do conteúdo, independentemente do reconhecimento da autoria e integridade da obra. Na pesquisa efetuada, que seja do nosso conhecimento, não encontramos um sistema DRM especificamente orientado para o meio académico, cuja principal intenção seja a de preservar a integridade e autoria da obra preservando a linha sucessória de direitos sempre que estes são transmitidos no decorrer do ciclo de vida do conteúdo.

Independentemente de algumas questões relacionadas com a problemática da privacidade e dos elevados custos de implementação (Campidoglio, Frattolillo, & Landolfi, 2008; Dhamija & Wallenberg, 2003; Felten, 2003a; Marques & Serrão, 2014; Conrado, Kamperman, Schrijen & Jonker, 2003), o DRM, ao fornecer ao funcionalidades necessárias para abordar a questão do controlo da utilização e distribuição de conteúdos, vem permitir que os fornecedores de conteúdos consigam ir ao encontro de uma eficaz proteção e governo de direitos de PI. Apesar da sua relevância, salvo raras exceções, os sistemas de DRM têm sido essencialmente desenvolvidos com vista à exploração comercial de conteúdos não tendo sido devidamente valorizados na sua utilização no contexto académico (Marques & Serrão, 2009). Por isso, esta tese está orientada para dar contributos a algumas das questões que a utilização destas tecnologias arrastam consigo, apresentando e propondo, sempre que possível, soluções com suporte em normas internacionalmente reconhecidas. A norma ISO/IEC 21000 (MPEG-21:VTS, 2004), também conhecida genericamente por MPEG-21, utilizada com o intuito de estabelecer uma *framework* para o envio e consumo de conteúdos em que tomam parte os principais intervenientes no seu ciclo de vida, vem criar as condições necessárias para uma abordagem correta da questão do controlo de direitos de PI sobre os conteúdos. Esta norma tem um âmbito bastante alargado de aplicação, suportando um vasto número de funcionalidades que permitem enquadrar-se numa alargada gama de domínios de aplicação. Por ter um papel de referência no desenho e desenvolvimento de aplicações de proteção de direitos de PI, fornecendo as especificações para o desenvolvimento das ferramentas necessárias a essa proteção, ao mesmo tempo que suporta a negociação de conteúdos e direitos, permite a

implementação de mecanismos de controlo adequados, capazes de criarem o ambiente propício ao respeito de direitos de PI sobre conteúdos digitais no meio académico.

2 Problema e questões de investigação

Ao tentar fornecer uma solução para o problema dos direitos de PI sobre conteúdos, os sistemas DRM acabam por se tornar em sistemas de informação altamente complexos pois envolvem fatores interdependentes do ponto de vista tecnológico, social e económico que se influenciam mutuamente (Ku & Chi, 2004; Liu et al., 2003; Abie, 2007). A vertente tecnológica que molda um sistema de DRM engloba normalmente três dimensões: a proteção do conteúdo, a sua distribuição e a garantia de que os direitos associados aos conteúdos são aplicados. Estas dimensões incorporam requisitos de segurança variados com implicações recíprocas em cada uma dessas dimensões. Alguns destes requisitos estão relacionados com as funcionalidades generalistas dos sistemas de DRM, enquanto outros estão orientados para o cumprimento de requisitos específicos para a qual o sistema foi concebido (Ku & Chi, 2004; Abie, 2007).

Nos anos mais recentes têm vindo a ser propostos diferentes modelos de DRM com características muito específicas (Hwang, 2008; Abie, 2007; Anderson, 2009), o que tem dificultado a sua aceitação em larga escala, pois as regras, conceitos e processos que os controlam são usualmente incompatíveis (Llorente, Rodriguez & Delgado, 2004). Apesar de grande parte da investigação nesta área se situar ao nível da proteção de conteúdos, o grande problema nesse campo reside na inexistência de um formato padrão de proteção de conteúdo pois cada sistema usa o seu próprio formato proprietário. Assim, é importante estabelecer uma solução que contribua para uma resolução duradoura deste problema, nomeadamente uma que permita associar, dinamicamente e de forma persistente, o detentor de direitos ao conteúdo sempre que este é utilizado. Independentemente de algumas questões que se possam levantar na criação e preparação do conteúdo, nomeadamente no estabelecimento de um formato de conteúdos e licenças plenamente aceites, ao nível da distribuição dois problemas, entre outros, se apresentam com grande relevância; o problema da distribuição segura das licenças que contêm as chaves que servem para cifrar/decifrar o conteúdo e o problema da delegação ou transferência de direitos concessionados a terceiros que essas licenças incorporam. Ou seja, como controlar a distribuição de licenças garantindo que os direitos inicialmente estabelecidos pelo autor/criador permanecem ao longo da linha sucessória. Em resumo, a solução passa por dar resposta às seguintes questões da investigação considerando o contexto académico:

- Quais os mecanismos mais apropriados que se podem incorporar numa solução global de DRM capazes de permitir a transmissão segura de licenças entre os intervenientes na partilha de conteúdo?
- Quais os mecanismos mais apropriados para o detentor de direitos os poder conceder a terceiros, mantendo controlada a linha sucessória de direitos?

Além disso, outras questões de investigação são igualmente relevantes, como:

(a) Qual a forma mais adequada de gerar as chaves de cifra/decifra de conteúdo de forma automatizada?

(b) Como proteger as licenças (ou objeto de direitos) que guardam as chaves de cifra/decifra do conteúdo?

(c) Qual a forma e o formato mais adequado para o "transporte" de conteúdos e licenças?
(d) Como se processa a transmissão de direitos entre os vários intervenientes durante o ciclo de vida do conteúdo?

(e) Como assegurar que as licenças emitidas são corretamente atribuídas relativamente aos direitos originais concessionados?

(f) Como assegurar que as licenças geradas são atribuídas aos utilizadores legítimos elegíveis do domínio académico?

(g) Como assegurar a utilização dos conteúdos dentro desse domínio?

A todas estas questões junta-se ainda uma outra questão de grande relevo para o futuro do DRM: será possível adaptar a arquitetura de uma solução DRM atualmente existente capaz de responder às questões acima referenciadas e que incorpore especificações de iniciativas *de* normalização (como por exemplo o MPEG-21) no contexto académico? Será que essa solução responde a estas questões, facilitando a gestão de direitos de PI sobre conteúdos no domínio académico, nomeadamente no processo de transmissão de direitos?

2.1 A investigação

Os sistemas de DRM atuais, graças a uma agregação de tecnologias de segurança, permitem que os detentores de conteúdo controlem o acesso e a sua distribuição restringindo a sua utilização de várias formas, mais ou menos vincada, consoante o contexto em que estão inseridos (Verslype & De Decker, 2006; Llorente, Rodríguez, Delgado & Torres-Padrosa, 2013). As atuais implementações, salvo raras exceções, são normalmente proprietárias e

escondem os respetivos detalhes (Verslype & De Decker, 2006). Uma grande maioria dos atuais mecanismos de DRM focam-se nas técnicas de proteção do conteúdo e deixam para segundo plano a sua distribuição no referente à transmissão de direitos (Zhang, 2011). Assim, o problema da partilha de conteúdos no contexto académico, do ponto de vista de proteção de direitos, pode ser descrito sucintamente em dois patamares distintos. Por um lado, ao nível da eficácia da proteção do conteúdo face ao contexto em que se insere, por outro, nos mecanismos que permitem a distribuição e posterior partilha do conteúdo. Para que possa ter sucesso, o sistema deve ter em conta a interação entre estes patamares de modo a aumentar a conveniência dos participantes, devendo identificar-se as tecnologias e também os sistemas mais apropriados que suportam o modelo de negócio inerente ao ciclo de vida do conteúdo (Iannella & Mclean 2002).

A investigação realizada no âmbito deste trabalho debruça-se precisamente sobre a forma como no meio académico o detentor de direitos de PI sobre conteúdos os pode proteger e controlar, nomeadamente os mais relevantes para o contexto académico, identificados nos estudos o *projeto ROMEO*[3] (Gadd et al., 2003b; Subramanya & Yi, 2006) e *Rights & Rewards*[4] (Bates, Loddington, Manuel & Oppenheim, 2007): o direito de preservação da integridade do conteúdo e o direito de atribuição. Uma vez que a abordagem seguida na investigação se baseia na utilização da tecnologia de DRM, o conteúdo é sempre mantido protegido e o distribuidor emite licenças que estipulam as operações permitidas sobre o conteúdo bem como as formas da sua utilização. Assim, procurou-se identificar e explorar o método eficaz no empacotamento (*packaging*) do conteúdo que o permite associar ao respetivo detentor de direitos, assim como os mecanismos apropriados na criação e distribuição de licenças que expressem as operações permitidas sobre o conteúdo de forma fiável e segura. Deste modo, é possível assegurar que o conteúdo é utilizado legitimamente, garantindo que a transmissão de direitos é realizada dentro do domínio académico, assegurando a linha sucessória.

Contrariamente aos sistemas proprietários, que raramente fornecem especificações e descrições da sua arquitetura, a norma ISO/IEC 21000 (Liu et al., 2003; Fragopoulos, Gialelis & Serpanos, 2009; MPEG-21:REL, 2005; MPEG-21:RDD, 2006), sendo *aberta*, permite definir ferramentas

[3] RoMEO Project (Rights Metadata for Open-archiving) funded by Joint Information Systems Committee (JISC), http://www.lboro.ac.uk/microsites/infosci/romeo/

[4] Rights and Rewards in Blended Institutional Repositories project is funded under the Joint Information Systems Committee (JISC) Digital Repositories Programme, http://www.jisc.ac.uk/whatwedo/programmes/digitalrepositories2005/rightsandrewards.aspx

elementares para a construção da base de sistemas de DRM. Por isso, é extremamente útil no controlo de direitos de PI em conteúdos de natureza académica, sendo, por isso, das mais indicadas para o desenvolvimento dos conceitos apresentados ao longo da investigação. Esta norma, e as várias partes que a compõem, ao definirem especificações que levam à implementação das ferramentas básicas com o propósito de possibilitar a criação, envio e aquisição de conteúdos digitais de uma forma segura respeitando os direitos de PI são um dos pilares do desenvolvimento dos sistemas de DRM atuais. Esta norma, pode assim ser entendida como um conjunto de especificações que, quando combinadas, podem originar uma solução compreensiva para um domínio aplicacional específico. Sendo independente do tipo de conteúdo, pois especifica um método genérico não só de empacotamento como de descrição e de processamento do conteúdo, permite especificar uma infraestrutura interoperável para a criação, distribuição e consumo do conteúdo capaz de servir como referência. Quando devidamente aplicada consegue fornecer o enquadramento adequado para a utilização de conteúdo não só académico mas também de diferentes domínios com vista à preservação de direitos de PI, pois incorpora as normas MPEG-21 IPMP (MPEG-21:IPMP, 2006) e MPEG-21 REL (MPEG-21:REL, 2005) capazes de suportar sistemas de DRM (Sheppard & Safavi-Naini, 2006a; Yang, Wei & Zhang, 2008).

Assim, e de forma a atingir alguns dos objetivos especificados, a norma e a integração de algumas das suas partes foi considerada na abordagem seguida, adaptando-se o sistema de DRM de especificação aberta e de código aberto OpenSDRM (Serrão, 2008) resultando no ARMS como caso de estudo, como plataforma capaz de suportar a partilha de conteúdos abrangidos por direitos de PI. Os conceitos apresentados ao longo da investigação inserem-se num contexto educacional e académico, não comercial, focando-se no objetivo de melhorar a gestão e partilha de conteúdos e direitos associados aquando da sua distribuição. A solução proposta, é baseada num modelo de DRM suportada pela plataforma ARMS que foi adaptada do OpenSDRM e suportada pela norma MPEG-21, já que as suas especificações são direcionadas para dar soluções a muitos dos problemas relacionados com os direitos de PI num vasto leque de domínios de aplicação (Angelides & Agius 2010; Sheppard, 2007; Van de Walle & Koenen, 2006). Muita da investigação na área do DRM, tem realçado o impacto da portabilidade de conteúdos e direitos, essencialmente a retransmissão de direitos entre utilizadores (Sans, Cuppens & Cuppens-Boulahia, 2007; Sachan, Emmanuel & Kankanhalli, 2011, 2012). A dificuldade de retransmissão de direitos é mais notória em sistemas DRM onde as licenças são personalizadas para só poderem ser usadas por um utilizador específico restringindo a sua

reutilização legal por terceiros. Esse assunto será aqui abordado, sendo proposto um mecanismo de retransmissão de direitos entre utilizadores em sistemas DRM baseados na identidade (Palavalli, Srinivas & Pais, 2008) com vista a manter a linha sucessória.

2.2 Abordagem metodológica

De acordo com as questões levantadas, a investigação vai ser orientada para dar uma resposta em "como efetuar a partilha de conteúdo implementando uma solução de DRM aberta orientada para o contexto académico e baseada em normas internacionais de forma a transmitir e preservar os direitos de PI sobre conteúdos partilhados, nomeadamente os direitos de autoria e o respeito pela integridade do conteúdo". Tendo em atenção a escassa informação existente no domínio dos sistemas de gestão direitos sobre conteúdos no contexto académico, uma abordagem de caso de estudo (Yin, 2009) foi considerada como a mais adequada (Benbasat, Goldstein, & Mead, 1987; Strauss & Corbin, 1990). De acordo com Yin (2009), as estratégias de caso de estudo são preferíveis quando a questão de investigação colocada envolve "como?" ou "porquê?" na análise de um fenómeno no seu contexto real. De modo a dar seguimento à investigação, tomou-se como objeto de estudo a integração de várias partes da norma MPEG-21 em conjunto com a plataforma "aberta" ARMS, desenvolvida e adaptada ao contexto em causa.

Consciente de que este método não permite a generalização em larga escala, o objetivo consiste em generalizar os resultados obtidos para propostas teóricas ao invés de populações ou universos. A metodologia adotada surge do confronto da abordagem da análise de casos de estudo apresentada por Yin (2009) e da adaptação do método ao processo de desenho em engenharia (Hess, 2001). Para dar seguimento ao trabalho de investigação foi necessário analisar várias normas internacionais e soluções de DRM "abertas", capazes de suportar a partilha de conteúdo no contexto académico. Da análise genérica sobressaiu o sistema de DRM OpenSDRM como o mais relevante para o fim em vista, do qual resultou por adaptação do mesmo, a plataforma ARMS. O passo seguinte consistiu em definir um modelo de gestão digital de direitos de referência. Assim, foi possível enquadrar a plataforma ARMS e perceber o seu modo de funcionamento, no respeitante à proteção e partilha de conteúdo assim como à definição e retransmissão de direitos associados no contexto académico tendo por referência a norma MPEG-21. Foi analisada a transmissão e mobilidade de recursos digitais proporcionados pela integração de várias partes da norma MPEG-21 com outras normas, estabelecendo-se a

estrutura genérica de transporte destes recursos num sistema DRM, capaz de assegurar níveis adequados de proteção.

Com vista a assegurar a permanência da utilização de conteúdo dentro do domínio académico foram definidos vários mecanismos de controlo, viabilizados pela norma MPEG-21, que possibilitam a preservação da linha sucessória de direitos quando se emitem licenças entre os participantes. Por fim, procedeu-se à elaboração da validação da proposta, considerando vários cenários de utilização no contexto académico, tendo em conta a transmissão de conteúdos e de direitos entre utilizadores que assumem vários papéis na plataforma ARMS.

3 Objetivo da investigação

Para dar resposta às questões anteriormente mencionadas, a investigação conduzida tem como objetivo geral especificar e desenhar uma solução de DRM que possa ser utilizada nos contextos educacional e académico dando resposta aos requisitos específicos dos detentores de direitos sobre o conteúdo digital partilhado no que respeita ao suporte oferecido à preservação dos seus direitos mais elementares neste contexto: a preservação da integridade do conteúdo e o direito de atribuição. Nesta linha de orientação pretende-se dar resposta à forma de como respeitar a transmissão de direitos entre os participantes no fluxo de conteúdo, de forma a manter a linha sucessória definida pelo autor/detentor do conteúdo.

Sendo atualmente a Internet o canal de distribuição de conteúdos por *download* o mais vulgarizado no meio académico, dar-se-á especial atenção a este canal. Será analisada a aplicação de um sistema de DRM no contexto educativo centrando a atenção na proteção do conteúdo, nos processos de distribuição e na gestão dos direitos associados, tomando por referência os direitos mais elementares que o detentor de direitos pretende preservar (integridade e autoria), não descurando outros direitos (Gadd, Loddington & Oppenheim, 2007). A redistribuição de direitos é uma das técnicas chave do DRM que torna o DRM mais aceitável para os utilizadores pois além de aumentar a motivação dos utilizadores comuns na aquisição, uso e partilha de conteúdos também diminui a possibilidade de atentados (Cheung et al., 2002). Por isso, esta tese incidirá sobre a área de deteção de violação de direitos (Sachan, Emmanuel & Kankanhalli, 2009, 2010), no correspondente à validação da emissão de licenças no contexto académico tendo em vista a preservação dos direitos transmitidos ao longo da linha sucessória.

São também de destacar outros objetivos relevantes nesta investigação:

1. Proposta de um modelo de referência que sirva de guia para sistemas de proteção de direitos sobre conteúdos digitais no contexto educacional e académico;
2. Verificação da viabilidade de exploração de um sistema de DRM de especificações e código aberto, devidamente adaptado ao contexto académico, de forma a ser capaz de dar resposta às necessidades básicas dos principais intervenientes neste meio;
3. Definição de mecanismos de concessão de direitos baseados na norma internacional MPEG-21 que assegurem o controlo de direitos no domínio educacional e académico, tendo em vista a preservação da linha de direitos sucessórios dos participantes no fluxo de conteúdo em DRM.

Tendo por base a proposta de um modelo de referência dar-se-á especial ênfase aos processos de transmissão de direitos e sua viabilidade de implementação numa plataforma "aberta" no contexto académico, tendo em conta a integração da norma MPEG-21, em especial a sua vertente de expressão e transmissão de direitos. A integração desta plataforma DRM com o sistema de gestão académica das instituições educacionais será tida em conta com vista a validar o licenciamento de direitos dentro do domínio académico aplicando mecanismos específicos que permitem a transmissão de direitos em concordância com a linha sucessória.

4 Contributos

Os principais contributos que pretendemos apresentar nesta tese incluem o desenvolvimento de novas abordagens com novas soluções que podem ser usadas na implementação do modelo proposto com vista à gestão de direitos de PI sobre conteúdos no contexto académico nomeadamente o controlo sobre direitos transmitidos. As novas soluções apresentadas envolvem formas seguras de gerir e utilizar conteúdos neste contexto com vista ao respeito pelos direitos de PI. As soluções propostas têm em vista a partilha de conteúdos dentro do domínio académico estabelecendo a ligação entre as licenças e conteúdo relacionado com o detentor, através de técnicas e mecanismos apropriados de modo a limitar a proliferação do uso ilegítimo de conteúdos e estabelecendo o respeito pela linha sucessória na emissão de licenças.

Com esta tese espera-se assim poder contribuir para o avanço da ciência, no domínio do saber das ciências e tecnologias de informação, especificamente na área da gestão de direitos digitais sobre conteúdos no contexto académico através de:

- Proposta de um modelo de referência de proteção de direitos de propriedade intelectual sobre conteúdos adaptado ao contexto académico, baseado em dois canais de transmissão distintos (um para o conteúdo e outro para licenças), capaz de satisfazer as necessidades de

preservação de direitos num sistema DRM genérico. Esta proposta de modelo de referência vem permitir a validação das licenças a emitir para utilizadores no meio académico através do recurso à interação com a plataforma de gestão das atividades académicas;

- Proposta de uma estrutura genérica de conteúdos e licenças baseada nas normas internacionais MPEG-21 que permita o seu transporte entre os intervenientes num sistema DRM, assim como o rastreio de direitos delegados;
- Novos mecanismos de processamento de emissão de licenças interligados à plataforma de gestão das atividades académicas de uma entidade académico que permitem controlar a elegibilidade dos utilizadores no domínio académico com vista à emissão de licenças baseados na norma MPEG-21 que validam o procedimento de delegação/concessão de licenças tendo em conta o respeito pela linha sucessória de direitos;
- Uma nova arquitetura suportada no modelo de referência proposto usando uma arquitetura orientada por serviços e capaz de permitir variados níveis de proteção e que incorpora especificações da norma MPEG-21 direcionadas para a realidade do licenciamento no contexto académico.

5 Estrutura do documento

Esta tese está organizada em cinco partes distintas e onze capítulos diferentes.

A primeira parte "Introdução e contextualização da investigação" está dividida em três capítulos. No primeiro capítulo é realizado o enquadramento da investigação. Este capítulo apresenta uma visão global do tema e do desafio colocado, focando a importância e a pertinência da investigação proposta, define os objetivos de pesquisa e identifica lacunas no domínio da investigação e literatura científica. Além disso, apresenta as contribuições, a estrutura global do documento e a terminologia utilizada. O segundo capítulo resulta do levantamento da problemática relativa à necessidade de proteção de conteúdos no contexto académico e da razão da utilização de sistemas de gestão de direitos de PI sobre conteúdos. De modo a perceber qual a tecnologia e mecanismos que os principais sistemas de DRM utilizam, realizou-se um levantamento e estudo sobre o estado atual e tipo de sistemas usados, assim como as diferentes tecnologias utilizadas. No terceiro capítulo efetua-se uma análise das principais soluções DRM baseadas em código aberto que recorrem a normas abertas. Esta análise termina com o levantamento das principais soluções com vista à seleção de uma delas para adaptação ao contexto académico.

A segunda parte " Proposta de modelo de referência de DRM e integração do OpenSDRM" é composta por três capítulos. O quarto capítulo incide no desenvolvimento de um modelo de referência que se foca na apresentação da base conceptual que o suporta. Além do modelo, é também proposta uma arquitetura genérica capaz de acomodar os interesses dos participantes no contexto académico, tendo em conta as especificidades dos processos de DRM relacionados com a proteção de conteúdos. O quinto capítulo dá continuidade ao capítulo anterior, mas incide no processo de transmissão de licenças e na sua proteção. Seguindo a contextualização da questão de pesquisa, faz-se a análise de casos de utilização estendendo o modelo anteriormente proposto às questões de retransmissão e rastreio de direitos, realçando a problemática existente nesta área que contribui para a sua indefinição, e apresentando possíveis soluções.

Finalmente o sexto capítulo analisa a viabilidade de adaptação do sistema OpenSDRM face aos requisitos específicos do meio académico tendo em conta a norma MPEG-21, demonstrando o alinhamento do OpenSDRM com o modelo proposto anteriormente, e realçando a sua adaptabilidade graças à sua arquitetura baseada em serviços. É aqui redefinida a arquitetura do OpenSDRM de modo a adaptar-se ao contexto académico.

A terceira parte "Transmissão de conteúdos e direitos no OpenSDRM adaptado" é composta por dois capítulos. O sétimo capítulo analisa a transmissão e a mobilidade dos recursos digitais proporcionados pela norma MPEG-21, quer do conteúdo quer da licença, assim como as respetivas estruturas capazes de viabilizar o seu transporte e proteção. Tem como contributo principal a definição de uma estrutura genérica de conteúdos e licenças, baseada nesta norma, que viabiliza o seu transporte entre os vários intervenientes num sistema DRM. São aqui analisados vários casos de utilização no respeitante ao descarregamento e superdistribuição de conteúdos na plataforma ARMS. O capítulo oitavo concretiza a análise do capítulo anterior verificando a aplicabilidade do modelo proposto sobre a plataforma ARMS que serviu como caso de estudo. Em concreto são descritos os processos de proteção de conteúdos e de transferência de direitos nas situações mais comuns a este meio utilizando as funcionalidades proporcionadas pelo ARMS.

A quarta parte "Transmissão de direitos e mecanismos de controlo" é composta por dois capítulos. O nono capítulo estende o enquadramento da delegação de licenças proposto no capítulo quarto, e discute como, na atualidade, é possível implementar políticas de transmissão de direitos expressas nas licenças de delegação que utilizam a norma MPEG-21. Alguns cenários de utilização, que capturam alguns problemas reais no contexto educacional e

académico, são aqui introduzidos dando-se realce ao controlo da concessão de direitos por parte do distribuidor tendo em vista a transmissão destes respeitando os limites na linha sucessória.

O décimo capítulo complementa o capítulo anterior introduzindo a definição de novos mecanismos de controlo de delegação de direitos, para o contexto académico tendo em vista uma concessão controlada de direitos transmitidos entre utilizadores.

A última parte deste trabalho "Conclusão e Investigação futura" é composta por um capítulo que conclui a investigação, evidenciando os resultados mais relevantes e a contribuição para o domínio científico. São também aqui apontados novas direções e oportunidades de investigação a realizar no futuro tendo por base o trabalho realizado.

Capítulo 2

Gestão de direitos de PI no meio académico e sistemas DRM

Resumo

Ao longo deste capítulo é efetuado um levantamento da necessidade e problemática da proteção de conteúdos no contexto educacional e académico e da razão da utilização de sistemas de gestão de direitos de propriedade intelectual sobre conteúdos, sendo descritos os fundamentos em que se baseiam os sistemas de gestão de direitos DRM. É igualmente apresentado o modo de funcionamento deste tipo de sistemas, a tecnologia subjacente e o modo como as entidades envolvidas no fluxo de conteúdo protegido estão estruturadas. Para se perceber qual a tecnologia e mecanismos que este tipo de sistemas utiliza, faz-se uma análise sobre o estado atual deste tipo de sistemas incidindo sob o ponto de vista de segurança e vulnerabilidades genéricas, assim como uma breve apresentação da problemática relacionada com o licenciamento de direitos.

1 Introdução

Desde o advento das Tecnologias da Informação e Comunicação (TIC) que o processo de inovação e integração tem marcado o mundo atual. Ao fazer realçar o conhecimento, a era da informação aumentou consideravelmente as preocupações relacionadas com a PI, em especial para as universidades e outras entidades do sistema educativo (Sun & Baez, 2009). Atualmente, é muito fácil para qualquer pessoa produzir e publicar conteúdos e a área da publicação académico também não deixou de ser afetada por esta revolução. Devido a estas mudanças está a surgir um mercado de conteúdos educativos digitais com uma abordagem que engloba a distribuição e venda de produtos tangíveis e a distribuição e licenciamento de produtos intangíveis (Diaz, 2009; Nelson, 2006). Esta mudança acaba por ter um impacto muito forte na gestão de direitos de conteúdos educacionais, pois o tipo de ameaças aos direitos de PI ganha outra dimensão. Ao investir na produção de conteúdos, o criador tem toda a legitimidade em querer proteger o seu investimento sujeito a direitos de autor, exigindo contrapartidas (financeiras, reconhecimento, entre outros) pela sua utilização, de modo a amortizar as despesas de produção. O meio académico é muito particular neste aspeto, pois a motivação que pode

estar por detrás dessa legitimidade é diferente de outras áreas e normalmente está relacionada com o desejo de o autor ter mais prestígio/reconhecimento perante os seus pares (Sun & Baez, 2009). A proteção da PI sobre os conteúdos é assim, essencial para evitar a utilização abusiva dos mesmos.

O acesso a repositórios de conteúdos educativos com direitos de PI é feito tradicionalmente através de processos de autorização de acesso onde a autenticação é baseada em credenciais ou em restrição de endereços IP. Como exemplo podemos referir o consórcio de bibliotecas b-On (http://www.b-on.pt) onde as instituições de ensino superior em Portugal, entre outras, podem aceder a conteúdos de cariz científico. Contudo, estes esquemas simples de proteção são facilmente contornáveis, o que cria sérios problemas no respeitante à preservação de direitos. Normalmente, os legítimos proprietários dos conteúdos tentam evitar estes abusos condicionando o acesso, apresentando declarações/notificações de direitos de autor e inserindo números de série. Mas a realidade demonstra que estes métodos não têm sido um sério obstáculo à violação de direitos sendo inúmeros os casos de desrespeito, mesmo no meio académico (Johns, 2010; Bretag, 2013). Pode-se assim deduzir que os sistemas de proteção de direitos de PI que se baseiam unicamente em esquemas de autorização de acesso não têm uma elevada eficácia. Uma forma comum de contornar esta vulnerabilidade envolve a implementação de mecanismos de proteção nos próprios conteúdos, permitindo a sua cópia física, mas inviabilizando a sua utilização de forma não autorizada. Ou seja, para que seja realmente eficaz, a proteção de direitos de PI de conteúdos deve ser intrínseca aos próprios, independentemente do lugar onde estão, permanecendo tecnicamente protegidos, e mantendo-se sempre essa proteção seja qual for a localização do conteúdo (Rosenblat & Dykstra, 2003).

No meio educacional e académico o tipo de conteúdo mais usual é aquele que é definido como sendo livre, ou seja, é percebido como de uso livre. Mas muito deste conteúdo é também conhecido como sendo "conteúdo aberto", tendo sido criado por autores com o intuito de o partilhar com o público. O autor concede aqui permissões, como a distribuição livre e a reutilização, num tipo de licenciamento conhecido como "licenciamento de conteúdo aberto". Este tipo de conteúdos tem vindo a aumentar consideravelmente nos últimos tempos (mais de 20 milhões de ficheiros, segundo a *Wikimedia Commons Repository*; http://commons.wikimedia.org/) dando uma enorme visibilidade aos seus promotores (Park, 2011). O licenciamento desses conteúdos assume um aspeto central, pois, assim, estes podem ser usados e partilhados automaticamente. Várias organizações desenvolveram licenças específicas para esse efeito (por exemplo, a iniciativa *Creative Commons*;

http://creativecommons.org), permitindo a partilha e reutilização do conteúdo. Contudo, existem outros licenciamentos mais restritivos que não permitem a reutilização do conteúdo com alterações. Além disso, uma restrição comum a ser seguida é a do respeito da autoria do conteúdo. Este tipo de licenciamento é muitas vezes utilizado quando o conteúdo contém informação que já está no estado final e que, por isso, não deve ser alterada ou adaptada. Estas licenças estão disponíveis livremente e podem ser aplicadas a qualquer tipo de conteúdo. O texto da licença é a base da tomada de decisão quando há disputas entre as partes envolvidas num conflito. Um movimento que faz uso desse tipo de licenciamento, e que é largamente conhecido no meio académico, é a iniciativa "acesso livre" Open Access (http://open-access.net/). Apesar desta iniciativa promover a partilha de conteúdos e contribuir para uma maior disseminação do conhecimento, as licenças utilizadas são meramente descritivas dos direitos associados ao conteúdo. Tal deixa uma questão em aberto: como proteger efetivamente o conteúdo para que este possa ser utilizado com o respeito dos direitos especificados no licenciamento? Uma possível resposta passa pelo processo de licenciamento e pela utilização de mecanismos de proteção. Estas são as peças chave na partilha de conteúdos de conhecimento abrangidos por direitos de PI, pois sempre que exista uma licença que possa ser interpretada automaticamente num contexto que assegure a verificação e validação dos termos nela expressa a sua partilha poderá ser realizada de forma controlada (Morin, 2009).

Ao pretender acelerar a partilha e uso de conteúdos muitos dos tipos de licenciamento existentes possuem alguns condicionalismos que devem ser observados. Um desses condicionalismos é o de que o conteúdo deve possuir uma atribuição ao autor de forma permanente, declarando quem é o detentor de direitos e respetivo licenciador. No meio académico, e em grande parte da economia do conhecimento, a atribuição de autoria é de enorme importância pois a autorização para utilizar o conteúdo é concedida partindo do pressuposto de que a autoria é devidamente reconhecida (Gadd, Oppenheim & Probets, 2003a). A fidelidade também é aqui importante, devendo por isso a integridade do conteúdo ser respeitada, pois muitos autores não desejam que as suas ideias sejam referenciadas sem ter a certeza de que são expressas de forma correta (Wenqing, Wanting & Di 2005). Cerca de 75% dos professores e investigadores do meio académico pretendem que esses esses dois requisitos sejam observados (Gadd et al., 2007; Bates et al., 2007). Estes são os direitos mais básicos que qualquer criador de conteúdos baseados em conhecimento pretende preservar. Não havendo garantias de que esses direitos possam ser preservados com grande eficácia pela ética e pelas leis em vigor a forma que se apresenta com melhores perspetivas de sucesso nessa área passa pela aplicação de medidas de

proteção tecnológica. Os sistemas DRM, pelas suas características, conseguem dar resposta a esta necessidade pois sobrepõem-se ao ciclo de vida do conteúdo, oferecendo garantias de satisfação das necessidades sentidas nesta área pelo meio educacional eacadémico não só na gestão do conteúdo mas igualmente na gestão dos direitos a ele associados. Apesar de algumas vozes discordantes referirem limitações impostas na utilização de conteúdos, o recurso aos sistemas de DRM vem trazer vantagens (Chaudhuri, 2007), tais como:

- A distribuição segura de conteúdos – ao encriptar o conteúdo, o sistema DRM vai permitir aos autores e distribuidores enviar esse conteúdo por redes não seguras (por exemplo, a Internet) de modo a que possa ser utilizado pelos destinatários corretos;
- A proteção do conteúdo digital – ao proteger conteúdos através da encriptação torna-se necessária a utilização de uma chave que decifra o conteúdo. Se o utilizador não possuir essa chave o conteúdo não tem qualquer utilidade;
- A identificação dos participantes - o recurso a certificados digitais fornece a capacidade de identificar os participantes garantindo que estes são genuínos;
- A autenticidade do conteúdo – a utilização de técnicas de resumo ("*hashing*") permite garantir que o conteúdo é autêntico e legítimo;
- O não repúdio da transação - a utilização de criptografia de chave pública garante que a transação foi realizada pelos participantes que nela tomaram parte. Ao verificar a assinatura correspondente à transação com as chaves dos participantes pode-se garantir a autenticidade da transação, tendo-se confiança de que os participantes estiveram envolvidos realmente na transação original.

2 Ciclo de vida do conteúdo e gestão de direitos

O ciclo de vida do conteúdo digital pode ser visto como um processo onde o conteúdo e informação associada (por exemplo, chaves criptográficas) são transmitidos de um participante para outro para que se execute uma ação de acordo com um conjunto de regras procedimentais (Llorente et al., 2004). Os processos inerentes à gestão dos direitos digitais fazem parte de um contexto mais lato que engloba a gestão do conteúdo. Neste contexto os fluxos de direitos ao longo do ciclo de vida do conteúdo fazem parte do processo de partilha de conteúdo. A Tabela 1, adaptada de (Collier et al., 2004b), fornece a base em que assenta o modelo de gestão do ciclo de vida do conteúdo e de algumas questões gerais sobre os direitos associados dos participantes envolvidos e das operações possíveis de realizar sobre o conteúdo durante o seu ciclo de vida.

Papel	**Ação**	**Observações**
Criação do conteúdo		
Autoria/cria	Criar novos conteúdos originais ou criar a partir de material já existente.	A licença pode ser definida quando o conteúdo é criado devendo-se considerar a intervenção de tecnologia de suporte. Os direitos devem ser consolidados quando o conteúdo é proveniente de múltiplas fontes.
Agrega	Juntar conteúdos de várias proveniências e reunir num trabalho mais compreensivo.	
Distribuição/oferta de conteúdo		
Publica	Preparar e enviar conteúdo para distribuição ao público.	Os direitos devem ser publicados, catalogados e distribuídos conjuntamente com o conteúdo. Informação sobre os direitos deve ser preservada ao longo da publicação e da distribuição. As licenças de distribuição são diferentes das de utilização.
Cataloga	Classificar e registar os atributos dos conteúdos.	
Distribui	Distribuir o conteúdo aos utilizadores alvo.	
Aquisição/consumo do conteúdo		
Pesquisa	Procurar conteúdo e descobrir aquele que obedece ao critério.	A informação de direitos pode ser utilizada como critério de procura. Os direitos devem ser adquiridos antes de usar o conteúdo.
Obtenção	Aquisição do acesso ao conteúdo no formato necessário para suportar a utilização desejada.	
Utiliza	Reproduzir e interagir com o conteúdo.	Os direitos determinam como e quando o conteúdo pode ser usado. A aplicação de direitos será assegurada quando o conteúdo for utilizado.

Tabela 1 – Ciclo de vida do conteúdo e questões sobre direitos

O fluxo de conteúdo ao longo do ciclo de vida representa os diferentes passos ou fases através das quais o conteúdo passa, desde a sua criação inicial (ou proteção, se não o detentor do conteúdo mas o fornecedor desse conteúdo) até à sua distribuição e aquisição (Marques & Serrão, 2011). No decorrer deste ciclo, vários atores, conteúdo, informação relacionada e processos podem estar envolvidos assim como um conjunto de condições que devem ser expressas de modo a que os direitos sejam observados. Em concreto existe um conjunto de regras que devem ser expressas e respeitadas com vista a que:

- Os autores sejam citados (através de um método específico);
- As ligações ao trabalho original sejam incluídas de modo a que o direito de atribuição seja observado;

- O conteúdo não possa ser alterado por nenhum processo de modo a que o direito de integridade não seja respeitado.

2.1 Gestão de direitos de PI no meio educacional e académico

O objetivo da maioria dos principais intervenientes no meio educacional académico, nomeadamente os professores e os investigadores, é partilhar conteúdos o máximo possível, recebendo a atribuição do crédito apropriado sempre que o seu trabalho é usado (Gadd et al., 2007). A autoria, ou atribuição de crédito, é peça fulcral da atividade académica e uma forma de mostrar o reconhecimento do mérito do(s) autor(es) pelos seus pares. Sabendo que a autoria pode ser ignorada ou que pode haver uma apropriação indevida, o que se pretende ao aplicar a gestão digital de direitos é precisamente evitar que o mérito pelo trabalho realizado seja atribuído ilegitimamente. Por isso, o interesse em usar sistemas de gestão de direitos PI tem aumentado, pois com estes sistemas pode-se garantir o devido reconhecimento da autoria das criações, assegurar a integridade das suas obras e regular como e por quem são usadas (Bates et al., 2007). Sendo a tecnologia de DRM orientada para a proteção de direitos e conteúdos, quando orientada para atingir os objetivos referenciados por (Collier & Robson, 2004), tal vem ao encontro das aspirações de uma grande parte da comunidade académica, o que aumenta o seu potencial para poder vir a ser adotado neste meio (Barik & Karforma, 2012).

No âmbito comercial, a aplicação de tecnologia capaz de assegurar a aplicação de direitos de forma automatizada sobre o conteúdo tem tido algum sucesso essencialmente na área de vídeo jogos e e-books (Earnings, 2014; Insider Monkey, 2013). Nas comunidades educativas e de investigação, este tipo de tecnologia raramente tem sido utilizado (salvo vários exceções muito pontuais e orientadas para fins comerciais, como por exemplo o IPOS-DS (Torres et al., 2010), uma vez que o conteúdo é distribuído para um utilizador que pertence ao meio, partindo-se do pressuposto de que o reconhecimento é realizado tacitamente. Nesta situação, normalmente, é concedido o direito de acesso ao conteúdo por parte do investigador ou professor através de uma validação simples no momento de distribuição. Mas nada fica assegurado sobre que uso o conteúdo possa ter depois de este estar nas mãos do utilizador. Assim, torna-se necessário estabelecer uma política de gestão de direitos que, por sua vez, requer a identificação do tipo de conteúdo digital que a comunidade pretende gerir assim como dos diferentes tipos de conteúdos e de modelos de direitos que esta apoiará. Depois de determinadas, estas políticas precisam de ser claramente definidas em termos processuais, tecnológicos e legais.

Para além destas diferenças relativamente a objetivos, também existem grandes diferenças nos conteúdos comerciais e educacionais (não comerciais) do ponto de vista do ciclo de vida. Em primeiro lugar, o conteúdo no meio académico é frequentemente modificado pelo "consumidor" e reincorporado em "novo" conteúdo que contém direitos de PI de múltiplas fontes. Em segundo lugar, professores, investigadores, alunos e as suas organizações agem como produtores, distribuidores e consumidores de conteúdos digitais, em simultâneo, e estes papéis não são estanques nem distintos (Collier & Robson, 2004). Apesar do tipo de participantes envolvidos na criação e consumo de conteúdos ter características diferentes (por exemplo autor, editor, gestor estudante ou professor) nada impede que o papel desempenhado se altere. Por exemplo, um professor pode ser um criador/autor, mas também um simples consumidor ou até mesmo um distribuidor autorizado de conteúdos da instituição educacional onde trabalha. Mesmo sendo a mesma entidade os seus interesses são bastante distintos. Por exemplo, um professor atuando como autor interessa-lhe proteger os seus direitos de autoria mas como utilizador interessa-lhe que o conteúdo seja genuíno.

2.2 Cenários de gestão de direitos e meio académico

A necessidade de ter métodos que limitem a forma como o conteúdo pode ser utilizado leva a que os detentores possam ter ferramentas e mecanismos que lhes possibilitem proteger os conteúdos que criaram e, provavelmente, estabelecer os seus próprios direitos de utilização sobre estes, podendo especificar aos potenciais utilizadores como é que os seus conteúdos digitais deverão ser usados (Gadd, Loddington & Oppenheim, 2007). Perante estes fatores, o DRM é uma das respostas possíveis, mesmo no meio educacional e académico, pois, ao disponibilizar estas ferramentas e mecanismos, vem dar resposta a esta necessidade a quem desejar preservar os seus direitos.

A gestão de direitos no meio académico é diferente da realizada noutros setores. Os objetivos da criação de PI na comunidade de investigação e ensino são diferentes dos do contexto comercial, logo, os métodos e tecnologias necessários para os apoiar não são os mesmos. Assim, é possível identificar dois cenários: o comercial e o não-comercial/académico (Marques & Serrão, 2012a), ambos inerentemente relacionados com o tipo de rendimento (financeiro, prémio, recompensa, entre outros) a que a utilização do conteúdo conduzirá (Tabela 2).

Comercial	**Não-comercial/Educacional**
Foca-se na rentabilidade financeira, que é conseguida através da garantia	Foca-se no prémio/recompensa, tornando o conteúdo o mais acessível e partilhado possível.

da vigência de direitos com base em métodos legais e tecnológicos.	
Assume que não há direito de acesso nem de uso se não houver licença.	Assume que todos podem aceder aos conteúdos e usá-los dentro de parâmetros legais ou de outras permissões/restrições.
Foca-se no licenciamento e proteção do conteúdo/licença, de modo a preservar os direitos dos detentores.	Foca-se na difusão global através da partilha do conteúdo com propriedade intelectual e da manutenção da integridade e atribuição de direito.
O conteúdo é usado por utilizadores que possuem licença. Existe uma corrente de atores pré-definidos que possuem papéis específicos relativamente ao ciclo de vida do conteúdo.	O conteúdo é usado e reutilizado (alterado, agregado) através de um processo colaborativo onde o utilizador pode recriar as criações; neste caso, a utilização tendo em conta as exceções permitidas ao direito de autor é a doutrina legal adotada. O papel dos atores relativamente ao ciclo de vida do conteúdo é indistinto.

Tabela 2 – Gestão de direitos no meio comercial e académico

Pela análise destas diferenças é possível concluir que as atividades relacionadas com a partilha de conteúdos no meio académico não comercial, nomeadamente nas áreas de investigação e ensino, requerem políticas, modelos e tecnologias que apoiem a partilha e a reutilização de recursos digitais e não as limitem. As soluções efetivas de gestão de direitos, sendo necessárias para possibilitar esta partilha, devem ao mesmo tempo implementar técnicas e mecanismos onde as condições que os detentores de direitos possuem, sejam respeitadas de modo a estabelecer um equilíbrio nos direitos de todos os participantes no ciclo de vida do conteúdo (Etinger, Vitasović, & Šehanović, 2009), de modo a não restringir a partilha do conhecimento.

3 Gestão digital de direitos

As diversas tentativas de implantação de sistemas DRM têm demonstrado que o seu sucesso depende não só da tecnologia, mas também dos aspetos relacionados com o modelo de negócio subjacente (Rosenblatt, Mooney & Trippe, 2004). Ao pretender definir a estratégia de como servir clientes, o modelo de negócio, em grande medida, afeta e é afetado pela tecnologia utilizada. O criador produz um conteúdo digital e fornece as regras de utilização a terceiros (distribuidor), que são responsáveis por garantir que este é usado adequadamente. Os fornecedores recebem o conteúdo dos criadores e distribuem-no de forma a este chegar aos seus utilizadores finais (consumidores). Para que estes utilizem o conteúdo, é necessário que obtenham a licença apropriada, o que acontece depois de o consumidor (utilizador final ou

cliente) enviar o pedido para o distribuidor da licença. A transação é terminada quando o utilizador final está satisfeito com as condições especificadas no modelo de pagamento (por exemplo, pagar para imprimir, pagar para ver, entre outros). De seguida, o criador do conteúdo é notificado acerca dessa transação. O tipo de proteção, o tipo de distribuição e a forma como se assegura a aplicação de direitos vai condicionar o modelo de negócios a selecionar e vice-versa.

Qualquer sistema DRM requer que os direitos sobre conteúdos tenham de ser expressos, pois só assim se consegue especificar os direitos a transmitir entre os participantes no ciclo de vida do conteúdo (Wang, 2006). Tal pode ser realizado mesmo recorrendo a uma sintaxe arbitrária, dependendo a interpretação desses direitos da implementação realizada no sistema. Mas tal não é recomendável, pois se um conteúdo for distribuído para outro sistema DRM, então deixa de ter qualquer utilidade. Por isso, é necessária uma forma normalizada de expressar e interpretar a especificação de direitos como forma de contributo para a interoperabilidade entre diferentes sistemas (Maroñas, Rodríguez & Delgado, 2009a; Prados, Rodriguez & Delgado, 2005). Do ponto de vista tecnológico, para assegurar a necessária proteção dos direitos num ambiente *online*, os sistemas de gestão digital de direitos recorrem a um diverso conjunto de técnicas e mecanismos que permitem disponibilizar, através de uma infraestrutura de rede, vários serviços, quer a consumidores, quer aos detentores de conteúdo (Buyens, Michiels, & Joosen, 2007; Michiels, Verslype, Joosen, & De Decker, 2005). A abordagem fundamental deste tipo de sistemas envolve a proteção do conteúdo para tornar possível o seu uso somente por aqueles que possuam as ferramentas/mecanismos para desproteger esse conteúdo. Estes só poderão ser utilizados (reproduzidos, impressos, copiados, entre outros) em aplicações especificamente concebidas para proteger a PI desses conteúdos, aplicações essas que necessitam de uma licença específica contendo a cifra e regras de utilização para que o utilizador possa usar esses conteúdos protegidos (Figura 2). Se os conteúdos forem transmitidos a terceiros, sem a respetiva licença, não será possível realizar a reprodução (Michiels et al., 2005).

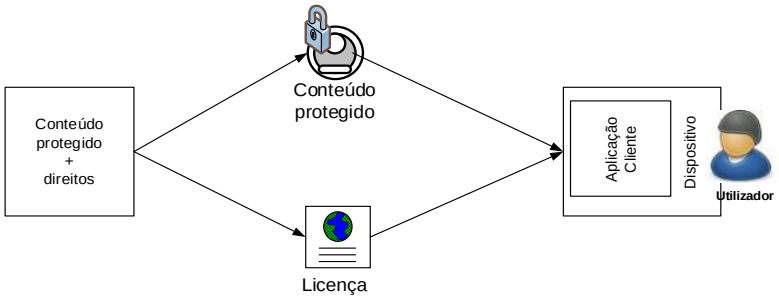


Figura 2 – Transmissão de conteúdos e direitos num sistema DRM básico

A licença pode ser atribuída a utilizadores ou a dispositivos e define inequivocamente quais as operações que o utilizador, através do seu dispositivo, está autorizado a exercer e as condições em que o pode fazer. Estas operações são definidas pelo fornecedor de conteúdos envolvendo aspetos relacionados com a utilização (por quem, onde e quando), nomeadamente os participantes envolvidos e as ações (ler, ouvir, executar, imprimir, outros), e as condições em que o conteúdo pode ser utilizado. Ou seja, a licença terá de conter informação correspondente ao licenciador (a parte que possui os direitos sobre o conteúdo, como, por exemplo, o autor), o licenciado (a parte a quem foram concessionados direitos, como por exemplo o aluno, a universidade, entre outros) e os termos do licenciamento (regras de concessão de direitos que asseguram a vigência das permissões/restrições e condições de uso) do conteúdo. Com este conjunto de regras torna-se possível codificar as mais variadas situações de utilização no meio educacional eacadémico, como por exemplo:

- Uma Universidade disponibiliza conteúdos de um curso a uma turma de alunos durante um mês. Após esse período, o curso continua com acesso livre apenas nos computadores da Universidade;
- Um aluno obtém um conteúdo sobre uma determinada temática à sua Universidade podendo visualizá-lo as vezes que quiser, imprimir certas partes de texto e/ou transferir o conteúdo para outro computador, mas só podendo utilizá-lo uma única vez;
- Um professor disponibiliza conteúdos para que os alunos matriculados nesse ano letivo em determinada disciplina da sua Universidade os possam visualizar. Se um aluno não matriculado na disciplina pretender visualizar esses conteúdos do curso, é-lhe solicitada uma pequena quantia monetária ou a matrícula nessa disciplina não podendo contudo imprimir, nem o usar noutro computador.

Estes exemplos mostram uma variedade de casos que, quando combinados, contribuem para uma enorme multiplicidade e complexidade de casos de utilização, que tornam a descrição de direitos de PI uma questão altamente complexa. Na tentativa de solucionar o problema, um vasto conjunto de regras estruturadas, permissões, restrições e sua combinação foram especificadas, originando o desenvolvimento de linguagens muito específicas para a expressão de direitos como a eXtensible Rights Markup Language (XRML) (Wang et al., 2002), a Open Digital Rights Language (ODRL) (http://www.w3.org/community/odrl/; Pucella & Weissman, 2006) e a MPEG-21 Rigths Expression Language (REL) (MPEG-21:REL, 2005). Independentemente das ferramentas e mecanismos de proteção utilizadas, o elemento diferenciador que dá relevância a qualquer sistema de DRM atual reside na aplicação destas

linguagens, pois os direitos aí descritos, quando corretamente interpretados e aplicados pelo sistema DRM, permitem assegurar os interesses dos participantes, assegurando a governação do conteúdo.

Consoante a complexidade da proteção do conteúdo dois possíveis cenários podem colocar-se na distribuição. No cenário mais simples o conteúdo não é protegido, mas o utilizador final terá de adquirir uma licença ou autorização do licenciador para que possa utilizar o conteúdo legalmente. No cenário mais complexo o conteúdo é protegido, e o utilizador só poderá usar o conteúdo através da aquisição de uma licença que especifica os termos e condições em que o conteúdo pode ser utilizado assegurando o respeito pelos direitos através de uma aplicação instalada no dispositivo terminal do utilizador. Ou seja, este último cenário faz-se pela incorporação de tecnologias e mecanismos de proteção. Em ambos os cenários os participantes e recursos acabam por ser os mesmos, mas a grande diferença reside na aplicação de tecnologias e mecanismos de proteção. A muito maior interatividade no cenário correspondente à proteção do conteúdo vem requerer a presença de outras funcionalidades do sistema DRM (por exemplo, autenticação e pagamentos), o que vem contribuir para aumentar a complexidade dos atuais sistemas de DRM.

3.1 Fundamentos sobre sistemas de gestão digital de direitos

Muitas abordagens têm sido concebidas para assegurar a aplicação de direitos sobre conteúdos, tendo obtido maior ou menor sucesso consoante a técnica utilizada e o contexto em que inserem (Zhang, 2013). Algumas usam técnicas bastante robustas de proteção de direitos aplicando automaticamente limites e restrições à utilização dos conteúdos, como forma de obrigar o utilizador a obedecer às condições definidas pelo detentor de direitos. Em grande parte, a eficácia de qualquer método de proteção utilizado num sistema DRM reside na capacidade de resistência do método utilizado para a ocultação da cifra que permite a proteção do conteúdo (Prihandoko, Litow & Ghodosi, 2012). Assim, uma boa gestão na distribuição destas cifras, assim como uma correta utilização das ferramentas de proteção por parte dos participantes que atuam sobre o conteúdo durante o seu ciclo de vida, pode garantir uma boa gestão da PI. Para tal, os sistemas DRM disponibilizam um conjunto de funcionalidades de proteção e também ferramentas capazes de assegurar uma boa gestão de conteúdos e de direitos de PI para estabelecer um equilíbrio balanceado de interesses dos participantes (Prihandoko et al., 2012).

Atualmente, existem diversas definições de DRM (Rosenblatt et al., 2004; Iannella, 2001; Martin et. al., 2002) não havendo contudo uma definição normalizada plenamente aceite. Uma

definição comum de DRM agrega-o a um conjunto de tecnologias que coletivamente suporta todos os estádios do ciclo de vida do conteúdo, desde a criação até ao consumo, permitindo pagamentos, prevenindo e evitando a utilização ilegal de conteúdos digitais através da proteção de direitos associados (Hwang, Yoon, Jun & Lee, 2004). O DRM também se refere a um conjunto de tecnologias de *hardware* e *software* e a serviços que controlam o uso autorizado de um determinado conteúdo e gerem, através dos direitos de utilização associados ao conteúdo, qualquer consequência dos atos de utilização durante o ciclo de vida do conteúdo (Zeng, Yu & Lin, 2011). Os sistemas DRM usam técnicas e mecanismos que fazem recurso de *software/hardware* seguro (Wu & Bao, 2008), armazenamento seguro (Snodgrass, Yao & Collberg, 2004), técnicas criptográficas (Hwang, 2008; Ku & Chi, 2004) e vários métodos de licenciamento (Iannella, 2008; Coyle, 2003; Koenen, Lacy, MacKay, & Mitchell, 2004) para prevenir a distribuição e utilização ilegal de conteúdo abrangido por direitos de PI.

São diversos os sistemas de DRM que aplicam muitos destes mecanismos e técnicas, mas do ponto de vista funcional o DRM pode ser visto sob os seguintes aspetos (Chaudhuri, 2007):

- pela identificação e descrição dos direitos de PI associados aos conteúdos e partes envolvidas na sua criação e administração;
- pela garantia da execução da aplicação (tecnológica) de condições/restrições de utilização.

Contudo, o seu objetivo não pode ser somente restringir o que o consumidor irá fazer com o conteúdo, mas dar opções de uso dentro do esperado pelo consumidor sem atentar contra os direitos dos detentores de direitos. As soluções de DRM são das mais vocacionadas para efetuar a gestão de direitos de PI sobre conteúdos pois dão a possibilidade (Abie, Spilling & Foyn, 2004);

(a) - ao fornecedor de um conteúdo de especificar os termos e condições associados aos objetos de informação digital, de os distribuir de forma adequada e de controlar a forma como são usados, com vista a assegurar a sua integridade;

(b) - aos consumidores de procurar bases de dados fornecedoras de objetos de informação digital, de fazer o *download* e consumir esses mesmos objetos e de negociar acordos especiais de utilização, seguindo as regras especificadas pelos detentores de direitos.

De um modo geral estes sistemas proporcionam (Abie, et al., 2004):

- Técnicas, processos, procedimentos e mecanismos de gestão digital de direitos e de rastreamento e monitorização do seu uso;
- Um quadro flexível de descrição e identificação de conteúdos digitais protegidos por direitos de PI, de modo a reforçar o cumprimento do conjunto de regras estabelecido pelos detentores de direitos e a proteger a privacidade dos utilizadores dos direitos;
- Infraestruturas seguras para a preparação, distribuição, armazenamento, manipulação e comunicação de objetos digitais nas fronteiras organizacionais de acordo com o nível de segurança necessário.

Para melhor entender as tecnologias e mecanismos que são utilizadas atualmente por estes sistemas, e assim enquadrar o meio académico no referente à proteção de conteúdos e direitos associados, a seção seguinte descreve os fundamentos básicos em que se suportam os atuais sistemas de DRM. No capítulo (Capítulo 3) faz-se um levantamento do estado da arte relativo aos sistemas de DRM debruçando essencialmente sobre sistemas de especificações abertas.

3.1.1 Fluxo de conteúdo e de direitos

Os conteúdos protegidos e as respetivas licenças estão normalmente associados aos identificadores dos conteúdos utilizados. No entanto, o grande problema é como o DRM pode assegurar que apenas os utilizadores legítimos podem aceder à licença, e consequentemente, aceder e utilizar o conteúdo. Isto é normalmente conseguido através da proteção do conteúdo com uma chave (ou várias chaves) (C_{EK}) que apenas é conhecida pela entidade distribuidora e a recetora. Tal pode ser realizável pela implementação de uma infraestrutura de chave-pública (PKI) (Weise, 2001) capaz de garantir a implementação de um ecossistema envolvente onde existe confiança mútua entre as partes envolvidas (Zhang, Pei, Ma & Yang, 2009). Protegendo a C_{EK} com a chave pública do utilizador ($K_{pub)}$ é possível assegurar que apenas os dispositivos autorizados e de confiança podem obter uma licença válida e, assim, ter acesso à chave do conteúdo (C_{EK}) e com isso, ao conteúdo (Figura 3). Assim, para se ter acesso ao conteúdo, o utilizador tem de possuir a chave do conteúdo correta e para ter essa chave tem de possuir a licença adequada (ou objeto licença[5] que a contenha). Podemos, assim, enunciar o princípio básico dos sistemas DRM:

Apenas o utilizador com uma licença válida pode utilizar um conteúdo específico se conseguir aceder ao mesmo (por exemplo, através de mecanismos criptográficos).

[5] A designação objeto licença e objeto de direitos será utilizada com o mesmo significado

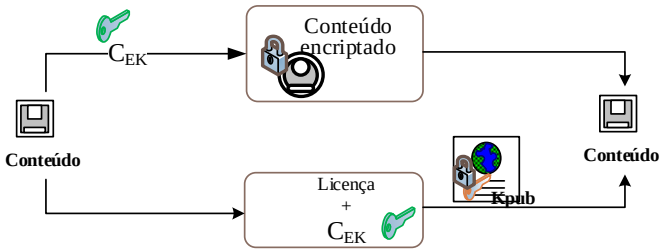


Figura 3 – A licença e o conteúdo encriptado e acesso ao conteúdo "em claro".

Por outro lado, *apenas o detentor de conteúdo ou um distribuidor autorizado pode criar uma licença válida para um dado conteúdo*. É a este princípio que se dá o nome de princípio de posse (Sans, Cuppens & Cuppens-Boulahia, 2007). Para garantir este princípio são usados mecanismos criptográficos, nomeadamente a criptografia de chave pública e as assinaturas digitais, assegurando que ninguém pode forjar uma licença aparentemente válida para um dado conteúdo.

Os sistemas DRM são desenhados com vista a gerir direitos sobre conteúdos ao longo do seu ciclo de vida aplicando técnicas e mecanismos que permitem a preservação de direitos baseados na identificação sistemática e no registo de informação acerca dos direitos e detentores de direitos associados ao conteúdo. No decorrer do ciclo de vida do conteúdo a transmissão de direitos e sua gestão não é obrigatoriamente realizada pelo autor/detentor do conteúdo. Em vez de gerir diretamente os direitos com os utilizadores finais, o detentor de conteúdo pode delegar esta tarefa a um distribuidor. Este último fica encarregue da gestão de direitos com o utilizador final ou, então, pode delegar esta função a outro distribuidor (Sans et al., 2007). Neste caso, não é o detentor de conteúdos que cria uma licença válida. Obviamente que isto não pode ser feito sem qualquer controlo das ações de todas as partes envolvidas na cadeia de distribuição. Para instituir direitos de concessão, o princípio de posse tem de ser estendido ao distribuidor autorizado. As licenças que controlam a utilização de conteúdos digitais têm de ser criadas de acordo com os direitos estabelecidos pelo seu criador quando aqueles são distribuídos (Sans et al., 2007) de forma que os direitos sucessórios sejam respeitados. Ao gerar licenças, deve existir um mecanismo de verificação para certificar que as licenças são válidas e que são criadas de acordo com os direitos e permissões instituídos pelos detentores de conteúdo ou de direitos transmitidos ao longo de toda a cadeia de valor digital (Sachan et al., 2009; Sachan & Emmanuel, 2011).

Depois de o utilizador obter a posse do conteúdo e a respetiva licença, é necessário verificar quais as operações que o utilizador está autorizado a realizar no conteúdo. Estas operações devem ser clarificadas adiantadamente por uma *aplicação* especialmente concebida para o

efeito do lado do utilizador (cliente). A tarefa de informar o cliente sobre os termos e condições de uso é realizada através do acesso a informação com as regras para a gestão de direitos, adicionada com os metadados na fase de preparação do conteúdo e realizada pelo seu fornecedor antes da entrega ao utilizador final. Esta informação e os metadados podem ser protegidos através de mecanismos criptográficos com a intenção de prevenir ou detetar a sua modificação (Kang, Kim, Park, Lee & Kil, 2006). Para definir os termos de utilização, é utilizada uma linguagem de expressão de direitos (*Rights Expression Language*-REL), com uma semântica e sintaxe apropriada (Barlas, 2006; Wang, 2005), que é incorporada na licença enviada ao utilizador (Kim, Jeong, Yoon & Ryou, 2006). A licença especifica os direitos de acesso e os direitos de utilização disponíveis para o consumidor que pretende usufruir de um determinado conteúdo (Wang, 2006). O cliente é a entidade do lado do utilizador final que executa de forma segura as operações relacionadas com a gestão de direitos, nomeadamente a interpretação das expressões de direitos inseridos na licença e assegurar a sua correta aplicação.

Num fluxo típico DRM (Abie, 2007), tal como pode ser visualizado na Figura 4, o detentor do conteúdo, em primeiro lugar, codifica o conteúdo num formato suportado pelo sistema DRM. De seguida, o conteúdo é protegido com uma chave e empacotado sendo definidas as regras de utilização para esse conteúdo. O detentor do conteúdo envia o conteúdo protegido e a chave conjuntamente com os direitos de utilização para um fornecedor e emissor de licenças, respetivamente. Quando o cliente consumidor está interessado no conteúdo, ele pode obter livremente a forma protegida do conteúdo desse fornecedor. Contudo, o consumidor não pode aceder ao conteúdo protegido até que tenha obtido a respetiva licença (ou objeto que contenha a licença) do emissor de licenças. Para obter uma licença, o consumidor deve ser elegível perante o emissor de licenças podendo posteriormente descarregar a licença para o seu dispositivo cliente. A licença pode conter informação sobre os mecanismos de proteção com os quais o consumidor pode aceder ao conteúdo. Para além disso, contém os direitos de utilização que controlam a forma como o conteúdo pode ser utilizado (Abie, 2007; Feigenbaum, Freedman, Sander & Shostack, 2002; Lee, Wu & Chang, 2007). O dispositivo cliente executa as ações introduzidas pelo utilizador e a sua confiabilidade resulta de ser reconhecido e autorizado pelas outras partes intervenientes e de não permitir acessos não autorizados ao conteúdo, assegurando a vigência de direitos sobre os conteúdos nos termos e condições especificados. Depois disso, o dispositivo usa a chave para desproteger o conteúdo, podendo o consumidor utilizá-lo, mas respeitando as regras de utilização definidas na licença.

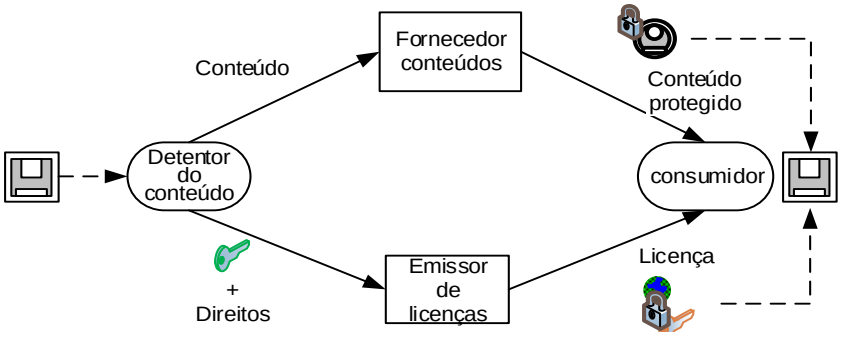


Figura 4 - Fluxo do conteúdo num sistema típico DRM

Um dos principais aspetos a considerar nos atuais sistemas DRM é a separação entre conteúdo (protegido) e direitos, o que permite que o conteúdo protegido possa ser distribuído livremente (Feigenbaum et al., 2002). No entanto, este não pode ser utilizado sem uma licença válida associada. O mesmo conteúdo pode estar associado a diferentes direitos de utilização que estipulam formas de uso diferentes, o que torna possível uma utilização flexível consoante o cenário de utilização.

3.1.2 Entidades DRM

De modo a melhor entender a forma como as várias entidades que intervêm no sistema atuam, procedeu-se a uma separação entre entidades que atuam sobre o sistema (os participantes) e outras mais tecnológicas que, inseridas no sistema DRM, disponibilizam as ferramentas e mecanismos com vista a uma proteção de direitos de PI sobre conteúdos (os componentes).

3.1.2.1 Participantes no DRM

São vários os sistemas os sistemas de DRM que têm sido propostos para a distribuição de conteúdos e licenças. Um cenário típico envolvendo duas partes pode ser considerando e envolve o autor/detentor de conteúdo e o consumidor (Lee, 2003; Camp, 2003; Cohen, 2003). Contudo, este tipo de sistemas não permite uma grande escalabilidade e são desadequados à elaboração aprofundada de estratégias de negócio (Dutta, Mukhopadhyay & Dowling, 2009). Atualmente, os sistemas de DRM envolvem múltiplas partes com múltiplos níveis de interação (Rosset, Filippin & Westphall, 2005; Zhang, Wu, Luo & Yang, 2005; Abie, 2007), resultado da separação entre conteúdos e os respetivos direitos que veio permitir aos fornecedores de conteúdos escolher variados canais de distribuição acomodando múltiplos modelos de distribuição (Morin, 2009). Visto os sistemas de DRM serem implementados de forma diferente, atualmente não existe uma norma comum de referência. Contudo, e apesar das entidades envolvidas num sistema de DRM possuírem muitas vezes nomes diferentes e

utilizarem métodos diferentes para atingirem o mesmo objetivo (Patriciu, Bica, Togan & Ghita, 2011), acabam por envolver necessariamente quase sempre os mesmos participantes: o detentor do conteúdo, o fornecedor do conteúdo, o emissor da licença, o consumidor (Liu et al., 2003) e o processador da transação (opcional). Cada um destes participantes possui papeis específicos, mas nada impede que muitas vezes exista alteração destes papeis consoante o cenário.

O detentor do conteúdo é a entidade participante que detém os direitos sobre o conteúdo sendo a parte mais interessada em proteger e assegurar que esses direitos são salvaguardados. O detentor de direitos pode ser o criador do conteúdo, ou até pode ter adquirido esses direitos ao criador. O detentor do conteúdo necessita de negociar um acordo com o fornecedor de conteúdo e o emissor de direitos com vista a estabelecer as condições de utilização do mesmo. Isto permite ao distribuidor de conteúdo disponibilizar o mesmo a mando do detentor de conteúdo usando meios para obter o devido retorno. As responsabilidades do detentor do conteúdo perante o sistema DRM passam assim por:

(a) proteger o conteúdo (utilizando criptografia);
(b) criar metadados relacionados com o conteúdo (a identificação do conteúdo, a localização da licença, e o tipo de mecanismo de proteção utilizado);
(c) enviar o conteúdo protegido ao fornecedor de conteúdos;
(d) definir as regras de acesso e utilização do conteúdo;
(e) enviar estes direitos e a chave de proteção (C_{EK}) ao emissor de direitos.

O fornecedor ou distribuidor de conteúdos é a entidade que disponibiliza conteúdo protegido aos consumidores e tipicamente é o responsável pelas seguintes funções (Subramanya & Yi, 2006):

(a) Empacotar o conteúdo protegido numa forma conveniente para consumo;
(b) Identificar de forma inequívoca o conteúdo, associando-o a um identificador único;
(c) Facilitar o envio de conteúdo, personalizando-o de acordo com as preferências do consumidor e permitindo a utilização de múltiplos formatos de forma transparente;
(d) Facilitar a comunicação entre consumidores, detentores de conteúdo, emissores de direitos e processadores das transações.

O emissor da licença é a entidade participante responsável por aplicar medidas que evitem uma má utilização do conteúdo. Tem assim por função, associar a cada uma das cópias do conteúdo uma licença (ou objeto de direitos), assim como a chave de protecção que vai permitir aceder ao conteúdo.

O consumidor é o participante que representa a pessoa que pretende adquirir um conteúdo para usufruir do mesmo no seu dispositivo. Para tal, necessita de instalar uma aplicação cliente no seu dispositivo e adquirir a respetiva licença. O consumidor pode efetuar o descarregamento deste cliente do fornecedor de conteúdos e proceder à sua instalação no dispositivo que detém (Ku & Chi, 2004). As aplicações cliente incorporam reprodutores (*players, readers, viewers*) e controladores DRM, acabando por desempenhar um papel crítico no sucesso da implementação do sistema, pois são os responsáveis por assegurar a aplicação de direitos expressos na licença (Ku & Chi, 2004). Na maioria dos sistemas DRM esta aplicação acaba por ser uma extensão dos reprodutores tradicionais através da incorporação de *software* extra, o que acaba por tornar estas aplicações componentes integrais de um sistema DRM. Através deste *software* extra o reprodutor abre e acede ao conteúdo baseado nas regras de utilização definidas na licença (Kim et al., 2006). Para obter a licença o consumidor tem de estar autenticado e ser entidade de confiança perante o emissor de licenças e satisfazer as exigências necessárias à obtenção dessa licença (Feigenbaum et al., 2002) (por exemplo ter um perfil que o enquadra dentro de domínio específico e/ou ter pago a licença). O processador da transação verifica da elegibilidade do consumidor quando contactado pelo emissor da licença. Essa elegibilidade pode envolver o pagamento de uma soma monetária por parte do consumidor e/ou a verificação de que o consumidor pertence a um domínio específico e obedece às condições especificadas na licença padrão que o detentor de direitos pré-definiu no decorrer da proteção do conteúdo. Caso esteja envolvida uma transação monetária (Figura 5), esta é a responsável por mediar a transferência financeira do consumidor para a entidade distribuidora da licença (3) e detentor de conteúdos (4). Esta entidade tanto pode estar integrada no servidor de licenças como pode aparecer numa forma independente, ficando o emissor de licenças encarregue de redirecionar o pedido do consumidor para um sistema de pagamentos de confiança capaz de executar a respetiva transação financeira (Rosenblatt et al., 2004; Michiels et al., 2005; Abbadi & Alawneh, 2008).

3.1.2.2 Componentes de DRM

Do ponto de vista da infraestrutura tecnológica o conjunto de componentes que disponibilizam aos participantes as diversas ferramentas necessárias à sua atuação no sistema DRM, possuem um papel crítico. Estas ferramentas e os componentes envolvidos suportam as atividades dos participantes no ciclo de vida do conteúdo. Estas entidades tecnológicas, ao terem de ser implementadas para darem suporte aos processos de DRM básicos, acabam por definir a arquitetura do sistema DRM. A arquitetura do sistema DRM é constituída, essencialmente, por três grandes componentes (Subramanya & Yi, 2006), (Wang et al., 2005): o Servidor de

Conteúdos (*SC*), o Servidor de Licenças (*SL*) e o dispositivo cliente (Figura 5). O SC aceita o conteúdo do detentor (o autor ou dono) e prepara-o para ser enviado para distribuição (1a). O conteúdo é então empacotado, protegido e armazenado num repositório conjuntamente com metadados, pronto para ser distribuído. A intervenção de um empacotador DRM (*SE*) prepara o conteúdo para distribuição segura (codificando o conteúdo e inserindo metadados e gerando as chaves de encriptação) antes de o transmitir ao utilizador final pelo servidor de distribuição (*SD*). O SL contém informação identificativa do conteúdo, assim como da concessão de direitos associados ao conteúdo e dos termos de utilização referentes ao exercício de direitos associados a um utilizador. Mediante o pedido do utilizador (1), se este for elegível para obtenção da licença e pagar o valor do conteúdo (2), essa informação é-lhe enviada sob a forma de licença (5) com a chave de encriptação embebida e protegida com a sua chave pública.

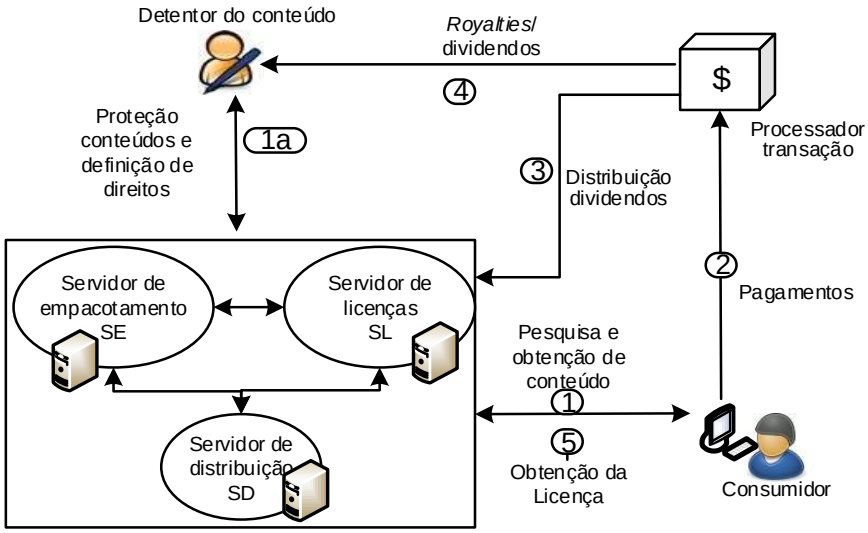


Figura 5 - Interações entre componentes e fluxos DRM

Quando a aplicação cliente residente no dispositivo do utilizador recebe o pedido do utilizador para exercer a vigência dos direitos sobre um conteúdo específico, um controlador DRM verifica se o cliente está autenticado, valida a identidade do utilizador, verifica a sua elegibilidade do utilizador e obtém uma licença de utilização do SL. De seguida recupera a chave de encriptação do conteúdo e desprotege-o, disponibilizando-o para a aplicação de reprodução (*player*) que interagindo com o controlador DRM e a licença de utilização anteriormente obtida irá assegurar que os direitos são aplicados.

Dependendo do tipo de participação perante o fluxo de conteúdo e de direitos no DRM há sempre que considerar duas vertentes: uma do lado detentor/ fornecedor de conteúdo e outra do lado consumidor:

- Vertente do detentor/fornecedor de conteúdo (Figura 6).
  - O detentor cria o conteúdo C num formato digital;
  - O detentor do conteúdo C transfere o conteúdo C para o SC;
  - O SC gera um identificador único (Id) e associa-o a C. Adicionalmente podem utilizar-se, também, tecnologias de identificação (*watermarking* e *fingerprinting*) para etiquetar e rastrear conteúdo;
  - De seguida SC protege C (por exemplo, usando uma chave secreta C_{EK} para encriptar com chave simétrica o conteúdo). SC codifica o conteúdo protegido, encripta-o, e empacota-o adicionando metadados e publica o conteúdo protegido (Cenc) empacotado (por exemplo no SD);
  - O SL coloca os dados referentes a direitos de utilização sob a forma de licença padrão. Além desses direitos, são acrescentados metadados que identificam a licença e a associam ao criador do conteúdo. Sempre que há um pedido de emissão de licença pelo utilizador é criada uma licença personalizada onde a C_{EK} é inserida, mas protegida com o recurso a criptografia de chave pública.

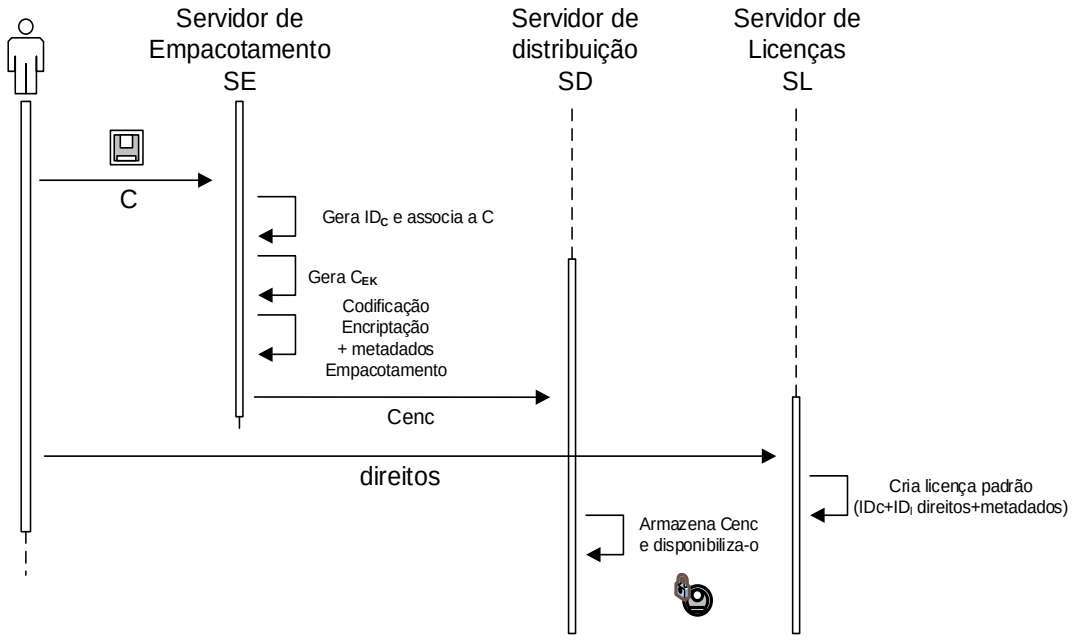


Figura 6 - Vertente detentor de direitos: fluxo de conteúdos e direitos

- Vertente do consumidor (Figura 7).
  - O consumidor instala no seu dispositivo uma aplicação cliente DRM específica e depois de pesquisar conteúdo através do SD envia um pedido para descarregar Cenc, identificado pela sua Id;

- Depois de se verificar que o dispositivo do consumidor é de confiança, o fornecedor de conteúdo autoriza o consumidor a descarregar Cenc e redireciona-o para o SL para poder obter a respetiva licença;
- O SL verifica a elegibilidade do consumidor redirecionando-o para o processador da transação de modo a concluir a verificação. Se houver transferências financeiras a efetuar entre distribuidor e detentor, estas poderão ser realizadas posteriormente;
- Quando a elegibilidade do consumidor estiver finalizada, o SL obtém a C_{EK} de SE e prepara para emissão uma licença personalizada para o consumidor, baseada nos direitos pré-estabelecidos pelo detentor do conteúdo na licença padrão (dependendo do cenário a C_{EK} poderá já ter sido enviada por SE e ter sido armazenada no SL quando a licença padrão foi criada);
- O LS cria então a licença contendo os direitos apropriados, metadados, C_{EK} encriptada e assina-a digitalmente guardando uma cópia. Depois, autoriza o consumidor a descarregar esta licença;
- Após receber a licença, a aplicação cliente DRM analisa-a, verifica a assinatura do emissor, extrai a C_{EK}, desencripta-a e utiliza-a para decifrar o conteúdo, podendo então o consumidor utilizar o conteúdo C de acordo com os direitos expressos na licença.

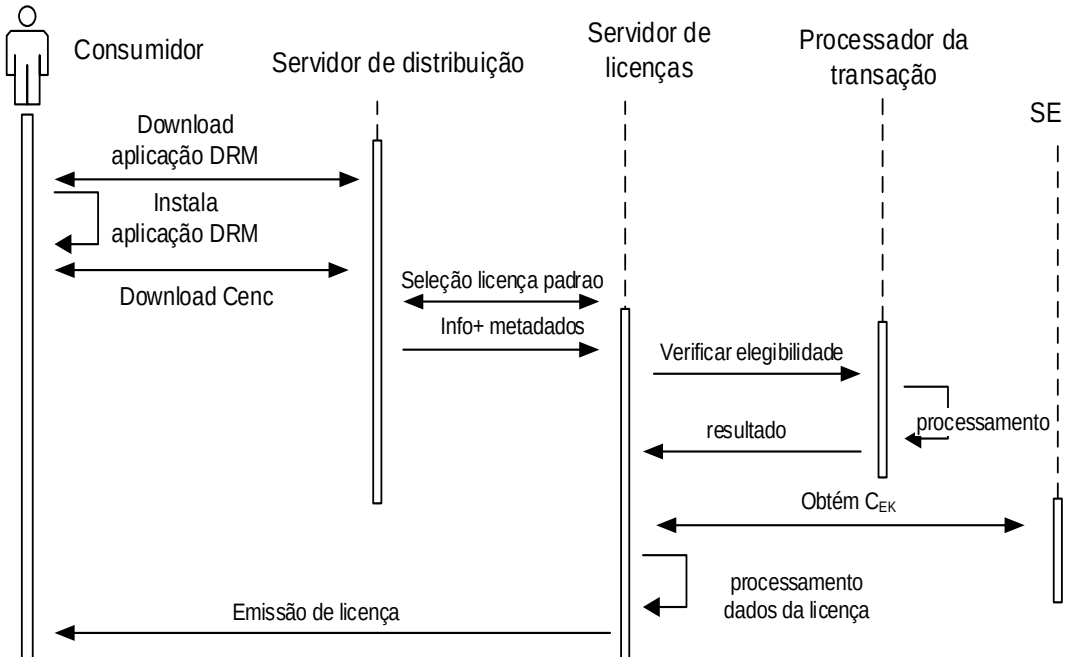


Figura 7 - Vertente consumidor: fluxo de conteúdos e direitos

Estando o conteúdo no lado do consumidor, existe a possibilidade adicional de este o distribuir a outros consumidores (por exemplo, via email). Nesse cenário, o utilizador, ao pedir para

exercer direitos, faz com que a aplicação cliente ative o controlador DRM que lê o conteúdo empacotado Cenc, obténha o Id respetivo e dados do consumidor autenticado no sistema e o redirecione para o SL. Aí poderá selecionar uma licença padrão com os direitos pré-definidos e pede para que lhe seja emitida uma licença para o conteúdo em causa. Os passos tomados a seguir são praticamente idênticos aos que foram descritos anteriormente na geração da licença.

4 Perspetiva estrutural do DRM

Tendo em conta as interações entre os participantes, componentes e suas funções, serviços e atividades, do ponto de vista estrutural pode-se apresentar o DRM sob várias vertentes: a funcional, a arquitetónica, por serviços e por camadas. De seguida proceder-se-á à análise de cada uma destas perspetivas.

4.1 DRM: estrutura funcional

A gestão de conteúdos e de direitos num sistema DRM implica, em termos genéricos, a definição do acesso ao conteúdo, aos metadados e a especificação de direitos associados assim como das transações (a atribuição do licenciamento às partes que possuem direitos e respetivos dividendos). Para que estas atividades se realizem, o sistema DRM disponibiliza um conjunto de funcionalidades (Llorente., Rodríguez, Delgado & Torres-Padrosa, 2013) às várias entidades que intervêm no sistema. As principais funções disponibilizadas pelo sistema cobrem essencialmente três áreas: a gestão de direitos, a gestão da utilização e a gestão do conteúdo (Diehl, 2008). A gestão de direitos define as restrições/permissões, as concessões e condições associadas ao conteúdo. A gestão de utilização assegura a aplicação das condições definidas pelo fornecedor enquanto a gestão do conteúdo lida com o conteúdo em si mesmo. Uma arquitetura funcional pode ser modelada em três áreas funcionais (Iannella, 2001; Rump, 2003; Zhang, 2013), correspondentes aos três patamares do ciclo de vida do conteúdo: a criação, a gestão/distribuição e a utilização (Figura 8).

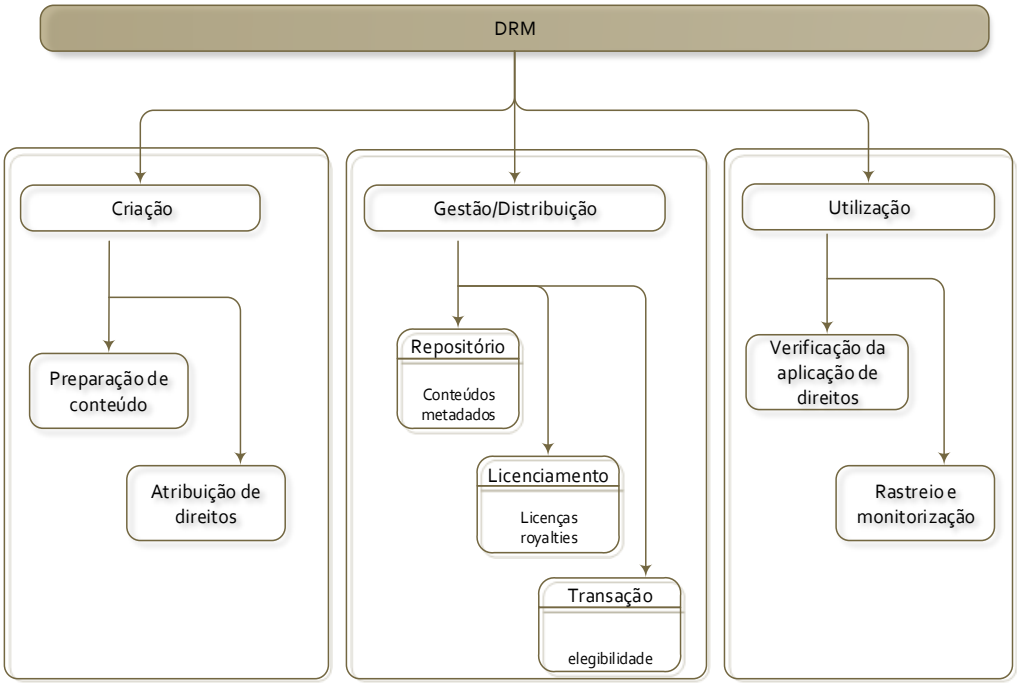


Figura 8 - Arquitetura funcional do DRM (adaptado de Iannella, 2001)

Estes três patamares, ou blocos, cobrem no seu conjunto a ação de todas as entidades (participantes e componentes) que intervêm num sistema de DRM, sendo capaz de fornecer uma solução de gestão de direitos completa, de início ao fim do ciclo de vida do conteúdo, estipulando o papel e comportamento dos vários módulos que cooperam e interoperam no sistema. De seguida faz-se uma breve descrição de cada um dos blocos (Iannella, 2001).

a) Criação e gestão do conteúdo

O primeiro bloco da arquitetura funcional do DRM tem em vista facilitar a criação de bens digitais. Tal inclui a definição e atribuição de direitos através de expressões específicas. A atribuição de autoria e a preparação do conteúdo para publicação são as principais características, não sendo necessário que os metadados sobre direitos estejam incorporados no conteúdo protegido devendo, contudo, ser facilmente acessíveis caso sejam requeridos. Duas funcionalidades devem ser tomadas em linha de conta:

- Criação de direitos e validação – a definição e atribuição de direitos sobre o conteúdo e a certeza de que os estes são consistentes com o modelo de negócio são aspetos fundamentais;
- A gestão de conteúdos e de direitos – a geração e gestão da(s) chave(s) de proteção do conteúdo e a preparação do conteúdo protegido resultante e da licença a emitir;

O conteúdo deve ser protegido e empacotado através da seleção das ferramentas apropriadas de modo a suportar a estratégia escolhida que assegure a correta aplicação dos direitos. Se for escolhida uma estratégia em que todas as aplicações têm de ser confiança, então o conteúdo deve ser protegido de modo a que somente uma aplicação de confiança consiga aceder ao mesmo (por exemplo através da desencriptação). Estas medidas de proteção deverão também estar presentes no bloco de distribuição da arquitetura. Esta situação coloca-se sempre que o conteúdo necessita de ser protegido de forma personalizada para cada utilizador final.

b) Gestão e distribuição do conteúdo

Para efetuar uma gestão capaz dos conteúdos e dos direitos associados recorre-se à utilização de técnicas criptográficas e ao controlo quer dos serviços disponibilizados pelo lado servidor quer do lado cliente. O bloco correspondente à gestão e distribuição, funcionalmente, deve aceitar o conteúdo do detentor e de acordo com os direitos especificados distribuí-lo aos utilizadores finais. Duas fases podem aqui ser identificadas: a distribuição de conteúdo e a distribuição de direitos. A oferta (catalogação e publicação) e a expedição (pesquisa, aquisição, envio) são processos que distinguem cada uma destas fases. Para atingir estas duas fases as seguintes funcionalidades devem ser disponibilizadas:

- Funções de licenciamento incluindo os pedidos de licenças de utilização. Os pedidos são verificados tendo em linha de conta os direitos especificados. Sendo o pedido válido, a licença é emitida e os dividendos distribuídos;
- Funções de repositório incluindo a aceitação de conteúdos dos criadores e permitindo o acesso a utilizadores finais, podendo os metadados ser manuseados separadamente do conteúdo;
- Funções de transação incluindo a verificação da conformidade do utilizador com o modelo de negócio. Para conteúdos comerciais um sistema de comércio eletrónico pode atuar como intermediário entre o utilizador final e o sistema de licenciamento, promovendo assim o uso de conteúdos e administrando os seus pagamentos. Para conteúdos educacionais, e de acordo com a nossa proposta a apresentar, esta função pode ser realizada pela plataforma/sistema de gestão de atividades académicas. Assim torna-se possível verificar e validar a elegíbilidade para obter a licença.

c) Utilização do conteúdo

O último bloco da arquitetura funcional DRM gere a utilização/consumo do bem digital. Independentemente da funcionalidade de procura de conteúdo ter de existir neste bloco, a partir

do instante em que este for transacionado, duas funcionalidades devem ser consideradas (Iannella, 2001;Arnab & Hutchinson, 2005):

- Funções que garantem que os direitos são aplicados e que asseguram a sua conformidade com o especificado nas licenças entretanto obtidas. A implementação de uma aplicação de confiança no lado cliente assegura a utilização do conteúdo de acordo com as regras especificadas, podendo bloquear utilizações indevidas;
- Funções de rastreio e monitorização do conteúdo para prevenir e desencorajar o uso ilícito de conteúdos através de relatórios de utilização de conteúdo (número de utilizações, pagamentos por uso, outros).

Uma característica comum nos sistemas DRM, que é facilmente percetível no seu desenho, é a divisão estrutural em duas áreas. De um lado a área do fornecedor, e do outro a área do utilizador. Uma outra característica comum reside na separação da área do fornecedor em duas subáreas: a do servidor de conteúdo e a do servidor de licenças. Tal é devido à utilização de dois canais distintos de distribuição. Um dos canais é usado para distribuir conteúdo protegido e o outro para distribuir licenças. Essa mesma separação pode ser entendida se considerarmos os seguintes elementos funcionais para a proteção de conteúdos (Mampaey & Villegas, 2012) (Figura 9):

- Chaves de proteção de conteúdo (*keys*) - são as chaves usadas para proteger o conteúdo (que podem ser criptografia) e também requeridas do lado do utilizador para desencriptar e aceder ao conteúdo. A chave de desencriptação do conteúdo é protegida de forma individualizada e enviada conjuntamente com as regras de utilização empacotadas na licença;
- Empacotador (*packager*) – este elemento é o responsável pela encriptação do conteúdo com a chave de encriptação, pela formatação dos dados num pacote que obedeça preferencialmente aos formatos internacionais e por associar o conteúdo a chaves e regras de utilização;
- Servidor de licenças (*License server*) - este é o elemento que colige a informação necessária ao processo de decisão de emissão de licenças, podendo incorporar funções de encriptação;
- Agente DRM (*secure agent*) - este elemento reside no dispositivo do utilizador e é responsável pela verificação da identidade dos utilizadores, integridade do dispositivo assim como por pedir, obter e desencriptar as licenças, fazendo assegurar a aplicação das regras nelas expressas;

- Dispositivo do utilizador – esta é a entidade que realiza a decifragem do conteúdo usando a chave enviada pelo agente DRM no decorrer do processo de concessão da licença. As funções de desencriptação e gestão das chaves poderão ser parcialmente implementadas num componente de *hardware* considerado seguro.

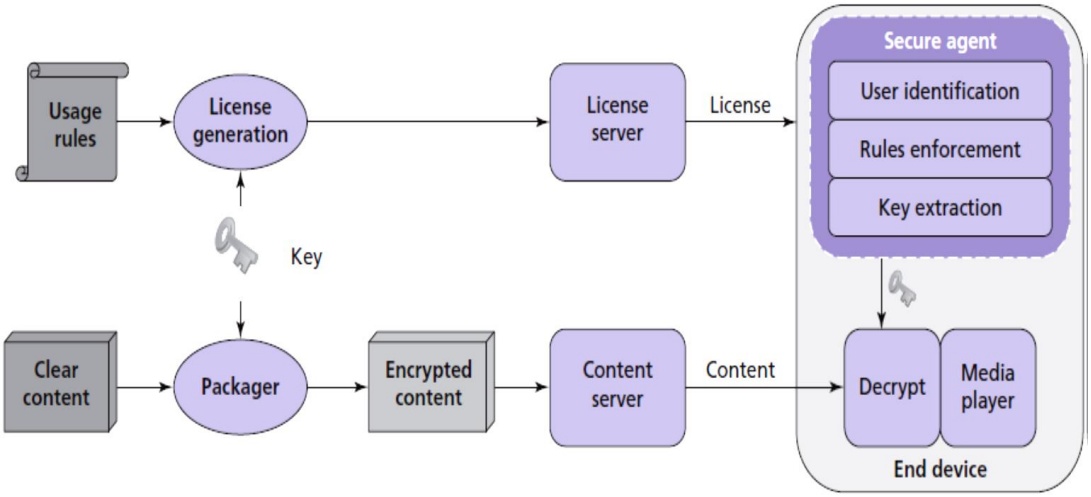


Figura 9 - Elementos funcionais para a proteção de conteúdo (Mampaey & Villegas, 2012)

Neste esquema (Figura 9), é percetível a existência dos dois canais de distribuição, diferenciadores das duas cadeias de informação encriptadas. Uma está relacionada com a cadeia de componentes do conteúdo, outra com a cadeia de chaves de proteção. Esta diferença permite estabelecer diferentes níveis de proteção que fazem com que os sistemas DRM tenham de implementar no fornecedor de conteúdos, no dispositivo dos utilizadores e no canal de comunicação mecanismos e técnicas de proteção de conteúdos e direitos associados (Mampaey & Villegas, 2012).

4.1.1 DRM e ferramentas tecnológicas

Os sistemas DRM, ao incorporarem um variado conjunto de componentes estruturais que disponibilizam aos participantes as funcionalidades necessárias de suporte aos serviços característicos deste tipo de sistemas, permitem a realização de um vasto conjunto de atividades altamente complexas que se influenciam mutuamente (Michiels et al., 2005). O objetivo destes componentes é fornecer as ferramentas necessárias aos participantes para que estes possam ter um ambiente controlado na distribuição e consumo de conteúdos, com o suporte aos direitos de PI. Numa perspetiva de segurança, o conjunto de ferramentas tecnológicas e mecanismos utilizados têm em vista assegurar a confidencialidade, a integridade e disponibilidade do conteúdo na sua distribuição, reprodução e utilização. Convencionalmente, os mecanismos de proteção de conteúdos são orientados para a proteção de direitos, proteção de cópia e controle

de acesso. Mas um sistema de DRM vai além disso e procura ser mais abrangente acabando por realizar mais e diferentes tarefas durante o ciclo de vida do conteúdo. Da análise da literatura (Michiels et al., 2005; Iannella, 2001; Rosenblat & Dykstra, 2003) é possível dizer que as tarefas mais importantes que as ferramentas e mecanismos de proteção devem oferecer são:

- Proteção de conteúdo;
- Monitorização da utilização;
- Rastreio da distribuição;
- Controlo de acesso e de utilização;
- Distribuição segura de conteúdo e chaves de acesso;
- Autenticação da fonte do conteúdo e recetor(es);
- Associação de direitos a conteúdos e utilizadores;
- Renovação do sistema de proteção.

Para que estas tarefas sejam concretizáveis, torna-se necessário a disponibilização de várias técnicas e ferramentas tecnológicas pelos vários componentes do sistema DRM. As mais importantes são de seguida descritas:

1. **Identificação/registo do conteúdo:** Com o objetivo de gerir e proteger a PI, é essencial haver um sistema adequado de identificação e descrição do conteúdo disponível (por exemplo, através de metadados). A identificação é um aspeto central no DRM a considerar pois permite a indexação e reconhecimento do conteúdo (Ku & Chi, 2004). Antes dos direitos sobre o conteúdo serem definidos, este tem de ser identificado sem ambiguidades de modo a que os utilizadores possam adquirir sem engano os direitos de utilização do mesmo. Os metadados relativos ao conteúdo poderão aqui fornecer alguma informação descritiva de ajuda (tipo de ficheiro, tamanho, entre outros), podendo fornecer dados de como se pode fazer uso do sistema de identificação (Ku & Chi, 2004). Contudo, não substituem o sistema de identificação e registo. Estes identificadores são essencialmente utilizados para (a) identificar única e inequivocamente o conteúdo e (b) associar o conteúdo aos metadados que o descrevem (Paskin, 2003). Além de identificar o conteúdo, também podem ser usados na localização de derivações do conteúdo ou conteúdos relacionados (Ku & Chi, 2004). De seguida apresentam-se os principais sistemas *standard* de identificação atuais (Tabela 3).

Sistema de identificação	*Standard*	Âmbito e grupo de trabalho
ISBN - ISO 2108:1992 (ISBN)	ISO 2108:2007 NISO Z39.84-2005 (R2010)	· Livros, *software*, vários media, · The International ISBN Agency.
DOI - Digital Object Identifier (DOI)	ISO 26324:2012	· Qualquer entidade de PI, · International DOI foundation (IDF).
ISAN – International Standard Audiovisual number (ISAN)	ISO 15706.2:2007	· Conteúdos audiovisuais, · ISO/TC 46/SC 9 WG1
MPEG-21 DII (MPEG-21:DII, 2005)	ISO/IEC 21000/3:2005	· Conteúdos digitais, · ISO/IEC JTC1/SC 29 WG11.
ISWC – International Standard Musical Work code (ISWC)	ISO 15707:2001	· Composições musicais, · The International ISWC Agency, · International confederation of Societies of Authors and composers
ISSN - International Standard Serial Number (ISSN)	ISO 3297:1998	· Publicações de séries, · ISSN International Centre.

Tabela 3 – Sistemas e *standards* de identificação/registo de conteúdos

Os metadados complementam a utilização de identificadores de conteúdo podendo indicar a forma de aceder ao conteúdo e até mesmo especificar as regras de utilização (Ku & Chi, 2004). Um exemplo de um esquema de metadados com enorme aceitação na comunidade académica é o Dublin Core (DCMI, 2013a), que fornece um conjunto normalizado de convenções para a descrição de conteúdos que facilitam a sua procura e descrição. Na sua forma mais básica contém 15 elementos não obrigatórios e que se podem repetir (por exemplo: *creator*, *date*, *description*, entre outros) (DCMI, 2013b).

2. **Medidas de segurança e ferramentas de proteção de PI:** o sistema DRM, ao requerer que a proteção de conteúdo seja persistente, recorre a um variado conjunto de medidas tecnológicas de proteção, de forma a controlar acessos e usos não autorizados (Marques & Serrão, 2012b). Tal pode envolver a codificação dos termos e condições sobre os quais o conteúdo pode ser utilizado, embebendo-os num ficheiro e permitindo a utilização desse conteúdo segundo as condições definidas, até à utilização de técnicas de computação segura (*trusted computing*) (Yan & Peng, 2011; TCG, 2011a; Cooper & Martin, 2006; Felten, 2003b) que asseguram a integridade da execução do código no dispositivo de

reprodução. A computação segura é uma tecnologia chave que determina a segurança global do sistema DRM. Com a utilização de técnicas como a "*remote attestation*" torna-se possível confirmar se o dispositivo está corrompido (Huang & Peng, 2009; Guang-yuan & Bei, 2013). Ao atuar como uma espécie de "*blackbox"* esconde as operações em execução e caso haja alguma alteração no seu processamento termina-as (Kang et al., 2006). Assim, é possível assegurar que quer o conteúdo desprotegido, quer as chaves de proteção (de encriptação) não serão expostas durante o processamento ou na utilização do conteúdo (Stumpf, Tafreschi, Röder, & Eckert, 2006; Francillon, Nguyen, Rasmussen & Tsudik, 2014). Apesar dos esforços, contudo, a sua eficácia ainda está por comprovar, já que a implementação deste tipo de tecnologia tem tido muitos contratempos (Castelluccia, Francillon, Perito, & Soriente, 2009; Stamp, 2002a; Wu & Bao, 2008; Oppliger & Rytz, 2005).

Independentemente da tecnologia aplicada, a mais generalizada de todas as técnicas usadas na proteção (quer do conteúdo quer da licença) faz recurso à criptografia, tanto de chave simétrica, como de chave assimétrica, tornando-a o núcleo das medidas aplicadas no sistema DRM e onde as outras técnicas se ancoram para garantir uma proteção eficaz. Também as assinaturas digitais permitem o não repúdio da emissão de direitos, atuando como meio de prova de direitos adquiridos e quando combinada com técnicas de resumo permitem a verificação da integridade quer do conteúdo quer da licença (Ku & Chi, 2004).

A criptografia, ao lidar com as questões relacionadas com a segurança, permite assegurar a confidencialidade, autenticidade e integridade necessárias à proteção do conteúdo e direitos associados quando este é transmitido através de canais públicos. Os contentores seguros são aqui utilizados para garantir que o conteúdo digital é somente acessível a consumidores autorizados (aqueles que possuem as credenciais corretas e obedecem às condições para as quais a licença tenha sido emitida) (Ku & Chi, 2004). Estes contentores podem ser conseguidos usando técnicas criptográficas (por exemplo, usando o AES) (Alanazi et al. 2010; AES, 2001) e quando utilizados em conjunto com criptografia de chave pública, assinaturas digitais e o uso de certificados digitais fornecem a confidencialidade e integridade necessárias à segurança básica de um sistema DRM (Ku & Chi, 2004). Os certificados digitais, englobados numa infraestrutura PKI, são aqui usados para a autenticação e verificação da identidade das partes envolvidas no sistema DRM. É essencial usar este mecanismo para acautelar que os componentes são legítimos e de

confiança e assim atestar que o conteúdo protegido disponibilizado tem uma proveniência legítima.

Outras técnicas como o *watermarking* (Nasereddin, 2011; Cox, Miller, Bloom, Fridrich & Kalker, 2007), *fingerprinting* ou *hashing* são usadas para embeber informação sobre o conteúdo, possibilitando a sua identificação e assim facilitar o seu rastreio, verificar a sua integridade ou personalizar uma instância do conteúdo em particular (Ku & Chi, 2004). O *watermarking* contribui para a preservação de direitos na medida em que permite associar um conteúdo ao respetivo detentor mesmo após a sua transmissão (Thomas, Emmanuel, Das & Kankanhalli, 2009; Piva, Bartolini & Barni, 2002; Dukhi, 2011). Como o *watermark* permanece associado ao conteúdo, então pode ser detetado de modo a rastrear qualquer ação indevida sobre o mesmo. Mesmo que seja removido pode-se utilizar o *fingerprinting* complementarmente como técnica para dar assistência como meio de prova (Ku & Chi, 2004; Gayathri, Thomas, & Jayasudha, 2012). Assim, a associação destas técnicas com técnicas criptográficas vem fornecer a eficácia requerida para a segurança da transmissão e proteção do conteúdo.

O grau de controlo sobre o acesso e uso do conteúdo é assim uma complexa matriz sendo a sua eficácia tanto maior quanto mais restritivas forem as medidas aplicadas (Marques & Serrão, 2012b), aumentando a sua força com o grau de robustez da função protetora da tecnologia (Unlu & Hess, 2005).

3. **Expressão de direitos**: para expressar os direitos associados aos conteúdos digitais são usadas linguagens de expressão de direitos. Estas expressões apresentam-se sob a forma de licenças num formato percetível pelos sistemas computacionais. A licença é o meio pelo qual se especificam os direitos acordados com o licenciado, os quais são normalmente expressos através de uma REL (Ku & Chi, 2004; Jamkhedkar & Heileman, 2009b), indicando as regras de utilização do conteúdo. Estas regras formam a base de suporte em que assenta um contrato entre o recetor (por exemplo, o utilizador final) e o emissor de direitos (normalmente o detentor do conteúdo) relativamente à forma como o conteúdo poderá ser utilizado e é constituída por dois componentes: a linguagem de direitos (sintaxe) e o dicionário de dados sobre direitos (semântica) (Ku & Chi, 2004). O primeiro refere-se às regras gramaticais e o segundo à ontologia que fornece significados aos termos usados nas regras gramaticais. Geralmente, a sintaxe de grande parte das REL é constituída por direitos (tipo de ações admitidas na utilização de um recurso incluindo as restrições de utilização, como por exemplo, limitação do tempo de utilização ou número de vezes que

se pode utilizar), condições (pré-requisitos a serem observados antes dos direitos poderem ser exercidos), o recurso (o conteúdo em questão onde serão exercidas as ações; deve ser identificado de forma inequívoca e não ambígua) e as entidades (as partes envolvidas no exercício dos direitos; Ku & Chi, 2004). Assim, em DRM, só há utilidade em recorrer a uma REL desde que se queira assegurar a correta aplicação dos direitos (Barlas C., 2006). Atualmente, existem em utilização vários tipos de RELs desenvolvidas quer por organizações de normalização quer por iniciativas independentes, não havendo, contudo, um formato uniforme (Jamkhedkar & Heileman, 2008). Todas estas linguagens são tipicamente baseadas numa especificação *standard* (Barlas, 2006): o XML. Pela sua aceitação e importância, são de realçar as seguintes REL: ODRL, MPEG-21 REL (MPEG-21:REL, 2005), e DRM-REL (OMA, 2011c). Visto as RELs serem a linguagem de comunicação de direitos nos sistemas DRM, o seu desenho, poder de expressão, limitações e outros atributos acabam por influenciar fortemente a estrutura e propriedades dos sistemas DRM (Jamkhedkar & Heileman, 2009b).

4. **Identificação/Autenticação de utilizadores:** Todas as entidades envolvidas num sistema DRM necessitam de estar identificadas de um modo único de modo a possibilitar a associação do conteúdo aos seus utilizadores e garantir que somente utilizadores legítimos podem aceder a esse conteúdo (Ku & Chi, 2004). Para suportar acessos autorizados, o DRM tem de utilizar mecanismos que permitam a identificação e gestão dos utilizadores que solicitam o acesso ao conteúdo. O sistema DRM verifica a realidade e validade da identidade dos utilizadores antes de os autorizar. Normalmente esses mecanismos recorrem a sistema de autenticação *Single Sign-On* (SSO) baseandos em login/password, sendo atribuído ao utilizador uma identificação (UserID) única no sistema (Ku & Chi, 2004). Para suportar acessos autorizados e garantir confiança entre as partes envolvidas, são utilizados métodos de autenticação baseados em criptografia onde uma terceira entidade de confiança (Autoridade Certificadora - AC) emite certificados que credenciam as entidades envolvidas podendo estas então autenticar-se mutuamente (Serrão, Serra, Dias & Delgado, 2007; Patriciu et al., 2011). Pode-se dar o exemplo de utilização de certificados quando:
    - O emissor das licenças tem de autenticar o cliente DRM do consumidor antes de emitir uma licença,
    - Um canal seguro e autenticado é estabelecido entre cada um dos pares de entidades intervenientes no DRM.

A AC, ao emitir certificados para todos os participantes e componentes permite criar uma rede de confiança entre as partes envolvidas garantindo a identificação desses intervenientes e reconhecendo-lhes a capacidade de atuar no sistema (Patriciu et al., 2011). A infraestrutura de PKI é assim de primordial importância no estabelecimento desta confiança, oferecendo um variado conjunto de serviços úteis aos sistemas de DRM, capazes de criar as condições adequadas. Estes serviços resumem-se a (Serrão et al., 2007; Serrão, 2008):

- Serviços de autenticação: a autenticação é necessária para assegurar que uma entidade é inequivocamente quem clama ser. Pode ser utilizada para garantir a identificação das entidades e a identificação da genuinidade/autenticidade dos dados.
- Serviços de integridade: estes serviços permitem garantir que os dados não foram alterados, além de permitir saber se e quando esses dados foram alterados.
- Serviços de confidencialidade: estes serviços permitem que os dados sejam somente acedidos pela entidade legítima a quem foram endereçados.

5. **Relato de eventos**: A existência de mecanismos que reportem o acontecimento de eventos no sistema pode ser necessária não só em situações que envolvam comprovativos de movimentos financeiros ao utilizar conteúdos (por exemplo, *pay-per-view*), mas também em situações em que aconteçam violações de direitos (Ku & Chi, 2004). Estes mecanismos, além de poderem ser utilizados na ajuda à coleção e distribuição de dividendos, também podem ser usados como ajuda na prova de aquisição de direitos sobre um determinado conteúdo (Rodríguez & Delgado, 2007b).

6. **Dispositivo do utilizador:** (muitas vezes referido como o cliente DRM ou dispositivo do consumidor) é a unidade de confiança no sistema DRM capaz de assegurar a aplicação de direitos sobre o conteúdo (Rosenblatt et al., 2004), quando devidamente credenciado. Este dispositivo executa a decifragem do conteúdo protegido no momento da sua utilização ao mesmo tempo que executa a aplicação de direitos. Para tal recorre a uma aplicação específica desenhada para o efeito que também assiste o utilizador a adquirir direitos sob a forma de licenças. Esta aplicação é essencialmente constituída por um reprodutor (*player*) e um controlador de DRM que asseguram a correta utilização do conteúdo face aos direitos expressos na respetiva licença de utilização (Ku & Chi, 2004; Rosenblatt et al., 2004). Em termos de segurança global do sistema, esta aplicação é um dos elementos cruciais, capaz de garantir que o conteúdo é acedido por utilizadores legítimos e consumido de acordo com as regras definidas na licença. Deve assim garantir a correta proteção das chaves de

encriptação, impossibilitar a utilização de técnicas de engenharia reversa e ser capaz de resistir a manipulações de modo a garantir a autenticidade, integridade e confiança na aplicação (Stumpf et al., 2006; Francillon et al., 2014). Além disso, deve ser capaz de detetar conteúdos e licenças ilegais e recusar a reprodução desses conteúdos, assim como reportar e assistir no seu rastreio (Ku & Chi, 2004). Para assegurar a aplicação efetiva dos direitos o dispositivo poderá incorporar módulos de software/hardware *Trusted Platform Modules* (TPM) (Sadeghi, 2008; Yan & Peng, 2011) resistente a falsificações, em conformidade com as normas do *Trusted Computing Group* (TCG) (TCG, 2011a; TCG, 2011b; TCG, 2011c) capazes de fornecer um grau eficaz de segurança (Ateniese, Fu, Green & Hohenberger, 2005). As normas Technological Protection Measures (TMP) adotadas pela organização ISO/IEC (ISO/IEC 11889-1:2009; ISO/IEC 11889-2:2009; ISO/IEC 11889-3:2009; ISO/IEC 11889-4:2009) permitem desenhar o dispositivo em conformidade com um nível de segurança elevado, fornecendo ao cliente DRM as principais funcionalidades básicas requeridas, como a "atestação" das aplicações e o armazenamento seguro de conteúdo e chaves (Abbadi & Alawneh, 2008).

7. **Sistema de pagamentos**: São usados para possibilitar as transações financeiras entre o consumidor e o emissor de licenças (Ku & Chi, 2004). Normalmente recorre-se a uma entidade bancária de confiança entre as partes, que garanta a segurança da transação e a distribuição de pagamentos (Rosenblatt et al., 2004; Michiels et al., 2005).

4.2 DRM: arquitetura

Do ponto de vista arquitetónico, os modelos DRM descrevem os diferentes elementos da arquitetura e as suas interações (Michiels et al., 2005). Essencialmente lidam com os servidores, serviços e agentes identificando os serviços e as entidades que fornecem esses serviços (Diehl, 2008). O desenho estrutural de qualquer arquitetura DRM está orientado para ir ao encontro de três objetivos: assegurar o retorno (financeiro ou não) proveniente da distribuição do conteúdo, assegurar a distribuição segura desses conteúdos e assegurar que os direitos das partes envolvidas são protegidos (Amit, 2012). A grande maioria dos sistemas de DRM propõem-se a satisfazer estes objetivos, podendo o seu desenho ser visto como uma variante da arquitetura típica DRM (Rosenblatt et al., 2004; Erickson, 2003; Schmidt, Tafreschi & Wolf, 2004) (Figura 10). Conceptualmente é composta por três grandes componentes: o servidor de conteúdos, o servidor de licenças e o dispositivo do utilizador também conhecido por cliente DRM (Rosenblatt et al., 2004; Stefik, 1997; Ridzon, 2009).

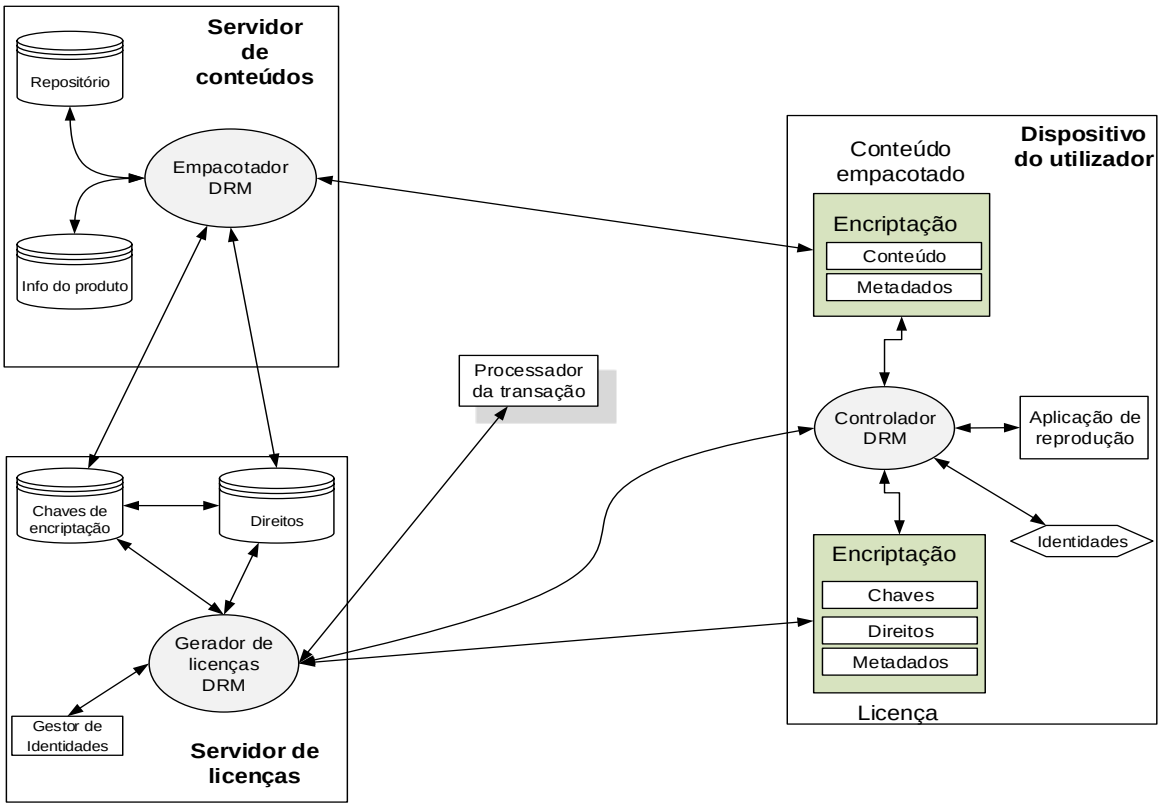


Figura 10 – Arquitetura típica DRM (adaptado de Rosenblatt, et al., 2004)

O servidor de conteúdos é o componente responsável por preparar e disponibilizar conteúdo protegido e consiste no conteúdo armazenado (repositório), informação acerca do conteúdo que se pretende distribuir e ferramentas que permitem disponibilizar as funcionalidades de preparação do conteúdo para distribuição (*empacotador*) (Rosenblatt et al., 2004; Ridzon, 2009).

O servidor de licenças é o componente responsável pela gestão da informação sobre licenciamento. As licenças contêm a informação acerca do conteúdo ou dispositivo, direitos e identidade do utilizador que pretende exercer direitos sobre o conteúdo. Além disso, a informação sobre as chaves de proteção do conteúdo podem estar aí armazenadas, sendo estas emitidas para o utilizador numa licença criada pelo gerador de licenças (Hwang, 2009; Rosenblatt et al., 2004; Ridzon, 2009).

O cliente DRM permite o acesso e a utilização controlada do conteúdo e para tal fornece os seguintes subcomponentes: controlador DRM, aplicação de reprodução e os mecanismos de verificação da autenticação do utilizador (Rosenblatt et al., 2004). O controlador é o componente responsável pela extração do conteúdo e metadados associados e pela interpretação e garantia de aplicação de direitos de acesso e de utilização. O cliente DRM é o único componente do lado do utilizador a quem é permitido desproteger o conteúdo encriptado, não

devendo expor este conteúdo desprotegido a outro *software*/*hardware* que não seja de confiança (Wu & Bao, 2008; Michiels et al., 2005). As suas maiores responsabilidades passam por: a) receber os pedidos para exercer direitos sobre o conteúdo protegido, b) recolher informação sobre a identidade do utilizador e verificar a sua elegibilidade para aquisição de uma licença, c) autenticar a aplicação que executa o exercício de direitos e d) recuperar as chaves de encriptação da licença e decifrar o conteúdo, disponibilizando-o para a aplicação de reprodução, executando operações sobre o conteúdo de acordo com direitos especificados na licença (Rosenblatt et al., 2004).

4.2.1 DRM: estrutura por camadas

Uma possível forma de estruturar o DRM pode ser através do modelo por camadas, o qual é compatível com o modelo de referência OSI (Jamkhedkar & Heileman, 2004). O seu objetivo é simplificar a estrutura altamente complexa em várias camadas de abstração simples. A grande vantagem da arquitetura por camadas reside na independência de cada camada que vai permitir desenhar o sistema em partes autónomas, ou módulos e assim ajudar a estabelecer uma maior *interoperabilidade* entre diferentes sistemas DRM (Amit, 2012). A contribuição deste tipo de modelo reside na abstração das funcionalidades proporcionadas num modo semelhante ao modelo de referência OSI (Miller, 2001), independentemente do tipo de conteúdo e lógica de negócio. Numa perspetiva de segurança podem ser estruturadas num modelo genérico de quatro a cinco camadas.

O modelo proposto em (Jamkhedkar & Heileman, 2009a) consiste de 5 camadas: camada aplicacional, camada negocial, camada de expressão de direitos, camada superior de aplicação de direitos e camada inferior de expressão de direitos. Uma outra proposta de modelo em quatro camadas (Diehl, 2008) descreve o comportamento de um sistema DRM através das suas principais características de segurança: gestão da confiança, gestão de direitos, aplicação de direitos e proteção de conteúdo. A Figura 11 mostra as interações entre estas quatro camadas e o lado do servidor e o lado cliente. A primeira camada nesta representação hierárquica é a gestão da confiança, a qual serve todas as três camadas inferiores assegurando que somente as entidades de confiança interatuam. O sistema deve poder negar ou fornecer aos participantes "não de confiança" serviços de interação muito limitados, para que estes possam vir a registar-se futuramente.

Nas atuais implementações de código aberto a forma mais comum de proporcionar confiança entre os intervenientes é através de mecanismos de autenticação que podem recorrer à utilização

de certificados digitais (Serrão, 2008; Patriciu et al., 2011). A autoridade certificadora (AC) emite certificados digitais para todos os componentes do sistema DRM que estejam em conformidade. Adicionalmente o certificado até pode conter declarações de capacidades, ou requisitos do seu possuidor. Por outras palavras, é através dos certificados digitais que a entidade emissora AC pode reconhecer que um detentor certificado está autorizado a executar um variado conjunto de funcionalidades e, estando autenticado, fica dotado de certas capacidades perante o sistema (Patriciu et al., 2011; Abbadi & Alawneh, 2008).

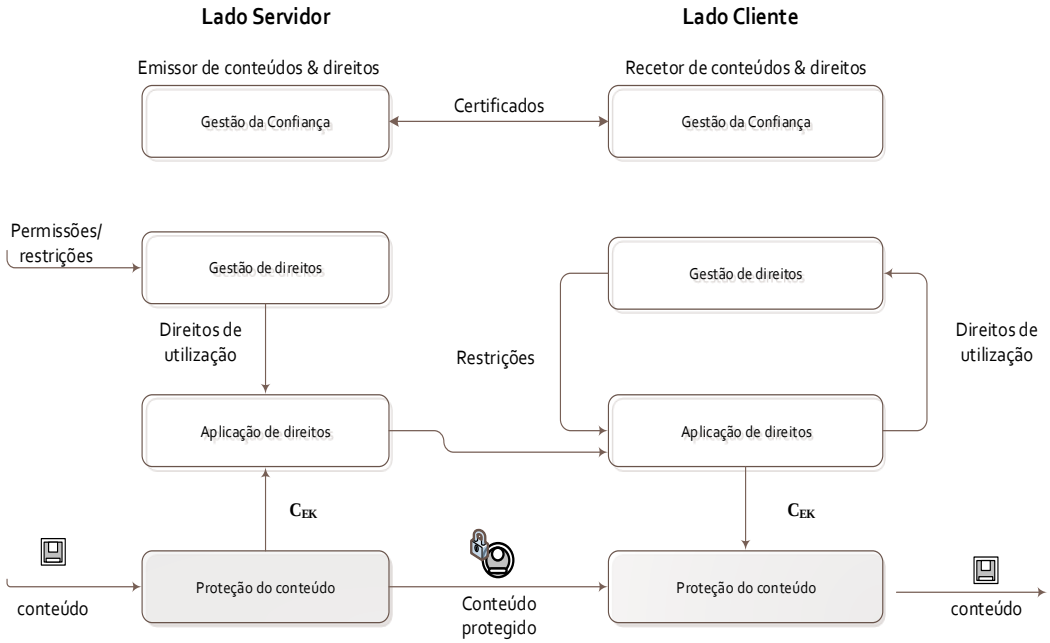


Figura 11 – Interação entre camadas do DRM (adaptado de Diehl, 2008)

Nesta visualização do modelo por camadas DRM, a gestão de confiança é responsável pela validação dos certificados assegurando que somente os emissores autenticados e em conformidade estão habilitados a criar e emitir licenças para os clientes de confiança e que somente os clientes autenticados e em conformidade são capazes de abrir as respetivas licenças fazendo também recurso a serviços de confiança existentes no sistema (Diehl, 2008).

A camada de gestão de direitos lida com os direitos de utilização associados ao conteúdo. Nesta camada, o fornecedor de conteúdos define os direitos a serem transpostos nos direitos de utilização e condições. A transposição é aqui realizada utilizando uma linguagem de expressão de direitos, como por exemplo o MPEG21-REL (MPEG-21:REL, 2005), e expede-os para a camada seguinte mais abaixo: a camada de aplicação de direitos.

A camada de aplicação de direitos permite assegurar que o conteúdo será exclusivamente utilizado tal como nas condições especificadas. Nesta camada existem essencialmente dois papéis (Arnab & Hutchinson, 2005): a proteção dos direitos de utilização associados ao

conteúdo, de modo a que não se consiga modificar os direitos de utilização sem ser detetado, e a garantia de que a aplicação dos direitos de utilização é assegurada e não é contornada.

4.2.2 DRM: estrutura por serviços

Com base nos principais papéis desempenhados pelos principais intervenientes num sistema DRM, é possível estabelecer de uma forma generalizada a relação entre a arquitetura de *software* ao nível aplicacional e os serviços que dão suporte às atividades dos intervenientes no sistema DRM (Michiels et al., 2005). Do ponto de vista do consumidor, para fornecer estas funcionalidades são necessários ao nível aplicacional a disponibilização de serviços pelos seus componentes. Do mesmo modo, e do ponto de vista do detentor de conteúdos e fornecedor, também é necessário que um conjunto de serviços esteja disponível de modo a tornar o sistema minimamente atrativo. O sucesso do sistema DRM será tanto maior quanto maior e mais eficaz for a oferta de serviços ao consumidor e ao fornecedor/distribuidor. Estes serviços têm uma relação direta com os componentes do sistema DRM anteriormente mencionados.

Alguns dos sistemas de DRM possuem as funcionalidades anteriormente mencionadas, estando estas geralmente disponíveis através de sete serviços (Michiels et al., 2005) (Figura 12):

- o serviço de conteúdos, *(Content Service)*, por exemplo, para oferecer suporte na procura e descoberta de conteúdos);
- o serviço de licenças (*License Service*), por exemplo, para permitir suportar a emissão de licenças);
- o serviço de controlo de acesso (*Access Service*), por exemplo, para garantir a produção de estatísticas de utilização);
- o serviço de rastreio (*Tracking Service)*, por exemplo, a produção de estatísticas de utilização);
- o serviço de pagamentos/financeiro (*Payment Service)*, por exemplo, oferecendo serviços de pagamentos eletrónicos);
- o serviço de importação (*Import Service)*, por exemplo, na submissão de conteúdo ao sistema DRM);
- o serviço de identificação (*Identification Service)* – por exemplo, na revelação de abusos (Verslype & De Decker, 2006).

O serviço de certificação só é necessário ao utilizar certificados digitais (*Certification Service* - por exemplo, na distribuição e revogação de certificados).

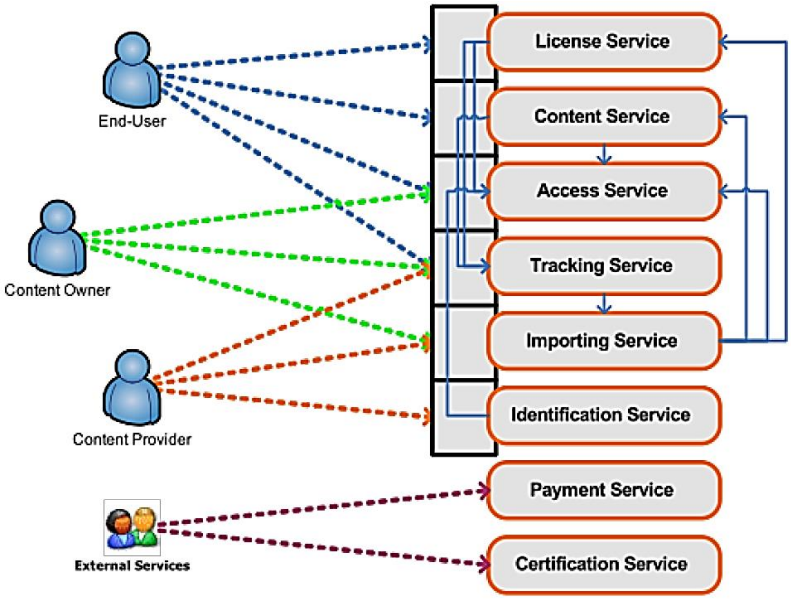


Figura 12 – Serviços genéricos da *framework* DRM (Serrão, 2008)

Estes serviços são necessários para suportar as tarefas inerentes ao fornecedor de conteúdos e ao consumidor e podem variar dependendo do papel desempenhado pelos principais participantes. O sistema DRM, para suportar um vasto conjunto de funcionalidades que suporte as principais atividades dos intervenientes (Llorente, Delgado, Maronãs & Florido, 2014), necessita de possuir uma fonte de dados de base comum a todos os serviços, compostos por identidades, conteúdos e direitos e as licenças e regras de partilha (Grzonkowski, 2010). Esta fonte de dados irá alimentar o conjunto de funcionalidades essenciais que são o pilar de outros serviços em camadas superiores (Grzonkowski, 2010). Num primeiro patamar temos a autenticação/autorização e regras de partilha de conteúdo e finanças (opcional). O patamar seguinte envolve a validação de direitos, a proteção de conteúdos gestão do conteúdo e a distribuição de dividendos (opcional). O último patamr no topo, consiste de dois elementos principais que atuam como serviços terminais que estabelecem a ligação ao sistema e ao utilizador através de interfaces específicos, permitindo a interação com o utilizador final e fornecedor do conteúdo.

Para que o ciclo de vida do conteúdo não seja interrompido, os vários serviços estão relacionados comunicando entre si, com vista a assegurar a compatibilidade com os quatro componentes estruturais base definidos no fluxo do conteúdo num sistema típico DRM (Figura 4). Na Figura 13 é possível visualizar a organização destes patamares.

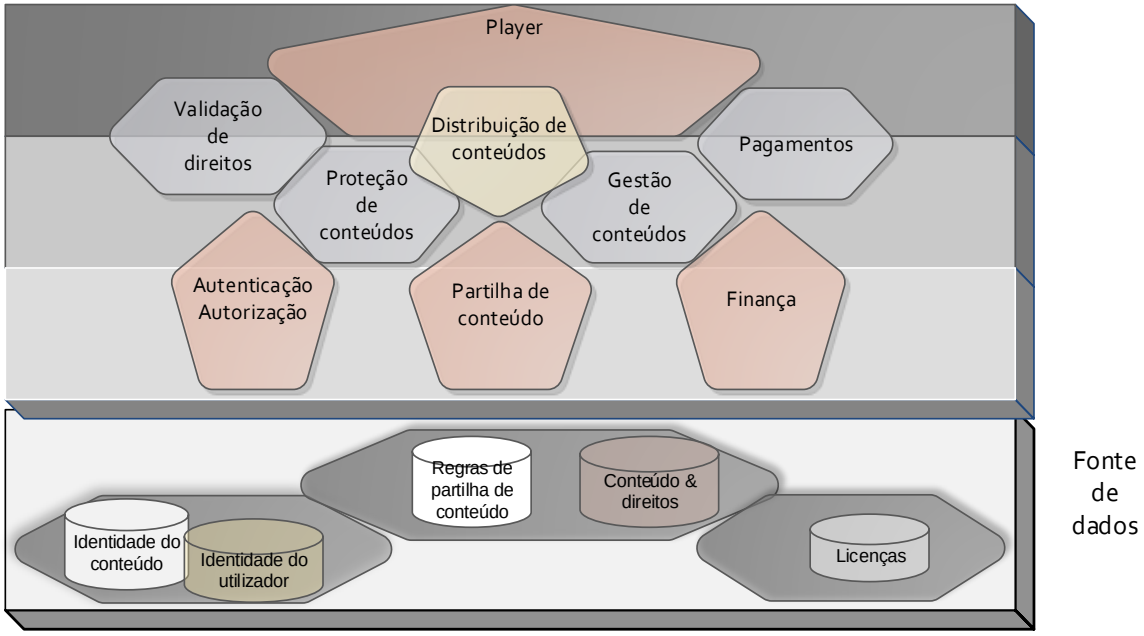


Figura 13 – Estratificação dos serviços DRM (adaptado de Grzonkowski, 2010)

Dependendo dos papéis assumidos pelos principais participantes, os serviços são o elemento de união entre as diferentes atividades em que os participantes intervêm (Grzonkowski, 2010). Um consumidor utilizando um *player*, ao usar estes serviços, pode contatar a fonte de dados principal com vista a poder adquirir o conteúdo e direitos associados, assim como o fornecedor de conteúdos pode fazer para poder estabelecer a proteção de conteúdo e definição de direitos. Assim, e dependendo do papel assumido pelo participante, a interação deste com as várias camadas pode ser diferente no mesmo sistema.

5 Aspetos de segurança do DRM

De um ponto de vista de segurança, para se poder estabelecer um ambiente DRM seguro, devem ser fornecidos serviços específicos de modo a que o conteúdo e as licenças sejam devidamente protegidos, assim como o dispositivo do utilizador deve garantir a aplicação de direitos de acordo com o nível proteção desejado (ISO/IEC 11889-3:2009, 2009). A segurança, ao ser um dos aspetos fundamentais nos sistemas DRM, leva a que um conjunto básico de requisitos tenham de ser satisfeitos. Os requisitos de segurança essenciais incluem a confidencialidade e a integridade do conteúdo, assim como a identificação única do utilizador no controlo de acessos e a existência de mecanismos de computação segura no processamento do conteúdo protegido e que assegurem a verificação e aplicação de direitos (Jonker & Mauw, 2004; Barhoush & Atwood, 2010). A segurança do canal de envio do conteúdo (que fornece a confidencialidade e integridade deste) em vez do conteúdo em si mesmo não é suficiente, pois

não garante uma proteção completa (Liu et al., 2003). Por isso, é requerida uma proteção persistente do conteúdo desde o momento que é enviado até ao fim do processo de consumo (Ku & Chi, 2004). Sendo a proteção do conteúdo realizada *offline*, e a chave que protege o conteúdo enviada por um canal diferente daquele por onde este é enviado, tal vem contribuir para a segurança da transação viabilizando a distribuição ilimitada e sem restrições do conteúdo protegido. Assim, o sistema DRM deve assegurar que os requisitos de segurança sejam observados, garantindo que propriedades como a integridade, autenticação, confidencialidade e não repúdio sejam acautelados nos pontos mais vulneráveis do sistema DRM, como, por exemplo, no conteúdo protegido, na licença e no cliente DRM (Hwang, 2008). A segurança nestes pontos deve ter em conta, essencialmente, três possibilidades de ataque: ataque aos protocolos DRM, ataque sobre contentores seguros (*secure containers)* (Grzonkowski, 2010) do dispositivo cliente e ataque sobre a aplicação de reprodução (Taban, Cárdenas & Gligor, 2006).

As regras de utilização do conteúdo, ao poderem ser inseridas como metadados na licença associada, vêm fornecer uma enorme flexibilidade na escolha de direitos pelo utilizador. Assim, de acordo com as suas necessidades, o utilizador escolhe a licença que mais lhe interessa e que depois irá aplicar sobre o conteúdo. Tendo em mente a separação conceptual entre conteúdo e licenças tal obriga a que tenha de se ter especial atenção à resistência a adulterações, quer do conteúdo protegido quer da licença. O processo de proteção do conteúdo e licenças é aqui atingido realizando o empacotamento seguro através da aplicação de várias ferramentas e técnicas de proteção (Ku & Chi, 2004). A confidencialidade e integridade do conteúdo podem ser alcançadas usando encriptação, assinaturas digitais e certificados digitais. A confidencialidade dos direitos também pode ser conseguida pela encriptação da licença, que, por sua vez, também contém embebida a chave de encriptação do conteúdo. Assim, e resumindo, no sistema DRM global a *confidencialidade* pode ser obtida usando encriptação, a *integridade* usando assinaturas digitais e a *autenticação* usando certificados digitais (Morin, 2009).

5.1 DRM - Vulnerabilidades

Qualquer sistema DRM deve garantir que os serviços disponibilizados sejam seguros nos seus pontos mais vulneráveis (conteúdo, licença e cliente DRM) (Hwang, 2008). Tendo cada um destes pontos as suas especificidades, são de seguida analisados do ponto de vista de segurança:

- Licença – Para ser segura a licença deve em primeiro lugar ser infalsificável, ou seja, deve ser impossível às partes envolvidas, exceto ao servidor de licenças, construir uma licença válida. Isto implica que a autenticidade da licença seja genuína. Uma outra propriedade importante que se tem de garantir é a integridade, ou seja, se houver qualquer alteração na licença esta será detetada tornando a licença inválida. Por fim, a licença deve estar ligada de forma unívoca ao conteúdo correspondente, assim como ao detentor da licença. Apesar de ser possível ligar uma licença a um ou mais dispositivos na posse do utilizador, contudo, estabelecer a ligação a um utilizador com presença física não é ainda uma tarefa fácil.

  A integridade e a impossibilidade de forjar uma licença sem que esta possa ser detetada pode ser alcançada aplicando assinaturas digitais. A associação da licença ao conteúdo correspondente pode ser alcançada inserindo um identificador único do conteúdo na respetiva licença. Tal identificador pode ser um resumo (*hash*) do conteúdo, ou um identificador DOI, ou outro tipo de identificação. A associação do conteúdo a um utilizador pode ser feita pela inserção de certificado pessoal do utilizador ou por um identificador único desse certificado.

- Conteúdo – Quando o produtor de conteúdo submete novo conteúdo, terceiros não o devem poder adulterar (integridade) nem devem poder aceder ao mesmo (confidencialidade) antes de este estar protegido. A autenticação faz com que seja possível determinar quem é o responsável pela submissão deste novo conteúdo no sistema DRM. O conteúdo protegido e distribuído pelo servidor de conteúdos só poderá ser consumido por utilizadores na posse da licença válida correspondente. Para todos os outros é necessário assegurar a confidencialidade do conteúdo. Contudo, tal nem sempre se tem demonstrado exequível pois a prática tem mostrado que é muito difícil de evitar que os consumidores se apoderem do conteúdo de forma desprotegida. Por esta razão, e sempre que haja deteção de violação, o servidor de conteúdos deve poder aplicar sobre o conteúdo desprotegido um mecanismo de deteção (por exemplo, através do *watermark* inserido no conteúdo) e rastreio.

  A combinação de assinaturas digitais e de certificados pode aqui ser utilizada para obtenção quer da integridade do conteúdo protegido quer da autenticação. A confidencialidade pode ser obtida usando a encriptação tanto por métodos de chave simétrica como de chave assimétrica. O envio da chave pode ser feito através da licença (ou objeto licença). O não repúdio no mecanismo de deteção de abuso sobre o conteúdo protegido pode ser conseguido pela combinação de assinaturas digitais e certificados. Pode haver situações

em que a identificação do consumidor pode ser inserida no conteúdo por *watermark* antes de este ser encriptado e enviado para consumo.

- O cliente DRM - Perante o sistema, somente as entidades que se podem autenticar como de confiança podem estar autorizadas a ter a posse do conteúdo de forma desprotegida (Abbadi & Alawneh, 2008) (por exemplo, o sistema operativo, o controlador DRM, entre outros). O interesse é manter seguras as chaves de proteção do conteúdo e o conteúdo desprotegido. Assim, pode-se garantir a sua confidencialidade sendo por isso importante a permanência da integridade das aplicações que constituem o cliente DRM (o controlador e o reprodutor entre outros) (Taban et al., 2006). Na licença deve-se ter em conta a sua integridade, pois qualquer alteração (por exemplo, alteração da validade) pode impedir o utilizador de aceder ao conteúdo.

  A obtenção de autenticação de diferentes entidades de confiança, combinada com a confidencialidade de dados, pode ser conseguida através de técnicas de computação segura (TCG, 2011a; Yan & Peng, 2011). Torna-se assim possível estabelecer um elevado nível de segurança recorrendo à aplicação de medidas de proteção tecnológica (Kang et al., 2006) capazes de proteger as chaves de encriptação do conteúdo (Prihandoko, Ghodosi, Litow, 2013). Aqui podem ser utilizados contentores seguros pois para desencriptar o conteúdo protegido, o cliente DRM necessita de uma chave secreta que não pode ser conhecida do consumidor. A integridade do cliente DRM, e até de outras entidades de *software* presentes, pode ser mantida recorrendo a técnicas resistentes a falsificações, de *self-checking white-boxing* e de *ofuscação* de código (Jin, Myles & Lotspiech, 2005; Horne, Matheson, Sheehan & Tarjan, 2002; VanOorschot, Somayaji & Wurster 2005; Cappaert, Preneel, Anckaert, Madou & De Bosschere, 2008; Michiels & Gorissen, 2007; Hwang, 2008; Hietanen & DeRosnay, 2006), entre outras.

5.2 DRM - conteúdos e licenças

Para que o cliente DRM consiga interpretar o conteúdo é necessário definir o formato do conteúdo protegido e respetivas licenças. Os sistemas DRM mais em voga utilizam formatos muito específicos, que tornam praticamente impossível a utilização, quer de conteúdo quer das respetivas licenças, quando se transfere de um sistema para outro (Jamkhedkar & Heileman, 2008). Contudo, existe uma base comum de informação que normalmente fica embebida no próprio conteúdo protegido ou na respetiva licença quando estes são preparados para

distribuição. A estrutura básica destes objetos (conteúdo protegido e licença) é de seguida descrita realçando-se a informação neles contida.

5.2.1 DRM - conteúdo protegido

A proteção de conteúdo em DRM baseia-se na utilização de mecanismos criptográficos que permitem a cifragem do conteúdo antes da distribuição de modo a impedir a interceção de informação valiosa durante a transmissão do conteúdo. Num sistema DRM um conteúdo protegido corresponde a um ficheiro que contém o conteúdo cifrado num contentor seguro em conjunto com outra informação relacionada, incluindo:

- Identificador único (Id do conteúdo) para o objeto encriptado poder ligar o conteúdo aos direitos de utilização;
- Informação acerca do algoritmo de encriptação utilizado;
- Informação acerca do emissor de licenças (por exemplo, a URL do LS ou a URI de aquisição da licença);
- Informação descrevendo o conteúdo (por exemplo, o título do conteúdo, o autor, outros);
- O valor do resumo do conteúdo (opcional na proteção da integridade do conteúdo);
- Assinatura do fornecedor de conteúdo.

5.2.2 DRM - licenças

Normalmente a licença é um ficheiro gerado para descrever os direitos de utilização de um conteúdo protegido (Barlas, 2006) baseado em XML A licença especifíca os direitos de acordo com o perfil do licenciado sendo estes definidos pelo detentor do conteúdo através de uma REL. Uma licença é uma agregação de permissões atribuídas por um detentor de direitos a um beneficiário que só pode ser emitida sob a autoridade do detentor de direitos e que contém a informação requerida para decifrar o conteúdo protegido nela especificada (Sheppard & Safavi-Naini, 2006b). Quando o utilizador pretende executar uma ação sobre o conteúdo, o seu dispositivo verifica se o utilizador possui uma licença e se esta está assinada por um emissor reconhecido e é válida, concedendo-lhe o direito de executar essa ação de acordo com as condições associadas (Sheppard & Safavi-Naini, 2006b). Existem essencialmente dois tipos de licenças: as licenças de (re)distribuição e as licenças de utilização (Sachan & Emmanuel, 2011; Sachan et al., 2012). Quando o detentor emite licenças ao(s) distribuidor(es) este(s) pode(m) posteriormente gerar licenças de redistribuição aos seus sub-distribuidores ou emitir novas licenças de utilização para os consumidores de acordo com as permissões e restrições definidas nas licenças recebidas (Sachan & Emmanuel, 2011). Tipicamente uma licença, ou objeto

licença, contém as regras de utilização, acordados com o recetor da licença expressos numa REL e contêm, além dos direitos de utilização, a cifra de proteção de conteúdo C_{EK}, a assinatura digital do emissor e metadados relacionados. As regras de utilização são o conjunto de direitos que o recetor pode praticar com o respetivo conteúdo na sua posse, tal como copiar, *pay-per-view*, alugar, imprimir, entre outros, e respetivas condições de utilização. A C_{EK} é a chave simétrica usada na encriptação/desencriptação do conteúdo associado; a assinatura digital é aquela gerada pelo emissor da licença (servidor de licenças) no ficheiro correspondente à licença com o objetivo de proteger a sua integridade e provar a sua autenticidade; os metadados contêm normalmente a seguinte informação:

- A identificação da licença (*License ID*): Um número de série que identifica inequivocamente a licença;
- A identificação do conteúdo associado (*Content ID*): Um número de série que identifica inequivocamente o conteúdo associado à licença;
- Identificação do fornecedor do conteúdo (*Content Provider ID*): Um número de série que identifica inequivocamente o fornecedor de conteúdo;
- Local (URL) de aquisição da licença (*License Acquisition URL*): o URL de onde a licença pode ser obtida (*downloaded*);
- Parâmetros criptográficos (sempre que forem necessários e aplicáveis): com vista a identificar não só o tipo de criptografia, mas também a parametrização aplicada;
- Resumo do conteúdo protegido (*hash*): é utilizado para proteger a integridade do conteúdo; se o resumo ou o conteúdo for alterado a assinatura será inválida;
- Assinatura digital do conteúdo.

5.3 Licenciamento em DRM

Vários autores têm proposto o conceito de domínio em DRM (Popescu, Crispo, Tanenbaum, & Kamperman, 2004; Doërr & Kalker, 2008; Win, Thomas, Emmanuel, & Kankanhalli, 2009; Sheppard, & Safavi-Naini, 2006b), com vista a solucionar o problema da partilha de conteúdo no que respeita aos requisitos dos detentores de conteúdos e consumidores. A ideia básica consiste em agrupar os dispositivos numa entidade abstrata, a que se dá o nome de domínio, e permitir que o conteúdo protegido flua livremente de dispositivo para dispositivo pertencente ao domínio (Doërr & Kalker, 2008). Assim, um domínio é formado por um conjunto de dispositivos onde o conteúdo legalmente adquirido pode ser livremente movimentado entre os dispositivos desse domínio sendo gerido pelo gestor de domínio. O domínio pode ser criado

por qualquer um e toda a autoridade de gestão do domínio e de emissão de licenças tem origem no criador do domínio (Sheppard, & Safavi-Naini, 2006b). Um dispositivo pode juntar-se ao domínio através de protocolos criptográficos envolvendo o controlador de domínio, responsável pelo mesmo. Em determinado tipo de sistemas, uma forma de controlar o domínio é definindo o número máximo de dispositivos que se podem juntar. Noutro tipo de sistemas esse controlo pode ser feito utilizando o emissor de licenças que atua como um controlador de domínio. Sendo aceite, o dispositivo recebe dados que o habilita a desencriptar a informação da licença referente a esse domínio (Safavi-Naini & Sheppard., 2010). Apesar de partilharem uma arquitetura semelhante (Doërr & Kalker, 2008) e poderem suportar vários modelos de negócio com utilizações em partilha social, partilha em redes domésticas e partilha entre membros de clubes (Sheppard, & Safavi-Naini, 2006b), não têm tido a aceitação em larga escala requerida pois a interoperabilidade entre os diferentes sistemas tem criado fortes barreiras de aceitação (Doërr & Kalker, 2008). Um dos grandes problemas manifestados por vários autores relaciona-se com a portabilidade do conteúdo e das licenças entre diferentes sistemas DRM (Jeong, Park, Kim & Yoon, 2007; Safavi-Naini, Sheppard, & Uehara, 2004; Taban et al., 2006). Além do formato do conteúdo poder ser diferente, a REL também o pode ser, obrigando a que haja uma "tradução" de direitos entre sistemas, tornando o processo extremamente complexo (Jamkhedkar & Heileman, 2008). Contudo diferentes iniciativas não são alheias a este problema tendo apresentado propostas de tradução entre diferentes sistemas (Jamkhedkar & Heileman, 2008; Delgado, Prados & Rodríguez, 2005b; Rodríguez & Delgado, 2006; Nadah, deRosnay & Bachimont, 2007; Maroñas, Rodríguez & Delgado, 2009a). Na tentativa de contribuir para uma solução para este problema iremos apresentar em capítulos posteriores algumas propostas que seguem normas internacionais, como o MPEG-21, baseando o conceito na verificação da sua elegibilidade do utilizador dentro do domínio académico antes da emissão da licença.

6 Conclusão

Ao partilhar conteúdo no meio académico deve-se considerar dois tipos de sistemas. Um sistema é mediado pela iniciativa de "acesso livre" com suporte no licenciamento *Creative Commons* onde os detentores de conteúdo pretendem disseminar conhecimento, mas baseados num sistema de confiança e respeito entre as partes. O outro faz recurso do DRM e é sua função proteger o conteúdo fazendo com que os direitos associados sejam respeitados recorrendo a medidas tecnológicas de proteção. Neste último sistema muitas e variadas técnicas, processos e mecanismos estão incorporados. Vários participantes interatuam com os mais diversos componentes tecnológicos de forma a viabilizar uma infraestrutura minimamente capaz de

assegurar a aplicação de direitos de PI numa multitude de relações que, independentemente da tecnologia, fazem com que este tipo de sistemas seja altamente complexo. Ambos os sistemas podem coexistir, dependendo de se querer ou não proteger o conteúdo no que respeita a direitos de PI tendo em conta as suas áreas de aplicação.

O DRM, fornecendo ferramentas e mecanismos para a gestão do conteúdo ao longo do seu ciclo de vida, e focalizando-se em aspetos que incluem o controlo do uso e gestão de informação sobre direitos, é a solução apropriada para poder solucionar muitos dos problemas relacionados com a proteção de direitos de PI. Dependendo do ponto de vista, vários tipos de estruturas podem ser desenhadas mas todas elas têm um ponto comum: a segurança. A integridade, a confidencialidade, autenticação e o controlo de acesso são aqui de se ter sempre em conta, podendo ser atingidas pela aplicação das mais diversos mecanismos e medidas tecnológicas de proteção.

Este capítulo, ao fazer o levantamento das tecnologias DRM e principais formas de o descrever, indica-nos também quais os seus pontos fracos, nomeadamente as suas principais vulnerabilidades e as questões relacionadas com interoperabilidade de conteúdos e das licenças, que são limitadoras da sua flexibilidade. No contexto académico, estas limitações não são de ignorar e somente a correta aplicação da tecnologia apropriada pode garantir o sucesso deste tipo de sistemas neste meio, e assim assegurar a preservação de direitos ao longo do ciclo de vida do conteúdo.

Capítulo 3

Análise de soluções de DRM "abertas"

Resumo

Ao longo do presente capítulo é analisado um conjunto de sistemas de DRM especificados num formato "aberto", com vista a melhor perceber o seu modo de funcionamento. São aqui apresentadas e analisadas seis soluções existentes: OpenSDRM (OpenSDRM, 2005), OMA-DRM (OMA, 2011e), MIPAMS (DMAG, n.d.), OpenIPMP (OpenIPMP, n.d.), DReAM (Fernando, Jacobs & Swaminathan, 2005) e Marlin (Marlin, n.d.). Com base nessa análise será selecionado o sistema que melhor se alinha para dar o suporte à proteção de direitos de PI no contexto académico.

1 Introdução

Apesar da divisão existente entre plataformas DRM designadas por "proprietárias", e como tal de especificações fechadas, e as que procuram ser "interoperáveis", e muitas vezes baseadas em normas internacionais e em código aberto (*opensource*), nem sempre ser muito clara, iremos considerar para análise algumas das mais conhecidas atualmente. A "abertura" destas soluções em termos de alinhamento com normas internacionais e o facto de serem disponibilizadas num formato de código aberto fazem com que sejam consistentes com a essência do meio académico onde a difusão do conhecimento é um dos objetivos a atingir para o bem da comunidade (Hahn, Lowry, Lynch, Shulenberger & Vaughn, 2009). A "abertura" pode ser entendida de duas formas: como especificação aberta de todos os componentes e funções e como implementação de tais componentes e funções em regime de código aberto. Apesar de existirem alguns sistemas cujas especificações se encontram publicadas, como, por exemplo, o sistema da *Open Mobile Alliance* (OMA, 2011e), no entanto, estes mesmos sistemas estão por vezes orientados a um domínio de aplicação muito específico (como, por exemplo, a indústria dos telemóveis) (Torres, Serrão, Dias & Delgado, 2008) que os limitam na sua área de aplicação. Independentemente desta limitação, não disponibilizam funcionalidades suficientemente abrangentes na gestão de licenças (González & Gil, 2008). Por isso, encontrar uma solução satisfatória que consiga abarcar o meio educacional e académico não é fácil de encontrar, pois nem todas as plataformas

DRM atuais obedecem a normas cuja especificação é aberta (ou pública), nem são de código aberto. Por esta razão somente são aqui apresentadas e comparadas soluções cujas especificações são de domínio público e que podem ser minimamente enquadradas nos conceitos aqui expressos.

2 Classificação de sistemas DRM

A classificação de sistemas DRM é bastante diversificada de acordo com o propósito a que se destinam. No entanto, uma das possíveis classificações, pode ter em conta a conectividade com o meio exterior, permitindo assim classificar estes sistemas em duas categorias genéricas: *offline* e *online* (Sun, Yang & Wang, 2005). Estes sistemas podem ainda ser divididos em sistemas baseados nos dispositivos e sistemas baseados na identidade (Palavalli et al., 2008; Sun et al., 2005) possuindo cada um vantagens/desvantagens consoante o cenário de aplicação (Koster, 2007).

Nos sistemas *offline* os clientes podem reproduzir os conteúdos sem terem uma ligação a um sistema central. Os mecanismos de autenticação estão embutidos nos programas (Sun et al., 2005). A grande vantagem deste tipo de sistema está na sua conveniência, pois os clientes não necessitam de qualquer ligação à Internet. A principal desvantagem reside no facto de, para além de serem menos seguros, este tipo de sistemas de DRM não poderem implementar de forma flexível as regras de utilização (estas são quase sempre fixas e predefinidas) (Sun et al., 2005; Koster, 2007).

Nos sistemas *online* os clientes podem reproduzir os conteúdos através de uma ligação a um sistema central, oferecendo um nível de segurança adicional que pode ser facilmente alterado através da ligação ao servidor (Sun et al., 2005). Como exemplo pode-se indicar os diferentes serviços de música *online,* os quais normalmente adotam este tipo de modelo.

No caso dos sistemas baseados nos dispositivos, os mesmos são muito específicos na seleção do dispositivo para reproduzir conteúdos. Quando o utilizador se regista no sistema DRM e procede à aquisição de conteúdos e direitos associados, a licença respetiva é emitida com a identidade pré-definida do dispositivo. Assim, é possível limitar possíveis atentados já que a licença ao ser restrita ao dispositivo para que foi emitida deixa de ser válida noutros dispositivos (CiscoVNI, 2014; Palavalli et al., 2008). Esta é uma das formas preferidas dos grandes fornecedores de soluções DRM comerciais (Microsoft, OMA, iTunes) que utilizam este tipo de sistemas.

Por sua vez, os sistemas DRM baseados na identidade fazem com que a autenticação esteja concordante com a identidade dos utilizadores. Se os utilizadores possuírem um determinado *token* (como por exemplo um *smartcard)* podem provar a sua identidade e assim podem reproduzir conteúdos em qualquer dispositivo bastando para isso usar esse mesmo *token* (Palavalli et al., 2008). Contudo, esta não é das melhores soluções pois obriga o utilizador a ter que recorrer a dispositivos adicionais (por exemplo o leitor de cartões) e com isso a ter custos extra, independentemente do inconveniente de ter que transportar sempre o cartão para poder usufruir do conteúdo no momento.

Na proposta apresentada neste trabalho preferiu-se recorrer a um sistema *online* baseado na identidade, sem a utilização de *tokens*, pois é a que garante uma arquitetura com mais flexibilidade, o que vem ao encontro das características de mobilidade de uma grande parte dos utilizadores do meio académico.

3 Sistemas DRM "abertos"

Atualmente as soluções existentes na área dos sistemas DRM são variadas, sendo muitas delas orientadas para a exploração comercial de conteúdos. Grande parte destes sistemas são proprietários, não sendo conhecidas quaisquer especificações e/ou descrições da sua arquitetura (Torres et al., 2008). Uma das razões é que muitos sistemas fazem recurso da obscuridade como a base em que assenta o seu próprio modelo de segurança (Stamp, 2002a; Llorente et al, 2014). O seu objetivo é impedir que os utilizadores consigam contornar os mecanismos de segurança implementados ao manter secretas a arquitetura e as funcionalidades do sistema. Outra razão tem a ver com o modelo de negócio das empresas que os exploram ao tentarem evitar que outras empresas concorrentes ofereçam sistemas funcionalmente equivalentes, diminuindo assim a sua influência (Schreiner, 2011). Como resultado, o(s) formato(s) de ficheiro(s) (conteúdo e/ou licença) têm tendência a tornar-se proprietários e os *metadados* embebidos a tornar-se incompatíveis com os de outros sistemas (Torres et al., 2008; Schreiner, 2011). Esta falta de comunicação impede uma partilha de conteúdo em grande escala. Por isso, entende-se que a melhor solução é aquela onde as especificações se baseiam em normas internacionais (Cheng & Rambhia, 2003; Torres, Serrão, Dias & Delgado, 2008), já publicadas, ou com enorme potencial de o virem a ser.

De seguida iremos analisar alguns sistemas e *standards* DRM cujas especificações e código são "abertos", isto é, de conhecimento e de utilização públicas: OpenSDRM, OMA-DRM, MIPAMS, OpenIPMP, DReAM, e Marlin. Estas soluções, por apresentarem potencial no

contexto da proteção de conteúdos abrangidos por direitos de PI, sendo vantajosas basearem-se em *standars* (Anido, et al., 2014) podem alavancar a utilização deste tipo de sistemas no contexto académico. Contudo, uma análise mais aprofundada indicar-nos-à qual é a mais alinhada ou com maior potencial para aplicação no contexto académico.

3.1 OpenSDRM

O OpenSDRM teve origem no projeto MOSES (*MPEG Open Security for Embedded Systems*) (MOSES, 2004). É um sistema DRM com uma arquitetura facilmente adaptável (OpenSDRM, 2005), pois graças ao seu desenho, pode ser configurado para utilização em vários modelos de negócio e para diferentes tipos de conteúdo. O OpenSDRM apresenta-se como uma solução orientada para a proteção de conteúdos que permite ser aplicado em qualquer meio em que exista publicação e negociação de conteúdos multimédia em formato digital (Torres et al., 2008). Esta solução é composta de vários elementos que cobrem a cadeia de valor da distribuição de conteúdos, desde a produção de conteúdos até à sua utilização. Vários aspetos relacionados com a distribuição de conteúdos e transação são cobertos: produção de conteúdos, preparação e registo de conteúdos, negociação, aquisição e distribuição são contemplados, assim como a autenticação dos principais utilizadores e reprodução condicionada (Serrão, 2008). Sendo uma solução baseada em código aberto., torna-se bastante interessante para o meio académico, pois oferece uma grande flexibilidade na sua adaptação (Torres et al., 2008).

Sendo esta solução composta por um conjunto de componentes distribuídos que permitem a troca de mensagens normalizadas sobre redes abertas, é de realçar que, acima de tudo, todos os seus elementos constituintes comunicam uns com os outros através de interfaces bem definidas onde é assegurada uma comunicação segura entre qualquer dos componentes da plataforma (OpenSDRM, 2005). Além disso, a solução pode ser complementada com vários elementos opcionais capazes de cobrir toda a cadeia de valor do conteúdo desde a produção até à utilização do conteúdo (Serrão, 2008). Obviamente que tem em consideração os aspetos principais no que se refere à distribuição e negociação de conteúdos tais como a produção, preparação e registo, distribuição interativa, negociação e distribuição e aspetos de autenticação e uso condicionado de conteúdos.

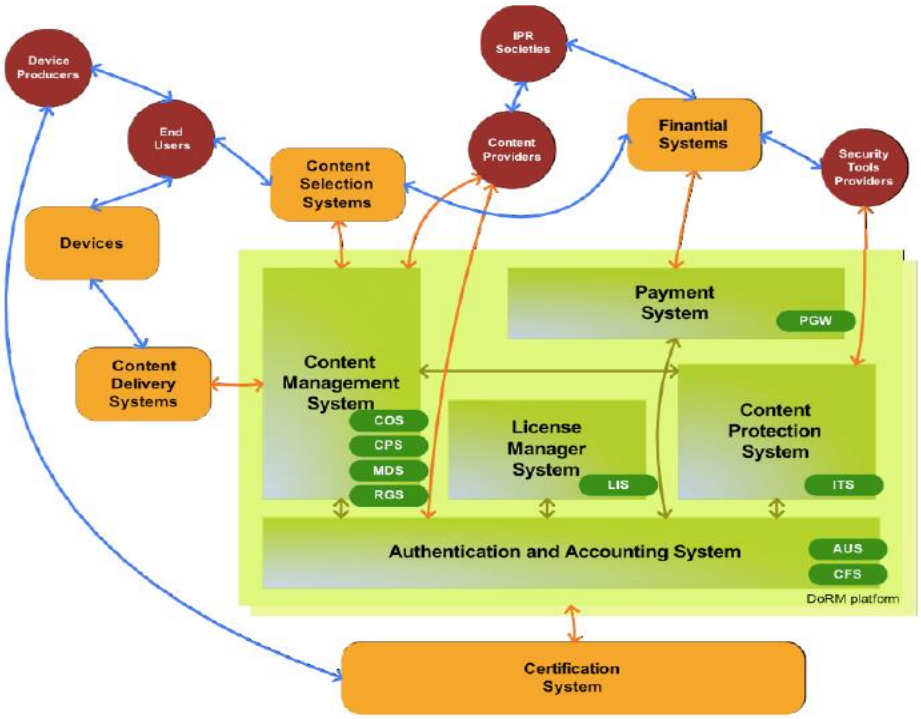


Figura 14 – Elementos da arquitetura OpenSDRM (Serrão, 2008)

Do ponto de vista conceptual a arquitetura do OpenSDRM (Figura 14) define um cenário capaz de lidar com múltiplos modelos de negócio para a distribuição de conteúdos abrangidos por direitos de PI (OpenSDRM, 2005). Conceptualmenete, esta arquitetura é suportada em três blocos distintos: conjunto de entidades internas capazes de fornecerem as funcionalidades DRM necessárias ao objetivo da plataforma; conjunto de entidades externas, mas que se relacionam com o DRM e, por fim, o utilizador (não necessariamente o utilizador final) (OpenSDRM, 2005).

Na plataforma OpenSDRM fazem parte um conjunto de componentes que trocam mensagens estandardizadas sobre redes abertas como a Internet. O OpenSDRM usa dois importantes conceitos na sua conceção: atores e componentes. Um ator é uma pessoa, entidade ou organização que usa um componente. Um componente é um artefacto ou ferramenta capaz de oferecer um conjunto de funcionalidades relacionadas com a gestão de direitos (Serrão, 2008). Os elementos arquitetónicos são de seguida descritos tendo em conta as suas funções (Serrão, 2008):

Sistema de autenticação e monitorização - constituído por dois componentes (AUS - Servidor de Autenticação e CFS - Servidor de Configuração), tem por objetivo registar e localizar todos os componentes e atores do sistema atribuindo e validando credenciais. É constituído por:

Servidor de Autenticação (AUS) - é usado para registo e autenticação de Atores e Componentes. Atua como um servidor que cria e distribui credenciais pelas outras entidades. As principais funcionalidades deste servidor, entre outras, são as seguintes:

- Registo no sistema dos componentes incluindo funcionalidades de atualização e de eliminação/anulação de componentes;
- Registo no sistema de utilizadores que interagem com os Componentes incluindo funcionalidade de atualização e de eliminação/anulação de utilizadores;
- Verificação e validação do agente do utilizador (*wallet)* instalado no sistema;
- Verificação e validação do intermediário (*gateway)* de pagamentos.

Serviço de Configuração (CFS) – constituído por um servidor de configuração, que regista a localização de todos os componentes para que estes possam ser acedidos. As principais funções deste servidor são:

- Registo da localização e detalhes dos outros componentes;
- Fornecimento de informação específica de um componente a outros componentes.

Sistema de gestão de Licenças – constituído pelo License Server (LIS), faz a gestão das licenças criando padrões (*templates*) consoante as definições do detentor do conteúdo e posteriormente enviando as licenças geradas aos utilizadores. É aqui de considerar a existência de mecanismos que ligam de forma protegida as licenças às chaves de conteúdo. As principais funcionalidades deste servidor são:

- Armazenamento seguro das chaves de proteção de conteúdo;
- Disponibilização de *relatório* de utilização das licenças;
- Criação de licenças específicas para o conteúdo e para o utilizador;
- Atualização e eliminação/anulação de licenças no sistema;
- Obtenção de licenças pelo utilizador.

Sistema de Ferramentas de proteção – (ITS) constituído pelo servidor de Gestão de Ferramentas - Protection Tools Server (PTS) - regista as novas ferramentas de proteção e recebe pedidos autenticados para descarregar especificamente certo tipo de ferramentas de proteção adequados ao tipo de conteúdo. Além disso, disponibiliza as ferramentas de proteção que permite ao Content Preparation Server (CPS) a proteção do conteúdo pelo detentor que pretende efetuar a proteção. As principais funcionalidades a realçar são:

- Listagem das ferramentas de proteção disponíveis;
- Inserção de novas ferramentas de proteção;

- Validação das funcionalidades de proteção disponibilizadas;
- Disponibilização para *download* das ferramentas de proteção.

Sistema de pagamentos (PGW) – constituído pelo servidor de pagamentos, verifica e valida as formas de pagamento realizadas pelo utilizador. As suas principais funções são:

- Requisição da intermediação pagamentos a partir da requisição do conteúdo;
- Subscrição/registo de novas lojas distribuidoras de conteúdo;
- Registo de pagamentos de transações realizadas.

Sistema de gestão de conteúdos (Content Management System) – é essencialmente constituído por quatro servidores que lidam diretamente com o conteúdo, preparando-o para ficar disponível ao utilizador final.

O Servidor de preparação de conteúdos (Content Preparation Server - CPS) recebe o conteúdo de uma fonte e codifica esse conteúdo em bruto (*raw*) para um formato específico (o formato de codificação fica fora do âmbito do OpenSDRM). As suas principais funções incluem:

- Codificação do conteúdo para um formato específico;
- Adição de metadados específicos ao conteúdo e ao detentor de direitos;
- Aplicação da proteção de acordo com a ferramenta de proteção selecionada.

O Servidor de Registo – (Registration Server - RGS) - atribui identificadores únicos ao conteúdo. As suas principais funcionalidades incluem:

- Registo de novos conteúdos;
- Registo de metadados;
- Listagem de conteúdos específicos que satisfazem um critério determinado,

O Servidor de envio de conteúdos (Media Delivery Server - MDS) – regista o armazenamento e o envio de conteúdos ao utilizador. As suas principais funcionalidades são:

- Registo da localização do conteúdo no sistema;
- Notificaçao do sistema, dos pedidos de uso do conteúdo;
- Notificação do sistema, dos *downloads* de conteúdo.

O Servidor de Comércio (Commerce Server – COS) – responsável por apresentar o conteúdo aos utilizadores. As suas principais funcionalidades são:

- Apresentação do conteúdo ao utilizador;
- Apresentação/negociação das condições de utilização.

Sistema do utilizador final - constituído por 2 componentes principais: o dispositivo que mostra o conteúdo (Media Player) e o agente DRM do utilizador (Wallet) que permitem ao utilizador interagir com o conteúdo e com os múltiplos componentes do OpenSDRM. Através do módulo Wallet é possível assegurar e exercer a aplicação dos direitos sobre o conteúdo protegido. As principais funções deste módulo são:

- Registo e certificação de utilizadores;
- Validação e certificação da Wallet;
- Armazenamento seguro de informação sensível;
- *D*escarregar as licenças sempre que necessário;
- *Descarregar* ferramentas de proteção, sempre que necessário.

Através do módulo de Reprodução de Conteúdos ou Player (Content Rendering Application/Media Player), o utilizador consegue visualizar e utilizar o conteúdo. O Player está ligado ao Wallet de modo a aceder à informação necessária para obter a licença e chaves do conteúdo, permitindo assim a reprodução do conteúdo protegido e governado por DRM. A sua implementação está dependente do tipo de conteúdo protegido (Torres et al., 2008). De acordo com as funcionalidades disponibilizadas são implementados variados serviços consoante os componentes e atores em causa (Figura 15).

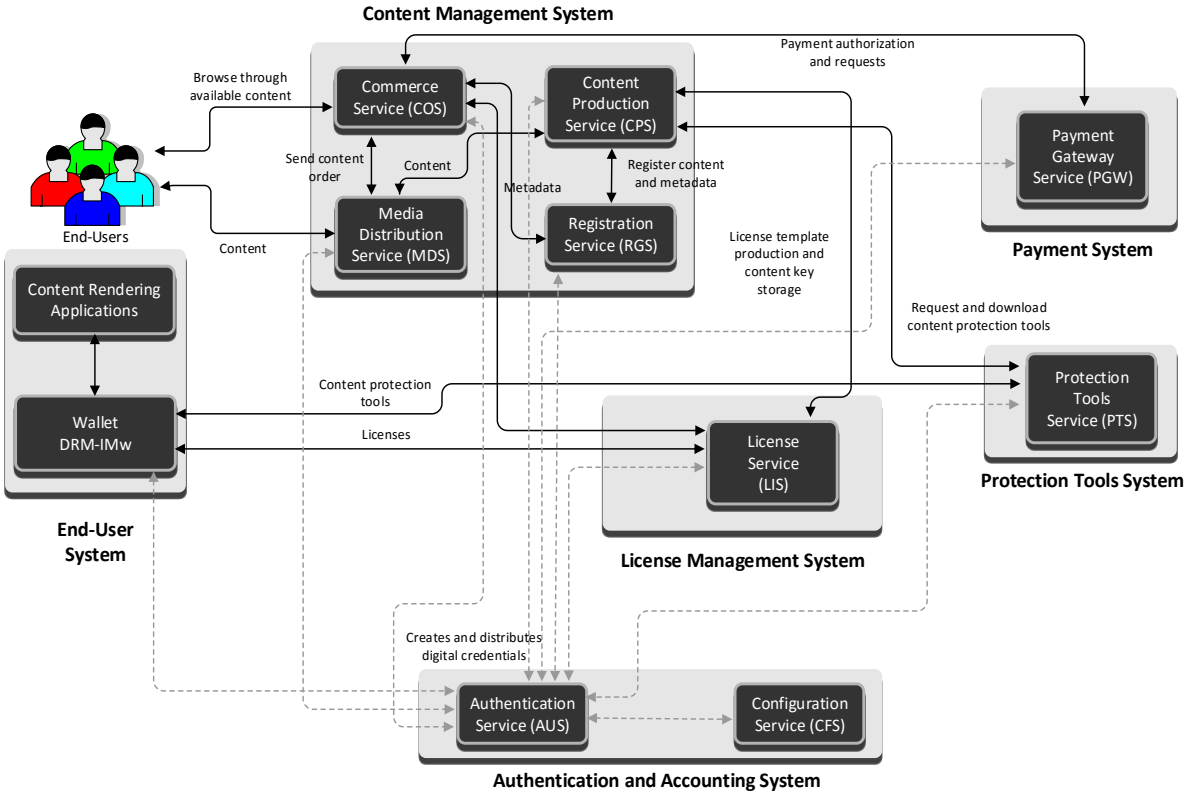


Figura 15 – Arquitetura da plataforma OpenSDRM (adaptado de Serrão, 2008)

Os componentes e atores que externamente interagem com os elementos da estrutura OpenSDRM (Figura 16) são os seguintes (Serrão, 2008):

- *User* – indivíduo que pretende consumir o conteúdo e que interage com o OpenSDRM identificando-se com vista a adquirir licenças e assim usufruir/usar o conteúdo;
- *IPMP Tools Provider* – entidade que cria e disponibiliza ferramentas de proteção de conteúdo (encriptação, watermarking, entre outras). A seleção de um tipo específico de ferramenta de proteção de um determinado fornecedor faz prever a existência de relações de negócio entre esta e o fornecedor de conteúdos;
- *Content Provider* – é o fornecedor de conteúdos que alimenta a plataforma OpenSDRM com conteúdos, metadados e os direitos relacionados.
- *Payment Infrastructure* – entidade que atua como facilitadora de funcionalidades de comércio eletrónico fornecendo serviços que lidam com pagamentos eletrónicos;
- *Certification Authority* – entidade responsável pela receção de pedidos de/para emissão de credenciais digitais a outras entidades no sistema. Estas credenciais serão utilizadas pelas entidades do sistema para se autenticarem e estabelecerem canais de comunicação seguros entre si. Esta entidade pode ser interna ao sistema OpenSDRM, podendo ser gerida por outra entidade, ou pode ser uma entidade comercial externa de certificação.

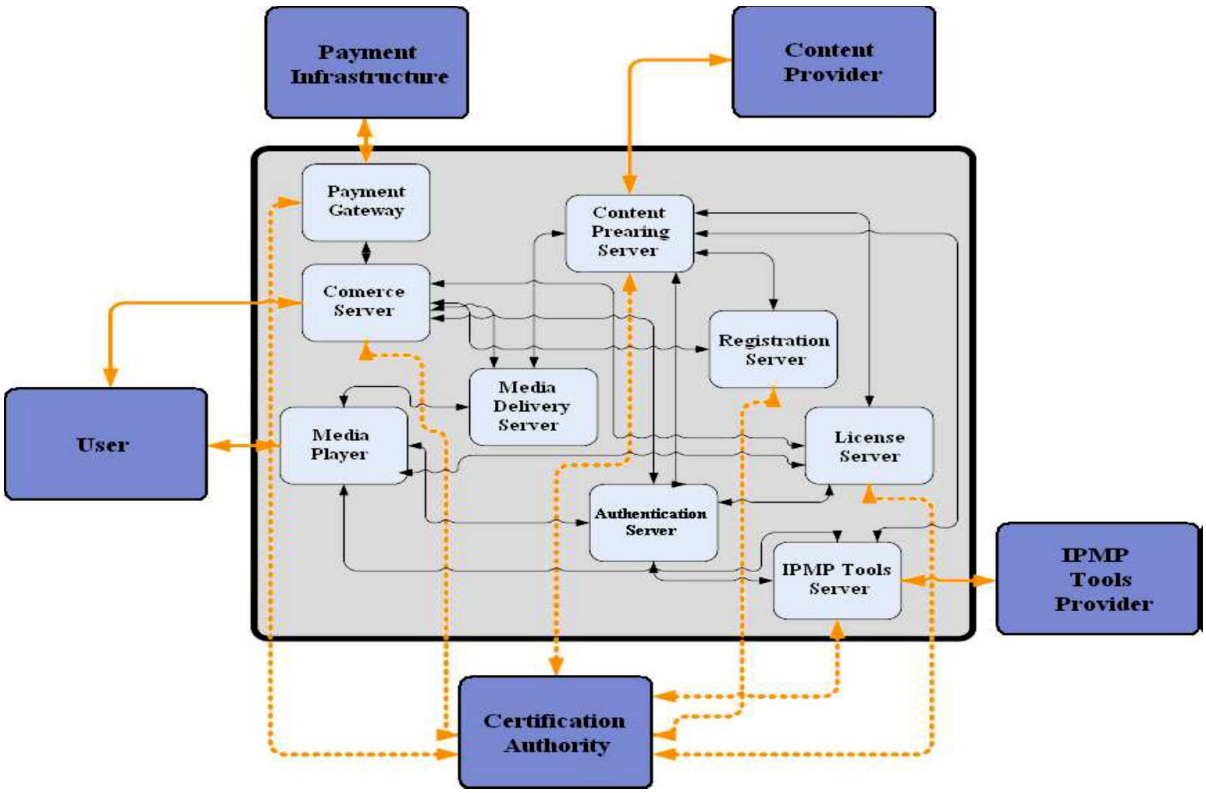


Figura 16 – Elementos externos e OpenSDRM (adaptado de Serrão, 2008)

De referir que os componentes da arquitetura comunicam uns com os outros através de canais de segurança sustentados pelo protocolo SSL/TLS (OpenSDRM, 2005). Os componentes internos são orientados à realização do serviço que fornecem, sendo auto descritivos expondo a descrição dos serviços que disponibilizam (via WSDL), permitindo aos outros componentes autenticados conectar-se e usar os seus serviços (OpenSDRM, 2005). A comunicação entre estes componentes é realizada através da permuta de mensagens SOAP (SOAP, 2007; Brown, Fox, Hada, LaMacchia, & Maruyama, 2001) e a descoberta e identificação de serviços é realizada através do servidor de configuração.

3.1.1 Licenciamento no OpenSDRM

A gestão de licenças no OpenSDRM é disponibilizada através de um mecanismo do lado do cliente, que se materializa através de um agente intermediário de DRM designado por *Wallet*. Esta *Wallet* é capaz de efetuar a gestão e acesso ao conteúdo protegido por diferentes aplicações, autorizando-as a executar determinada ação sobre o conteúdo de acordo com os termos e condições da licença. Esta camada de *software* permite a coexistência de variados tipos de conteúdos protegidos e de aplicações DRM num único sistema cliente (Serrão, 2008). Visto a maior parte dos atuais sistemas serem do tipo vertical (oferecendo uma solução global específica de proteção de conteúdo desde a criação até ao consumo), esta solução, ao permitir a integração de outros módulos externos e ao permitir que várias aplicações de processamento de conteúdo possam partilhar o acesso ao mesmo mediadas pelo Wallet, pode ser classificada como do tipo horizontal (Serrão, 2008; Serrão, Serra, Dias & Delgado, 2006c). Deste modo, o lado cliente passa a contribuir para uma maior interoperabilidade (Figura 17), já que o OpenSDRM pode acomodar diferentes tipos de aplicações cliente.

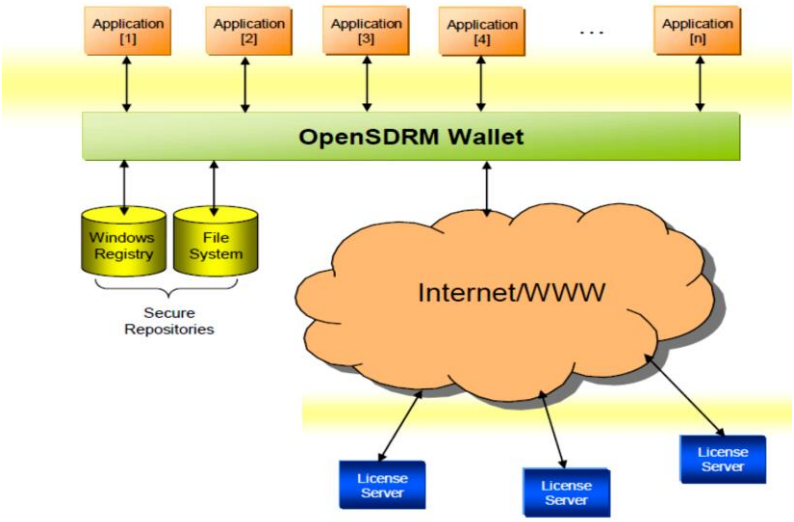


Figura 17 - OpenSDRM Wallet mediação do acesso a licenças (Serrão, et al, 2006c)

Com vista a autenticar a aplicação perante a Wallet no OpenSDRM de modo a que esta possa executar ações sobre o conteúdo num ambiente de confiança mútua, torna-se necessário que a aplicação saiba como executar os seguintes passos:

- Inscrição e pedido de autenticação na Wallet, permutando as credenciais de modo a possibilitar a autenticação da aplicação através do estabelecimento de um canal seguro;
- Solicitar a autorização à Wallet para executar ações sobre o conteúdo nomeadamente a extração do identificador único e o pedido de permissão para usar o conteúdo. A Wallet é também responsável pela obtenção da licença a partir do LIS, por analisá-la e interpretá-la verificando se os direitos nela expressa podem ser aceites ou rejeitados como ações a realizar sobre o conteúdo (OpenSDRM, 2005). Obviamente que a obtenção da chave cifrada que protege o conteúdo com as ferramentas apropriadas de proteção e a sua transmissão à aplicação é um dos passos essenciais que a Wallet tem de tomar em conta (Torres et al., 2008).

No lado do servidor, é ainda possível que um ou mais servidores de licenças possam emitir licenças associadas ao conteúdo e ao utilizador, de modo a que o conteúdo possa ser consumido pelo utilizador consoante o tipo de pedido realizado para poder consumir o conteúdo.

3.2 Open Mobile Alliance (OMA-DRM)

O âmbito de aplicação das especificações OMA-DRM versão 1.0 (OMA, 2004a), visa o estabelecimento de um ambiente propício ao consumo controlado de conteúdos digitais (*media objects*), permitindo aos fornecedores de conteúdo expressar os direitos de utilização (como por exemplo evitar que o conteúdo seja copiado ilegalmente e distribuído a terceiros, permitindo modelos como a superdistribuição (Kawahara, 1990) essencialmente em dispositivos móveis, possibilitando a sua pré-visualização). A versão 2 da OMA-DRM (OMA, 2011a; OMA, 2011b; OMA, 2011c; OMA, 2011e) já estende a versão inicial, permitindo a autorização bilateral entre emissor de direitos e dispositivos baseando-se em certificados e infraestruturas de chave pública e assinaturas sobre as licenças ("*Rights Objects* - RO") (Sumita, Ishikawa & Ueno, n.d.). Esta nova versão permite a possibilidade de partilhar conteúdos dentro de um domínio de dispositivos podendo os RO's ficar ligados ao dispositivo ou a um domínio (Koster, Montaner, Koraichi & Iacob, 2007). Essencialmente é constituída por quatro partes: *Public Key Infrastructure* (PKI) system, *Rights Object Acquisition Protocol* (ROAP), *DRM Content Format* (DCF) and *Rights Expression Languages* (REL). Comparativamente com a versão inicial, o suporte a funções avançadas de segurança baseadas em PKI é a parte principal mais

relevante que foi adicionada, entre outras, (Sumita et al., n.d.), sendo as licenças transferidas de modo mais seguro usando os mecanismos PKI. Contudo, a popularidade desta nova versão do OMA-DRM tem sido bastante reduzida, não sendo alheio a tal a dificuldade de implementação, em larga escala, de um sistema de certificação e autorização baseado em PKI.

Esta versão, inicialmente orientada para a proteção de conteúdos relacionados com o toque de telemóveis (Diehl, 2012; Buhse & van der Meer, 2007), tem sofrido uma enorme evolução baseada nas indicações do mercado, que deram origem a duas subversões (OMA-DRM V2.1.1 e OMA-DRM V2.2). A versão OMA-DRM V2.1.1 (OMA, 2010b) foi aprovada em 2010. As funcionalidades mais diferenciadoras relativamente à versão 2.0 incluem (a) *metering*: recolha de informação sobre a utilização do conteúdo (b) confirmação da instalação de um RO e (c) diferenciação de conteúdos: com este mecanismo uma faixa musical não poderá ser usada como toque de telemóvel. A versão OMA-DRM V2.2 (OMA, 2011e) apareceu em 2011 e suporta novas funcionalidades como a) gestão de anúncios por tipo de aquisição e uso, e b) suporte estendido a jogos e aplicações. As especificações OMA-DRM v2 definem o formato e o mecanismo de proteção do conteúdo e da licença, assim como o modelo de segurança para a gestão das chaves de cifra/decifra (Diehl, 2008). Além disso, também definem como os conteúdos e licenças são transportados para os dispositivos através de vários mecanismos mas não abrangendo as interações entre as entidades de rede. Apesar de se direcionar para o mercado dos dispositivos móveis, existem tentativas de aplicar este tipo de sistema a outros ambientes como o das *set top boxes* (Rosenblatt, 2009). Este sistema está contudo orientado para este tipo de ambiente muito específico, não oferendo funcionalidades suficientemente flexíveis para a gestão de licenças em todos os domínios, sendo esta uma condicionante da sua interoperabilidade.

3.2.1 Arquitetura OMA DRM

Do ponto de vista estrutural a norma OMA-DRM define um conjunto de atores e componentes na sua arquitetura de referência. Os mais relevantes são: DRM Agent (DRM-A), Content Issuer (CI), Rights Issuer (RI), Utilizador e dispositivo de armazenamento.

- O DRM-A representa a entidade de confiança no dispositivo. Esta entidade tem por obrigação assegurar que os direitos de PI sejam aplicados sobre o conteúdo controlando o acesso e uso sobre o mesmo.
- O CI envia o conteúdo para que este seja formatado e preparado para ser recebido pelo DRM-A. Também define a forma como o conteúdo pode ser transportado do CI para o

DRM-A usando mecanismos de transporte alternativos. O empacotamento do conteúdo pode ser realizado diretamente pelo CI ou este pode recebê-lo de uma entidade externa.

- O RI é a entidade que atribui permissões e condições ao conteúdo e gera o RO. Este é representado em XML e expressa as permissões e restrições, através de uma REL, associadas ao conteúdo.
- O utilizador é um indivíduo que faz uso do conteúdo a que acede através do DRM-A. O dispositivo do utilizador permite que o conteúdo seja armazenado mesmo quando este está desligado. O sistema OMA DRM habilita o CI a distribuir o conteúdo protegido e habilita o RI a emitir RO do conteúdo protegido. O sistema é independente do formato do conteúdo, sistema operativo e ambiente de execução. Para o utilizador consumir o conteúdo deve contactar o RI para adquirir os respetivos direitos (Sumita et al., n.d.). O RI concede as permissões adequadas para o conteúdo protegido, sob a forma de RO ligado de forma criptográfica ao dispositivo do utilizador. Uma vez que o conteúdo está protegido usando criptografia, ao ser distribuído só poderá ser usado com o RO que lhe está associado e que foi emitido pelo RI (Diehl, 2012).
- O dispositivo de armazenamento permite que o utilizador possa armazenar o conteúdo e executar as operações necessárias para que o conteúdo protegido possa ser acedido e utilizado de acordo com os termos e condições expressos no RO previamente obtido.

Na versão OMA-DRM 2 o emissor de conteúdo empacota e protege o conteúdo, encriptando-o com uma chave simétrica do tipo AES a 128-bit AES (C_{EK}) (Diehl, 2012; Patriciu et al., 2011). O RI descreve os direitos de utilização associados ao conteúdo através de ODRL em concordância com a definição do detentor de direitos. Estes direitos de utilização são empacotados com a C_{EK} num objeto de direitos. Este objeto está ligado, usando criptografia, ao conteúdo que especifica e fica associado a um DRM Agent a que está endereçado (Diehl, 2012). Apesar do conteúdo poder ser distribuído de forma descentralizada, o mesmo já não acontece com o RO, pois este é gerado e distribuído pelo RI de uma forma controlada. O sistema OMA-DRM não obriga a que o conteúdo e o RO tenham de estar agregados podendo ser enviados ao dispositivo conjuntamente ou em separado (Sumita et al., n.d.)

O DRM Agent é uma entidade de confiança que é executada no dispositivo recebendo o conteúdo e a licença (Diehl, 2012). Todo o DRM Agent possui um par de chaves pública/privada conjuntamente com um certificado emitido pela autoridade. Este certificado transporta igualmente informação sobre as características do DRM Agent (Diehl, 2012). Baseado nisso, o emissor de direitos pode decidir se aceita a emissão de uma licença. Além

disso, o emissor de direitos encripta a licença somente para o DRM Agent definido, assinando todas as licenças que emite (Diehl, 2008).

Adicionalmente à definição da proteção do conteúdo, o OMA-DRM também define a forma como os objetos DRM são enviados aos dispositivos. Para tal no OMA-DRM v2 é definido o conceito de domínio que permite a partilha de conteúdo entre terminais móveis e outros terminais como os PCs (Sumita et al., n.d.). O RI mantém o controlo sobre os ROs a serem partilhados num domínio e gere as subscrições dos terminais nesse domínio baseando-se num conjunto de protocolos de nome *Rights Object Acquisition Protocol* (ROAP) (Sumita et al., n.d.). O ROAP é o nome comum para um agregado de protocolos de segurança a implementar entre o RI e o DRM Agent no dispositivo (Sumita et al., n.d.). A emissão de ROs para o domínio e a permuta de mensagens envolvidas na subscrição do domínio são realizadas utilizando o ROAP. Este protocolo fornece várias funcionalidades relacionadas com a segurança, incluindo a transmissão de ROs, confidencialidade de dados, autenticação mútua baseada em PKI, sincronização e revogação de certificados digitais. É constituído por três tipos de protocolos relacionados (Sumita et al., n.d.) com:

- registo do dispositivo do(s) utilizador(es);
- pedido e aquisição do objeto de direitos;
- junção ou abandono de um domínio.

O ROAP é descrito em XML, recorrendo-se à XML Encryption, para garantir a confidencialidade de dados, e à XML Signature para possibilitar a autenticação mútua. Além disso, algoritmos já testados, como o RSA e Secure Hash Algorithm 1 (SHA-1), são aqui utilizados para garantir a confidencialidade e autenticação (Sumita, Ishikawa & Ueno., n.d; Diehl, 2012).

A função domínio é uma das funcionalidades da versão OMA-DRM v2.0 que permite a partilha de conteúdo entre dispositivos respeitando os limites da utilização pessoal. O RI define o domínio, gere as chaves e controla os dispositivos que podem aceder ao domínio mantendo os RO's para serem partilhados dentro do domínio. Cada chave de domínio corresponde à geração de um domínio específico (Sumita et al., n.d.). A emissão de ROs para o domínio, o registo de dispositivos e a troca de mensagens envolvidas na subscrição são executadas através do ROAP (Diehl, 2012; Lee, Lee & Shin, 2007).

Ao tentar aceder ao conteúdo protegido, o DRM Agent acede à respetiva licença associada (só o pode fazer se possuir a licença gerada especificamente para si) (Diehl, 2012). A camada de

gestão de direitos interpreta então a expressão ODRL inserida na licença e extrai as permissões e restrições. Ao mesmo tempo passa a C_{EK} para a camada de proteção de conteúdo que desencripta o conteúdo fazendo então com que o conteúdo possa ser utilizado, mas assegurando a aplicação dos direitos em conformidade com o expresso na licença (Diehl, 2012). Os passos para distribuir conteúdos são descritos em (OMA, 2011d).

O conteúdo é encriptado e empacotado num formato específico OMA-DRM (DRM Content Format - DCF) e só pode ser usado tal como foi especificado no RO (Sumita, Ishikawa & Ueno, n.d.). Para tal o sistema incorpora um mecanismo que permite ao DRM Agent verificar a integridade do DCF, permitindo assim detetar possíveis modificações não autorizadas desse conteúdo (Rodríguez, Gallego & Delgado, 2007c).

Os ROs são usados para especificar as regras de consumo do conteúdo, sendo a sintaxe e a semântica das permissões e restrições expressas através de uma REL (ODRL) em formato XML (Sumita et al., n.d.). Estas permissões e restrições, conjuntamente com outra informação relevante, serão apresentadas ao utilizador. Além disso, o RO também governa o acesso ao conteúdo pois inclui a C_{EK} que encripta/desencripta o conteúdo. Um RO simples pode estar associado a múltiplas peças de conteúdo, sendo assim possível atribuir diferentes permissões a diferentes componentes de um objeto compósito.

O RO é protegido usando a chave de cifra de direitos (R_{EK}). Como a chave que cifra o conteúdo, $C_{EK,}$ está inserida no RO, acaba por também ficar protegida com a R_{EK} conjuntamente com outra informação. A R_{EK} fica ligada através de criptografia ao DRM Agent, de modo a que somente este possa aceder ao C_{EK} e consequentemente ao conteúdo (Rodríguez, Gallego & Delgado, 2007c). Para garantir a integridade do RO, este é assinado pelo RI (Rodríguez, Gallego & Delgado, 2007c). Sendo o conteúdo protegido inerentemente seguro, este pode estar armazenado em qualquer lugar fora do dispositivo. O mesmo se poderia dizer do RO, mas algumas permissões requerem a manutenção do estado pelo DRM Agent, (como, por exemplo, o número de reproduções). Os RO's contendo tais permissões não podem ser copiados ou armazenados fora do dispositivo pois isso resulta na perda da informação sobre o seu estado (como, por exemplo, o número de reproduções) (OMA, 2011d).

A seguinte descrição explica os detalhes dos procedimentos simples de aquisição de conteúdo como, por exemplo, um descarregamento (*download)* simples ou o de super-distribuição no OMA-DRM (Sumita et al., n.d.).

No caso de "download simples", o conteúdo encriptado e protegido e os ROs são obtidos diretamente de um fornecedor de conteúdos (por exemplo considere-se o caso de um utilizador que paga para fazer o *download* de uma faixa de música – aquisição do RO - e que depois a começa a ouvir). O dispositivo adquire o conteúdo encriptado no formato DCF (Figura 18 (1)). Se o CI e o RI estiverem implementados em componentes distintos, torna-se necessário um procedimento adicional entre eles para a partilha da chave que protege o conteúdo (Figura 18 (2)). De seguida, o dispositivo adquire o RO a partir do RI com vista a poder começar a usar o conteúdo (Figura 18 (3)). Para este processo é utilizado o ROAP na aquisição do RO, assim como a cifra do RO como contramedida de possíveis falsificações e autenticação mútua entre o dispositivo e o RI como contramedida de *spoofing* (Sumita et al., n.d.).

No caso da superdistribuição, o conteúdo é encriptado e formatado com base no formato DCF, podendo ser duplicado e distribuído livremente a outros (por exemplo, um utilizador pode dar a sua música a um amigo através de email ou Bluetooth (Figura 18 (4)). Se o recetor do conteúdo quiser ouvir a música terá de adquirir um RO do RI e pagar o estipulado (Figura 18 (5)). O ROAP é usado para a aquisição de ROs tal como no *download* simples (Sumita et al., n.d.). Os utilizadores podem fazer um *preview* do conteúdo adquirindo RO específicos antes de adquirir o RO definitivo (Sumita et al., n.d.).

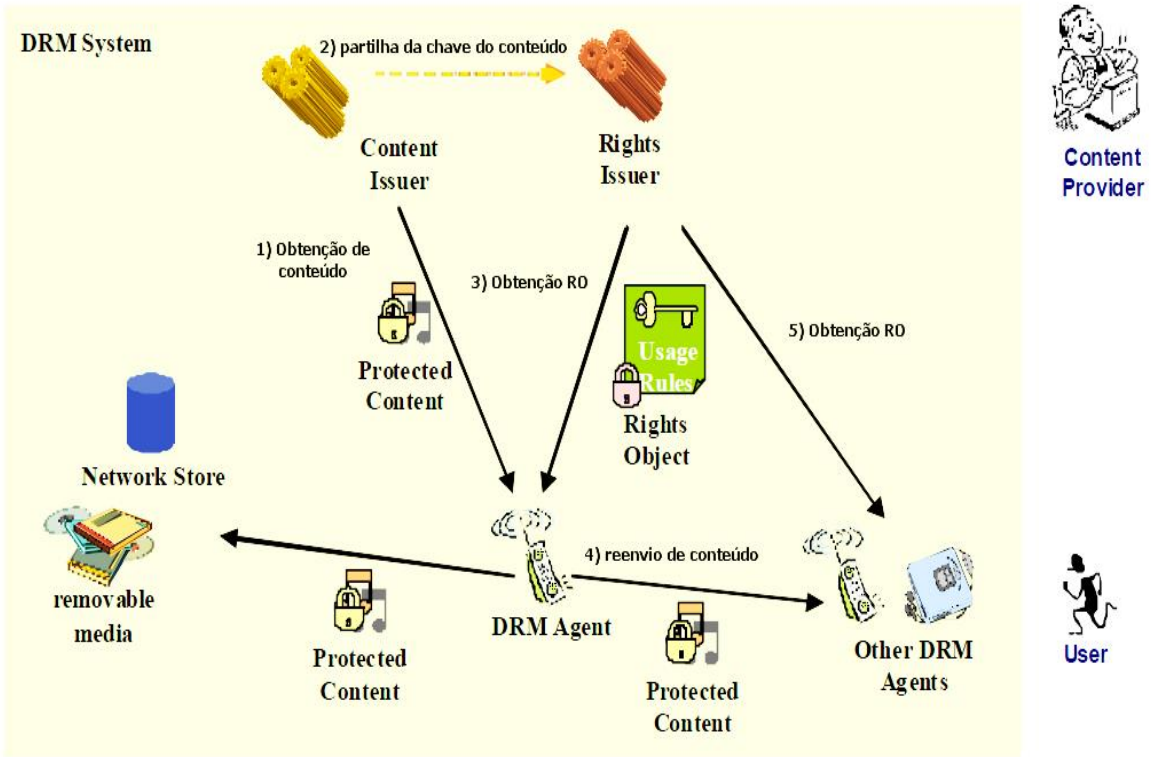


Figura 18 – Arquitetura funcional de OMA-DRM (adaptado de OMA, 2011d)

3.3 MIPAMS

O sistema MIPAMS (*Multimedia Information Protection and Management System*), está orientado a serviços de gestão e distribuição de conteúdos seguros e foi desenvolvido por DMAG-UPC (*Distributed Multimedia Applications Group, Universitat Politècnica de Catalunya*). O MIPAMS vai ao encontro de uma parte importante da cadeia de valor, desde a criação e distribuição de conteúdo até ao consumo pelos utilizadores finais, baseando-se numa abordagem orientada a serviços *Web* que dá corpo à sua arquitetura (Serrão, Rodriguez, & Delgado, 2011). Consiste de vários módulos e serviços, fornecendo uma enorme variedade de funcionalidades necessárias à governação e proteção de conteúdos (Delgado, Torres, Llorente & Rodríguez, 2011). Vários módulos estão incorporados na sua arquitetura disponibilizando cada um deles partes das funcionalidades. Para suportar toda a infraestrutura, a arquitetura faz a distinção entre o utilizador final e os servidores necessários (Delgado, Llorente & Rodriguez, 2012) e, ao recorrer a uma abordagem modelar dos seus componentes, permite a adição de novos módulos à medida que estes são necessários. A Figura 19 ilustra os componentes básicos e os serviços presentes.

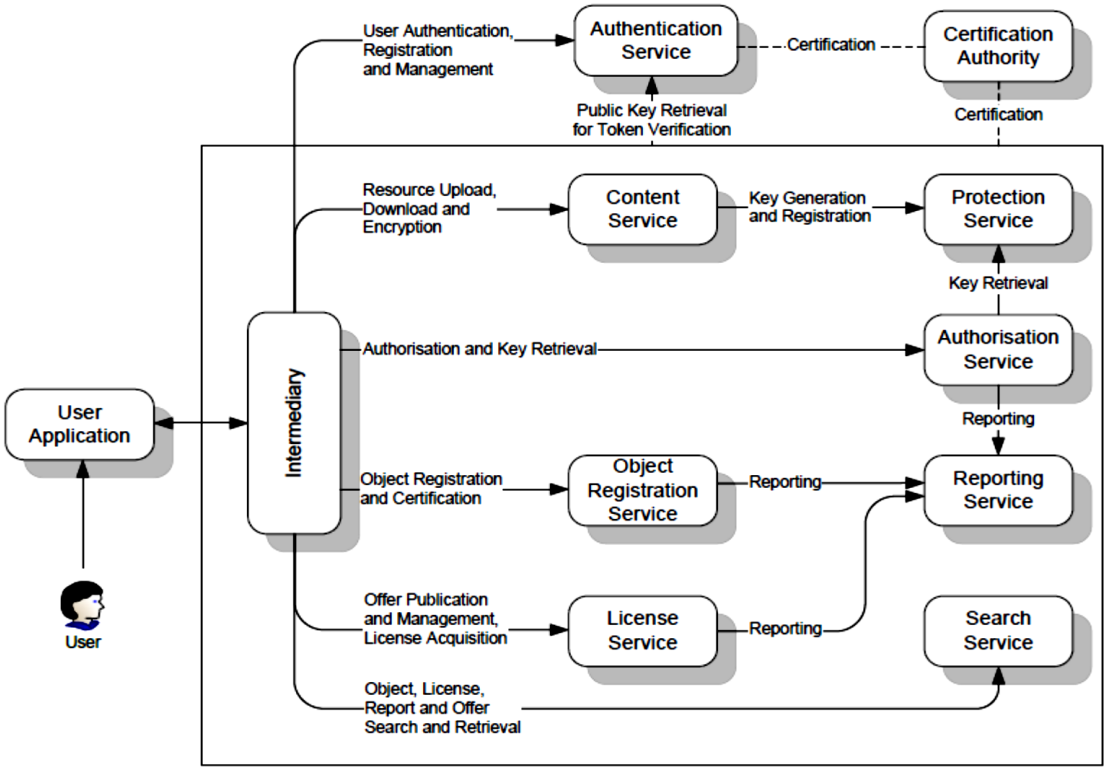


Figura 19 – Arquitetura da plataforma MIPAMS (Delgado et al., 2005b)

De uma forma sucinta, as funcionalidades de cada componente representado na arquitetura são as seguintes (Delgado et al., 2005b; Delgado, Llorente & Rodriguez, 2012):

- O *Content Service* (CS) permite às aplicações fazerem o *upload* e *download* do conteúdo. O conteúdo pode ser opcionalmente encriptado a pedido e conforme os mecanismos de encriptação disponíveis. Se for selecionada a encriptação, então serão pedidas as chaves de proteção ao *Protection Service* e registadas através deste serviço no decorrer da encriptação. O carregamento de conteúdos requer que o conteúdo seja identificado única e inequivocamente.
- O *Object Registration Service* (ORS) permite o registo de representações digitais (objetos digitais) dos conteúdos e metadados associados. Esta informação é empacotada usando o formato MPEG-21 Digital Item XML-based format (MPEG-21:DID, 2005). O *Object Registration Service* regista e assina digitalmente objetos de modo a ser possível verificar a sua autenticidade e integridade. Fornece também o identificador único para carregar os conteúdos no CS.
- O *Authorization Service* (AS) verifica se o utilizador possui uma licença apropriada que lhe conceda o direito de executar a ação pretendida sobre o conteúdo de acordo com o mecanismo definido. O AS partilha o acesso ao repositório das licenças com o *License Server*. Caso o utilizador esteja habilitado a realizar uma ação sobre o conteúdo e este estiver encriptado então o AS recupera as chaves de encriptação do *Protection Service* e envia-as à aplicação que as requereu, sendo esta a única forma de aceder às chaves de encriptação.
- O *Protection Service* (PS) é responsável por gerar as chaves de encriptação a pedido, registar as chaves de encriptação associadas ao conteúdo unicamente identificado e fornecer as chaves de encriptação para o conteúdo protegido para o AS. Ao utilizar os esquemas e descritores da norma MPEG-21 IPMP (MPEG-21:IPMP, 2006), o PS acaba por oferecer a possibilidade de descarregar as ferramentas de proteção que foram usadas e que agora podem ser utilizadas pelas aplicações.
- O servidor *License Service* (LS) lida com a oferta de direitos e emissão de licenças. As ofertas de direitos são disponibilizadas pelos criadores de conteúdos/detentores de direitos após registarem o conteúdo no sistema. A emissão de licenças refere-se ao processo pelo qual a licença é gerada como consequência do ato de aquisição de direitos, ou pela atribuição de concessão de direitos a terceiros pelo detentor. As licenças são aqui expressas usando a REL MPEG-21 *Rights Expression Language* (MPEG-21:REL, 2005).
- A *User Application* (UA) consiste num reprodutor (*player*), ferramenta de edição, *browser* ou outro meio gerido pelo utilizador para lidar com as funcionalidades de DRM, como o

registo e acesso a conteúdo protegido. De modo a garantir confiança, o UA possui um módulo interno que consiste de um repositório local de licenças seguro, informação de proteção e outra informação relacionada. Dependendo do caso, poderá estimar o *fingerprinting* de conteúdos, desproteger o conteúdo, realizar autorizações, rastrear operações e gerir a informação sobre a proteção do conteúdo.

- O *Intermediary* (I) atua como um gestor mediador de fluxos e pode ser uma parte integral da UA ou ficar localizado no lado do servidor de modo a reduzir-se a complexidade do UA. (e.g. *Web* portal, *brokerage* service). Pode ser visto como um intermediário a quem o UA requer que a execução de várias operações sejam realizadas, tais como o registo de objetos, o *upload* de conteúdos, aquisição de licenças, …etc.
- O *Search Service* (SS) permite às aplicações executarem pesquisas através dos metadados do sistema MIPAMS, atuando assim como o *frontend* para pedir qualquer informação (conteúdos, licenças,…etc.) presente nas bases de dados do MIPAMS.
- O *Reporting Service* (RS) colige os relatórios de utilização relativos ao registo de objetos, emissão de licenças e das autorizações concedidas, podendo atuar como gerador de relatórios do tipo MPEG-21 Event Report (MPEG-21:ER, 2006) utilizados com o fim de gerar estatísticas e/ou rastreio.
- O *Authentication Service* (ATS) é necessário para autenticar a identidade dos utilizadores. Ao gerar *tokens* SAML (Security Assertion Markup Language) que permitem identificar os utilizadores MIPAMS e assinando-os digitalmente tem uma forma de garantir ao sistema a autenticidade e integridade destes garantindo assim a autenticação correta dos utilizadores. Além disso, o ATS permite também o registo e gestão de dados do utilizador (por exemplo, desativação de conta, modificação de dados pessoais…etc.)
- A *Certification Authority* (CA) é a entidade reconhecida por todos que garante a confiança ao global no sistema, emitindo certificados aos diversos componentes e atores que fazem parte da arquitetura sob a forma de certificados X.509 e de chaves privadas.

3.3.1 Protocolos envolvidos

Em qualquer sistema distribuído é importante dar especial atenção à comunicação entre as diversas entidades, a qual deve ser segura entre as partes envolvidas. No MIPAMS é não só importante assegurar a permuta segura de conteúdos e de licenças mas também das ferramentas de proteção e adaptação do conteúdo e da informação necessária à transação. Para isso, as várias entidades que providenciam os serviços de comunicação fazem-no através de canais de segurança que utilizam o protocolo SSL/TLS, o que acaba por assegurar uma maior segurança

no decorrer da transmissão/receção de dados (Torres, Rodríguez, Llorente & Delgado, 2004). Para que os componentes possam trocar informação, faz-se recurso a serviços *Web*, implementados no sistema através do protocolo SOAP.

3.4 OpenIPMP

O OpenIPMP é um projeto de código aberto desenvolvido pela empresa Objectlab (OpenIPMP, n.d.), baseado na família de *normas* MPEG, infraestruturas de chave pública (PKIs), Digital Object Identifier (DOI) para identificação de conteúdos, e na linguagem ODRL para expressão de direitos. O OpenIPMP implementa uma solução de DRM completamente funcional com o suporte a encriptação/desencriptação de conteúdos, gestão de licenças, identificação de conteúdos e de gestão de utilizadores. O OpenIPMP tal como definido pela ObjectLab "é uma coleção de ferramentas/serviços capazes de assistir uma infraestrutura robusta, escalável e adaptativa capaz de suportar a gestão e envio/entrega segura de bens digitais ao longo de todo o ciclo de vida do conteúdo" (OpenIPMP). A comunicação entre os componentes da sua arquitetura é realizada através de serviços *Web* (Figura 20).

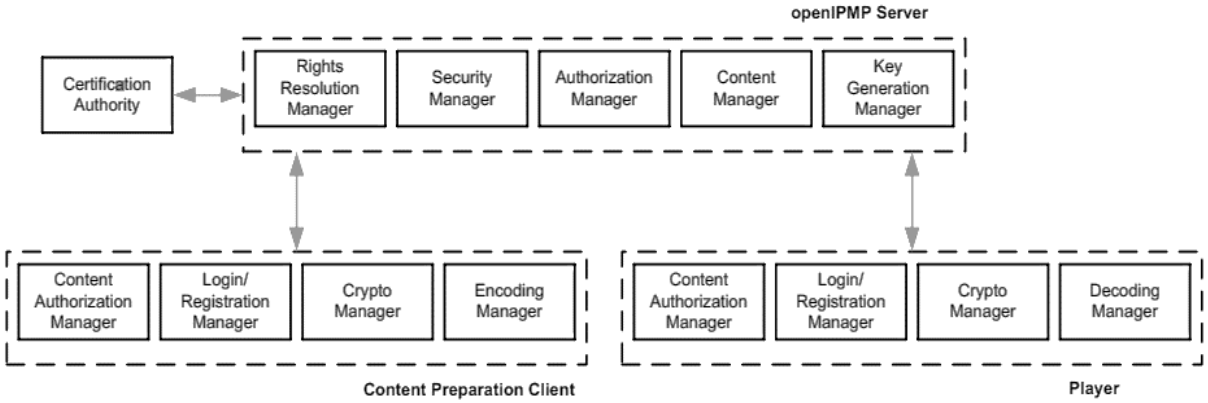


Figura 20 - Arquitetura OpenIPMP (Serrão, Marques, Dias, & Delgado, 2006b)

O sistema OpenIPMP engloba a gestão de utilizadores e sua identificação, a aplicação de algoritmos de encriptação do conteúdo e a proteção do canal de distribuição. O seu desenho é baseado num conjunto de normas abertas tais como o OMA-DRM v2.0 (OMA, 2011e), no "*Internet Streaming Media Alliance (ISMA) Encryption and DRM signaling* (ISMACrypt)" (Koenen, 2002) e especificações MPEG4 (MPEG-4:IPMP-X, 2005). Para a proteção de conteúdos existem dois tipos de algoritmos de encriptação disponíveis: se o conteúdo for distribuído por difusão (*streamed*) a encriptação utilizada é ISMACrypt ou a cifra DVB-CSA, mas se o conteúdo for distribuído com base num conteúdo estático do tipo ficheiro, a cifra utilizada pode usar criptografia AES ou *Blowfish Block Cipher* (BBC) (Schneier, 2007). Os conceitos chave por trás do OpenIPMP estão relacionados com (Chiariglioni, 2008):

- Gestão de direitos: o sistema permite múltiplas formas de definição e aplicação de direitos de utilização, sendo as linguagens de expressão de direitos suportadas a MPEG-21 REL e a ODRL,
- Gestão de utilizadores: o sistema emite a cada utilizador um certificado digital que o identifica ao registar-se; esse certificado é emitido e assinado pela Autoridade de certificação do OpenIPMP,
- Gestão e identificação do conteúdo: logo após a criação e upload para o sistema, o conteúdo é identificado, gerido e monitorizado ao longo do seu ciclo de vida.
- Proteção de conteúdo – na proteção do conteúdo o sistema adota vários normas criptográficas abertos como PKI, certificados X.509, criptografia de chave simétrica e assimétrica, SSL e armazenamento seguro (RSA Security PKCS#12).

Em termos operacionais, diferentes conjuntos de componentes OpenIPMP podem combinar-se ou interagir dando origem a um conjunto de ferramentas ou serviços. Contudo, e apesar de estar disponibilizada sob o regime de código aberto., o número de soluções conhecidas deste tipo com aplicação é praticamente inexistente. Apesar da sensatez das tecnologias escolhidas e independentemente da reduzida documentação sobre a implementação do sistema, o seu maior problema está na inexistência de uma especificação sobre o seu código aberto (Chiariglioni, 2008).

3.5 DReaM

Resultante de uma iniciativa da Sun Microsystem com vista ao desenvolvimento de uma solução baseada em normas abertas, o projeto DReaM (*DRM everywhere available*) (Fernando, Jacobs & Swaminathan, 2005) tem por base um conjunto de especificações de interoperabilidade do projeto Opera Eurescom (Wegner, 2003). A sua estrutura arquitetónica suporta a separação entre a gestão de direitos, a autenticação e identificação de utilizadores, licenciamento, a aplicação de direitos, e sistema de proteção (Fernando et al., 2005; Serrão et al., 2006). Esta separação torna possível a escolha e seleção independente de várias tecnologias sem comprometer a solução global. São de considerar dois elementos chave: um é separação da gestão de direitos do sistema de proteção de conteúdos e outro a separação dos serviços de identificação e autorização dos dispositivos de *hardware* do utilizador. Tendo como objetivo central a criação de um sistema DRM interoperacional, capaz de se relacionar com outros sistemas e tecnologias de proteção o DReaM também pretendia suportar conjuntamente serviços de acesso condicionado acabando por permitir a coexistência de instâncias múltiplas

de componentes relacionados com a proteção de conteúdos (*player*, licenciador e empacotador) e componentes não específicos de proteção de conteúdos (Patriciu et al., 2011). Contudo, atualmente, este projeto não apresenta qualquer atividade (DReAM).

3.6 Marlin

A iniciativa Marlin baseia-se em normas abertas e teve desenvolvimento a partir da *Marlin Developer Community* (MDC) com o objetivo de criar uma plataforma interoperável para os grandes produtores de conteúdos. Baseia-se em projetos anteriores, como o Nemo e o Octopus (MDC, 2006), e possibilita a implementação de um conjunto de funcionalidades relacionadas com gestão do relacionamento entre serviços, redes, e conteúdo digital. Ao basear-se no projeto Octopus herda a característica principal da sua arquitetura, que é a gestão de direitos centrados no utilizador, a qual é diferenciadora de outras arquiteturas DRM existentes mais centradas no dispositivo; isto significa que o conteúdo está ligado ao utilizador e não ao dispositivo (MDC, 2006). Apesar de estar mais orientada para a área comercial e baseando-se numa arquitetura generalista e bastante expressiva, a gestão de direitos no Marlin baseia-se no Octopus DRM *engine* (MDC, 2006), o que o torna muito flexível pois permite a implementação de vários modelos de utilização suportados sobre um modelo de grafos (MDC, 2006). Esta flexibilidade é viabilizada por *tokens* (*action* e *conFiguration tokens*) gerados por um servidor de e-commerce a pedido de um cliente DRM que o habilita a pedir licenças. É suportado por quatro tipos de objetos (conteúdo, licença, nó e ligação) onde o nó pode representar um dispositivo, utilizador, domínio ou subscrição e a ligação entre nós representa a ligação. Assim, os objetos de um nó representam entidades do sistema (dispositivos e utilizadores) e as ligações entre nós representam as relações. Cada nó possui propriedades criptográficas (por exemplo, chaves podem ser partilhadas com outros nós - chaves de partilha) e as chaves que devem permanecer secretas ao nó (chaves de confidencialidade) (MDC, 2007; Keoh, 2011). Na ligação entre dois nós, esta pode ser descrita como representativa de um nó como "pertencendo a" ou "é membro de". Por sua vez, a ligação também tem propriedades criptográficas e é um objeto auto protegido que não pode ser falsificado podendo haver um objeto *control* associado à ligação para assegurar a aplicação de condições nesta (Keoh, 2011). Um utilizador pode usar um conteúdo obtido em dispositivos múltiplos e um dispositivo pode ter vários utilizadores. A relação entre utilizadores e dispositivos é mencionada usando os nós e as ligações diretamente através de um grafo. Uma ligação de um dispositivo para um utilizador implica que o dispositivo esteja associado ao utilizador. Fornecendo a flexibilidade de ligar licenças a qualquer nó, um conteúdo ligado a um nó implica que o mesmo só pode ser reproduzido nesse dispositivo em particular,

enquanto uma ligação a um domínio e utilizador permite ao dispositivo que pertence ao domínio ou a dispositivos que foram ligados à conta do utilizador consumir o conteúdo. A ligação ao nó de subscrição implica que somente utilizadores com uma subscrição no serviço possam reproduzir o conteúdo no dispositivo ligado à sua conta de utilizador. Baseado na ligação, determina como a chave de encriptação do conteúdo é acomodada na licença (a chave do conteúdo é encriptada com a chave pública do nó a que está ligado). Esta licença contém quatro componentes: chave do conteúdo, protetor, controlador e controlo (Keoh, 2011). A relação entre estes componentes é ilustrada na Figura 21.

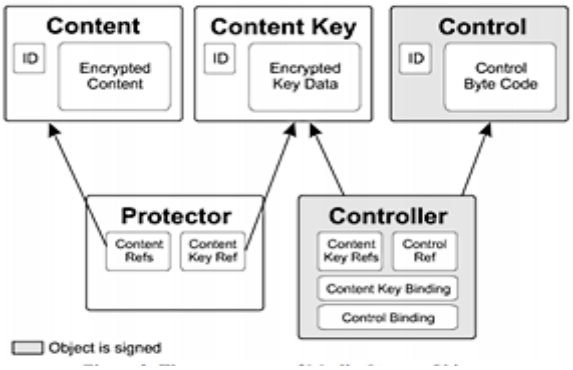


Figura 21 – Componentes do objeto licença Marlin (Keoh & Vrielink, 2009)

O componente de controlo na licença objeto é composto por rotinas executáveis codificadas que verificam as permissões e regras de utilização. Para assegurar a sua integridade o objeto é assinado pelo detentor de conteúdo e toda execução é realizada numa máquina virtual de nome *plankton* onde todas as instruções são processadas. A avaliação das regras de utilização requer o armazenamento seguro de valores em locais seguros e que possam ser lidos ou gravados mais tarde (Keoh, 2011). Para tal existe um local persistente de armazenamento, o *seashell*, que permite ao sistema Marlin gerir o tempo de vida dos dados e as suas políticas de acesso. Por defeito, as rotinas de controlo só podem aceder aos dados cujo detentor é o mesmo que o autor do componente de controlo de onde o código foi carregado (Keoh, 2011).

Sendo um objetivo claro do sistema Marlin deixar que o utilizador tome o controlo do conteúdo, tal leva à centralização da gestão de direitos no utilizador (Kamperman, Szostek & Baks, 2007), dando-se assim mais flexibilidade de dar esse conteúdo a terceiros e de adicionar um dispositivo em qualquer altura, dependendo tal da conveniência do utilizador. A proteção e a gestão de direitos são realizadas da mesma maneira que em outros sistemas de DRM, isto é, usando controladores DRM e licenças. Para determinar se um cliente tem direitos sobre um conteúdo protegido, o Marlin calcula uma série de ligações que conectam o utilizador à subscrição (Keoh & Vrielink, 2009). Ao adquirir conteúdo o cliente Marlin é instruído a pedir o nó do utilizador

correspondente, e o nó da ligação. A responsabilidade de criação de ligações é atribuída ao sistema de comércio eletrónico que está implementado como serviço Marlin. O direito de consumir conteúdo Marlin protegido é avaliado determinando se o nó conteúdo é alcançável pelo nó do utilizador (MDC, 2006). Os principais componentes da arquitetura Marlin são ilustrados na Figura 22.

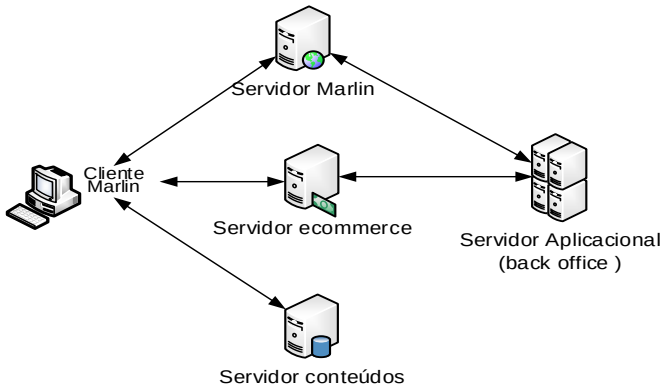


Figura 22 - Componentes e arquitetura Marlin (adaptado de MDC, 2007)

O conteúdo a ser protegido é encriptado com uma chave aleatória (chave do conteúdo) originando o objeto conteúdo. Os direitos associados são convertidos no programa de controlo. Este define o destino do conteúdo objeto e verifica se o nó correspondente possui as ligações necessárias para atingir os nós requeridos. A chave do conteúdo está ligada ao nó, assim como o programa de controlo está ligado ao nó Octopus. A licença Marlin possui a chave encriptada do conteúdo, o programa de controlo encriptado e a assinatura do programa de controlo (por exemplo HMAC). Quando o cliente Marlin recebe uma licença verifica se a mesma está ligada ao nó em causa. Se a verificação for positiva, o cliente desencripta o programa de controlo e passa-o a uma máquina virtual. O programa de controlo verifica o destino do objeto conteúdo, isto é, até que ponto os nós a que são direcionados são alcançáveis por este nó. De seguida, o cliente DRM desencripta a chave que protege o conteúdo e descodifica o conteúdo objeto.

Estando orientada para dispositivos eletrónicos de consumo doméstico, o Marlin assume que o cliente DRM é executado num ambiente "fechado" e controlado, sendo por isso de maior confiança do que os sistemas que são executados em computadores de arquitetura aberta (Diehl, 2012). Consequentemente pressupõe-se que a confiança entre as partes é mais robusta, pois é assumido que os sistemas baseados em *hardware* garantem uma maior proteção das chaves secretas do que os baseados nas técnicas de obscuridade por *software* (Diehl, 2012). O seguinte conjunto de especificações é usado pelo Marlin (MDC, n.d.):

- *Marlin Core System Specification* define os elementos comuns de base (componentes, protocolos e domínio) e as suas interações ao nível mais elevado que permitem a interoperabilidade entre os dispositivos e os serviços Marlin.
- *Marlin Broadband Delivery Specification* define capacidades adicionais dos dispositivos que suportam a Internet, como por exemplo a obtenção de licenças *online*.
- *OMarlin Specification* define a interoperabilidade entre OMA-DRM e o Marlin, com vista à partilha de conteúdos em dispositivos móveis que suportam a norma OMA-DRM.
- *Marlin IPTV End-point Services Specification* define o comportamento de IP TV *sets*.
- *Marlin Common Domain Specification* define a implementação de "domínio autorizado", ou seja como é efetuada a gestão dos dispositivos domésticos de rede.
- *NEMO* framework (Networked Environment for Media Orchestration).

Uma das vantagens do Marlin reside na flexibilidade dada ao utilizador que lhe permite a) transmitir o conteúdo a terceiros, b) associar conteúdo a outro domínio, e c) dar autorização temporária permitindo aceder ao conteúdo a partir de um dispositivo fora do domínio. Esta flexibilidade proporcionada pelo Marlin é bastante desejável pelos utilizadores pois aumenta-lhes a sua mobilidade (Kamperman et al., 2007). A arquitetura Marlin, ao incluir uma *gateway* OMA-DRM, permite habilitar os clientes Marlin a comportarem-se como DRM Agents, o que vai ao encontro das exigências necessárias para que estejam satisfeitos os requisitos de um DRM Agent (Patriciu et al., 2011). Perante tal situação, o conteúdo em conformidade com OMA-DRM pode ser recebido, processado e consumido tal como se estivesse a utilizar um dispositivo em conformidade com o OMA-DRM, não sendo necessário efetuar qualquer alteração no emissor de direitos OMA (Patriciu et al., 2011). A estrutura do ficheiro OMArlin permite conter um objeto de direitos OMA e uma licença Marlin, assim como a informação relacionada que permita a obtenção da licença no formato requerido (Yuan, Zhao, Zhang & Tian, 2012). Contudo, o OMArlin somente é aplicável aos sistemas que suportem as especificações OMA e Marlin.

4 Resumo das características primárias das soluções

Depois de se analisar cada uma das soluções é possível concluir que a maioria envolve quase sempre os mesmos participantes básicos com operações bastante similares, sendo por isso aparente que seguem um fio condutor. Para melhor se perceber as soluções DRM apresentadas,

é de seguida apresentado uma lista não exaustiva[6], que tenta capturar as suas principais caraterísticas base, independentemente do sistema operativo que as suportam. Na Tabela 4 faz-se uma análise das principais características fundamentais (regras de utilização e outras) que as diferenciam.

Regras de utilização:	OpenSDRM	OMA	MIPAMS	OpenIPMP	Marlin
Suporte a múltiplos dispositivos	√	√	√	√	√
Envio de licenças em separado	√	√	√	√	√
Envio de licenças embebidas	√	√	√	-	√
Licenças ligadas a dispositivos	X	√	X	-	X
Licenças ligadas ao utilizador	√	X	√	√	√
Licenças ligadas a domínio	X	√	X	X	X
Formato de ficheiro	Vários	DCF	Vários	MPEG-4 MPEG-2	Vários
Mecanismo transporte	Download Streaming	Download Streaming	Download Streaming	Download Streaming	Download Streaming
Superdistribuição	√	√	√	√	√
Validade temporal da licença	√	√	√	-	√
Pay per view	√	√	√	-	√
Subscrição	√	√	√	-	√

Caraterísticas adicionais:	OpenSDRM	OMA	MIPAMS	OpenIPMP	Marlin
Documentação	√	√	√	√	√
Código aberto	√	X	parcial	√	X
Autenticação	√	√	√	√	√
Ferramentas de proteção adicionais (watermarking, …)	√	-	√	-	-
Pagamentos	√	X	√	X	X
Plugin do *Web* browser	√	X	√	-	X

Tabela 4 – Características fundamentais de soluções abertas de DRM

As soluções DRM aqui analisadas partilham de um modo genérico as mesmas características: as suas especificações são de domínio público e disponibilizam interfaces documentadas e são acessíveis publicamente (Torres et al., 2008). A plataforma Marlin encontra-se largamente

[6] Visto o DReaM não ter atualmente qualquer atividade não o iremos considerar nesta análise.

implementada em dispositivos orientados para consumo doméstico (por exemplo na Playstation 3) e serviços, essencialmente os de TV baseados na Internet (Keoh, 2011). Contudo, muita da tecnologia está patenteada pela Intertrust, tal como o OMA-DRM, requerendo a sua utilização o investimento adicional em *royalties* a pagar para realizar uma implementação legal. Relativamente ao OMA-DRM é de notar que muitos operadores de telecomunicações da área dos telemóveis a utilizam (essencialmente a versão 1.0). O OpenIPMP, apesar de estar disponível como de código aberto.[7], disponibiliza documentação bastante reduzida o que limita a sua viabilidade de implementação. O OpenSDRM e o MIPAMS são essencialmente usados pela comunidade académica, não sendo a tal estranho o facto de terem concorrido e recebido financiamento público da União Europeia. Quer uma quer outra têm evoluído com o tempo e o OpenSDRM converteu-se num projeto de código aberto.[8], o que abona a seu favor. Sendo a segurança um aspeto chave a ter em conta nos sistemas DRM, qualquer das soluções aqui descritas vai ao encontro deste requisito, fornecendo um ambiente suficientemente seguro para a realização das operações relacionadas com a proteção do conteúdo. Ao fazerem utilização extensiva de criptografia (simétrica e assimétrica), credenciais digitais e protocolos seguros que permitem a proteção e partilha de conteúdos conseguem garantir um elevado nível de segurança.

O OMA-DRM, apesar da sua orientação para o setor específico relacionado com a indústria dos telemóveis, pode contudo ser utilizado em variados cenários de aplicação (Torres et al., 2008). Diferentemente do OMA-DRM que está dependente do formato do contentor do conteúdo, o OpenSDRM é um sistema mais independente não só nesse aspeto, mas também no que se refere ao modelo de negócios, expressão de direitos e independência da plataforma no que respeita a mecanismos de proteção (Torres et al., 2008). O OpenSDRM ao poder ser adaptado a diferentes tipos de conteúdos e a diferentes modelos de negócio faz aumentar a versatilidade da sua implementação consoante o cenário de aplicação em causa.

Comparando o OpenSDRM com o OMA-DRM, quer uma solução quer outra, definem arquiteturas cujo objetivo é lidar com a distribuição de direitos diretamente com o consumidor (no OMA-DRM através do DRM Agent e no OpenSDRM através do Wallet) (Torres et al., 2008). Utilizam mecanismos que fazem a interpretação de direitos e autorização do lado do utilizador recorrendo a protocolos específicos (ROAP no OMA-DRM e serviços *Web* no

[7] http://sourceforge.net/projects/openipmp/

[8] http://sourceforge.net/projects/opensdrm/

OpenSDRM) para obter os direitos das entidades emissoras (o RI no OMA-DRM e o LIS no OpenSDRM). O MIPAMS, ao basear o formato do conteúdo em itens digitais MPEG-21 e ao utilizar uma linguagem de expressão de direitos como o MPEG-REL, também é capaz de possuir uma versatilidade ao mesmo nível do OpenSDRM. De um ponto de vista arquitetónico quer o MIPAMS quer o OpenSDRM estão plenamente orientados para funcionar via Internet. No cômputo geral são mais avançados que o OMA-DRM sendo comparáveis ao nível das funcionalidades (Torres et al., 2008). Independentemente disso, o OpenSDRM é mais extensível que o OMA-DRM já que:

- O mecanismo de *license templates* (Serrão, 2008) presente no OpenSDRM permite uma fácil extensão da linguagem de expressão de direitos podendo qualquer uma das atuais RELs ser facilmente adotada;
- O Wallet, cujo equivalente no OMA é o DRM Agent, não só é capaz de realizar a autenticação e registo, descarregar a licença, assegurar a aplicação de direitos e autorização, permitindo descarregar novas ferramentas de proteção sempre que necessário;
- O OpenSDRM oferece a funcionalidade de realização de pagamentos; o OMA já não;
- Os mecanismos do OpenSDRM são independentes do tipo de conteúdo governado, enquanto o OMA possui o seu próprio formato.

As principais diferenças entre o MIPAMS e o OpenSDRM são listadas de seguida (Delgado, Torres, Llorente & Rodríguez, 2005a):

- O OpenSDRM disponibiliza o componente Wallet que pede e gere as licenças, executando as autorizações localmente. Um único Wallet pode ser utilizado por diferentes aplicações no mesmo dispositivo enquanto o MIPAMS utiliza um *plugin* de confiança para cada aplicação (ou uma aplicação confiável);
- O OpenSDRM é agnóstico relativamente à utilização de RELs enquanto o MIPAMS propõe diferentes mecanismos para realizar a tradução entre diferentes RELs (por exemplo, entre ODRL e MPEG-21 REL (Delgado et al., 2012);
- O OpenSDRM fornece um componente de preparação de conteúdo (CPS) que recebe o conteúdo em bruto e codifica-o num formato específico universal (base64) enquanto o protege e adiciona metadados. Por sua vez, o MIPAMS deixa esta funcionalidade para ferramentas específicas do lado do utilizador deixando que a proteção e licenciamento sejam realizados no lado servidor;

- O MIPAMS executa a autorização dos utilizadores baseado numa cadeia de licenças (desde o detentor de direitos até ao utilizador final) cobrindo toda a cadeia de valor, enquanto o OpenSDRM usa uma única licença relativa ao utilizador;
- O MIPAMS viabiliza pós-pagamentos através de interfaces de supervisão e rastreio enquanto o OpenSDRM deixa este assunto em aberto nas mãos de uma entidade externa.

Quer uma plataforma quer outra fazem uso extensivo de normas internacionais no que respeita à implementação de funcionalidades base. A Tabela 5 apresenta a relação entre os principais blocos e cada um dos sistemas focando-se no suporte a MPEG-21.

OpenSDRM	MIPAMS	Blocos da estrutura funcional DRM (Capítulo 2)
MPEG-21 REL ODRL	MPEG-21 REL ODRL , MPEG-21 ER	Bloco de Utilização (verificação de aplicação de direitos, rastreio e monitorização)
MPEG-21 DID MPEG-21 DII MPEG-21 IPMP MPEG-21 REL Dublin Core Criptografia	MPEG-21 DID MPEG-21 DII MPEG-21 IPMP MPEG-21 REL Dublin Core Criptografia	Bloco de Gestão/Distribuição (repositório) Bloco de Criação (preparação do conteúdo, atribuição de direitos)
MPEG-21 DID MPEG-21 DII MPEG-21 IPMP Dublin Core	MPEG-21 DID MPEG-21 DII MPEG-21 IPMP Dublin Core	Bloco de Gestão/Distribuição (licenciamento, transação)
-	-	Bloco de Gestão/Distribuição (transação)

Tabela 5 – OpenSDRM, MIPAMS e *standards*

5 Conclusão

Atualmente existe uma grande variedade de sistemas DRM proprietários e normas abertas, mas estes não seguem um único *standard* quer no que se refere à proteção de conteúdos, quer à expressão de direitos e informação relacionada, quer ao formato do próprio conteúdo protegido. Neste capítulo fez-se um levantamento das principais soluções de DRM abertas, de modo a conseguir-se entender o seu modo de funcionamento e quais as principais diferenças entre elas. É percetível que estes sistemas têm um grande número de componentes comuns, apesar de os seus nomes serem diferentes consoante a plataforma, e em muitos casos possuirem até o mesmo tipo de fluxo de informação. Recorrendo de uma forma sistematizada à proteção de conteúdos

e direitos associados através da criptografia, contudo, a forma de transmissão de direitos desde o detentor até ao utilizador final nem sempre é clara pois normalmente estão orientados para garantir a eficácia da proteção do conteúdo, não se focalizando em particular na forma como os conteúdos e direitos são transmitidos, nomeadamente no seu formato capaz de garantir uma maior interoperabilidade entre as plataformas. Assim, não é estranho o facto de este tipo de sistemas se focalizarem na exploração de conteúdos do ponto de vista comercial (sendo por isso dada prioridade à sua proteção) não se dando especial atenção às especificidades do contexto académico.

A existência de interfaces documentadas e de domínio público viabiliza a implementação de outras aplicações ou até que outras soluções de DRM possam utilizar essas interfaces. Além disso, a disponibilidade do código fonte facilita a integração dos vários elementos constituintes do DRM, pois, ao permitir a definição de interfaces por terceiros, acaba por lhes aumentar as possibilidades de escolha das funcionalidades disponíveis. Por isso, a escolha de uma solução robusta e credível baseada em soluções DRM "abertas" torna-se uma necessidade do ponto de vista de integração. O OpenSDRM vai ao encontro destas características, sendo por isso a solução indicada com vista à sua adoção na partilha de conteúdos abrangidos por PI no contexto académico.

Parte II

Proposta de modelo de referência de DRM e integração do OpenSDRM

Capítulo 4

Proposta de modelo conceptual de referência de DRM para contexto educacional

Resumo

O objetivo deste capítulo tem em vista apresentar a primeira contribuição desta tese e consiste na proposta de um sistema de DRM que atue como um modelo de referência de arquitetura, capaz de permitir a aplicação dos conceitos da gestão de PI em conteúdos, tendo em consideração os requisitos específicos no que respeita às necessidades dos principais intervenientes na cadeia de valor de um sistema de gestão digital de direitos. Sinteticamente, a abordagem passa pela identificação e descrição das principais entidades envolvidas no fluxo de conteúdo em sistemas DRM, quais as suas funções e os seus requisitos principais e a sua forma básica de atuação. Com base nisso, são descritas as interações entre os vários componentes e a forma como se processa a proteção e distribuição do conteúdo no modelo proposto. Tendo por base as interações no decorrer do fluxo de informação, é depois proposta uma arquitetura de um sistema de DRM que nos irá servir de referência, identificando-se as principais fases das operações relacionadas com a proteção e partilha de conteúdo. Por fim, é realizada uma análise à proposta de modelo, sob o ponto de vista dos requisitos da transferência de direitos plasmados na licença.

1 Introdução

A partilha do conteúdo está associada a uma cadeia de transmissão onde há que considerar um fluxo constituído por três passos sequenciais: a criação, a distribuição e o consumo (Figura 23) (Marques & Serrão, 2009; Zhang, 2013; Iannella, 2008; Marques & Serrão, 2011).

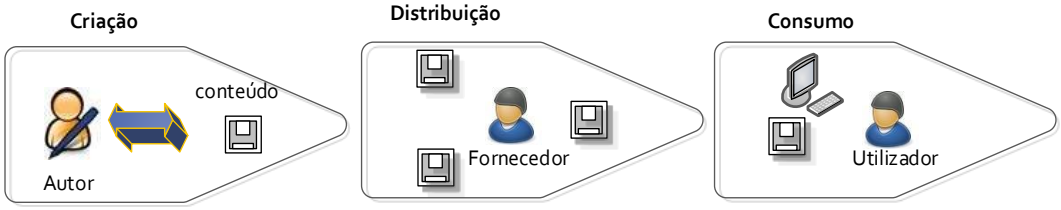


Figura 23 – Fluxo de conteúdo

O primeiro passo nesta cadeia é a criação, na qual o autor pode "empacotar" o seu conteúdo num único pacote e enriquecê-lo com metadados, criando assim um veículo de transporte de dados. O conteúdo pode ser qualquer trabalho criativo que o autor pretende publicar e partilhar, podendo ser de qualquer tipo, como, por exemplo, uma apresentação, um ficheiro áudio/video ou um simples documento texto. O autor pode combinar uma multiplicidade de conteúdos num único pacote agregando-os e até pode acrescentar metadados que descreva o conteúdo com informação suplementar para o consumidor (Ku & Chi, 2004). Por exemplo, numa apresentação estes metadados podem conter detalhes sobre o contacto do autor ou uma breve descrição da mesma. Além disso, até poderá adicionar informação sobre o licenciamento e sobre a forma como o utilizador pode usar a apresentação. Quando o autor finalizar o empacotamento, poderá então disponibilizar o ficheiro e distribuí-lo. Este é o segundo passo desta cadeia, ou seja, a distribuição. Aqui, os metadados anexados podem aumentar a visibilidade do conteúdo, pois ajuda o consumidor a encontrar mais facilmente o conteúdo e a categorizá-lo. O consumidor não necessitará de aceder ao conteúdo, em si mesmo, para saber mais informação acerca deste, pois o pacote de dados disponibilizado, ao conter metadados, pode permitir aos consumidores pesquisar por conteúdos baseados em critérios específicos ou até mesmo por determinados tipos de licenças. Tal contribui não só para a disseminação do conteúdo, mas também para uma partilha mais eficaz. No terceiro passo do fluxo de conteúdo, o consumidor já recebeu e está na posse do ficheiro escolhido e pretende reproduzi-lo ou utilizá-lo de uma outra forma. Se o conteúdo tiver sido publicado com uma licença de utilização, o consumidor, caso o pretenda utilizar, será informado acerca desta licença e, se necessário, informado dos termos do licenciamento, concordando, ou não, com as condições declaradas. Tal assegura que o consumidor, ao saber a forma como é permitido o uso do conteúdo, esteja consciente dos termos de utilização. Após a sua concordância, então poderá proceder ao consumo desse conteúdo (Figura 24).

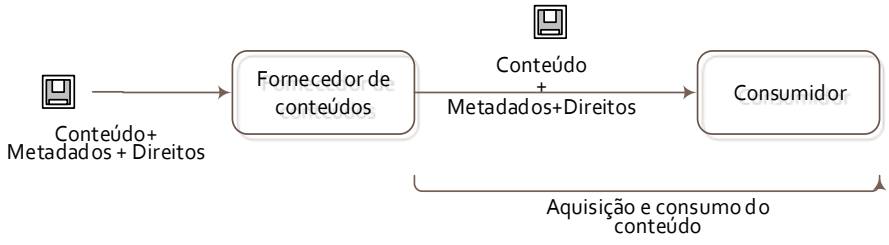


Figura 24 – Fluxo de conteúdo desprotegido (aquisição e consumo)

Contudo, se o autor tiver protegido o conteúdo com vista a assegurar a aplicação dos seus direitos autorais, este passo final poderá ser completamente diferente. Nesta situação, o

conteúdo protegido apenas poderá ser usado se for devidamente desprotegido recorrendo à mecanismos apropriados, por exemplo usando uma chave de decifra, a qual, normalmente, está contida ou na licença, ou num pacote de dados específico ou no próprio objeto digital (Ku & Chi, 2004; Blanchi & Petrone, 2001) que pode conter ambos. Esta proteção é uma das peças mais importantes, pois sendo intencionada para manter e preservar os direitos de PI pretende assegurar que os direitos de acesso definidos no passo de criação são respeitados (Ku & Chi, 2004). Para tal, têm de existir mecanismos não só para realizar e controlar a proteção do conteúdo, mas também que assegurem a vigência dos direitos e condições no decorrer da utilização do mesmo, monitorizando-os (Ku & Chi, 2004; Iannella & Mclean 2002). O DRM, sendo orientado para a proteção e preservação de direitos de PI do detentor (Iwakiri & Thanh, 2015), é solução tecnológica mais favorável que permite realizar esse controlo e monitorização, pois permite aos fornecedores e distribuidores de conteúdos terem as ferramentas adequadas para esse efeito, mas também possibilitar aos utilizadores finais escolherem diferentes tipos de licenças consoante a utilização que pretendem dar ao conteúdo (Ku & Chi, 2004). A expressão de direitos torna possível aos emissores de direitos oferecer e transmitir aos utilizadores finais vários tipos de direitos de utilização, a pedido. Esta alargada oferta permite selecionar variados tipos de licenças, o que contribui para uma melhor experiência de utilização, sendo o DRM, por isso, a solução mais adequada capaz de permitir a proteção de direitos de PI sobre conteúdo (Ku & Chi, 2004).

2 Conteúdos e DRM

No meio académico, há a necessidade de distinguir dois tipos de conteúdos: conteúdos livres/grátis (conteúdos não governados a que o utilizador pode aceder sem licenças e sem quaisquer restrições a nível de permissões) e conteúdos protegidos (que são governados e estão sujeitos a medidas de proteção tecnológica, como encriptação, máscaras, marcas de água, entre outros) (Marques & Serrão 2012b). Desta distinção resulta que o utilizador pode interagir de formas diferentes com outras entidades do sistema: no primeiro caso poderá interagir com o fornecedor de conteúdos para obter conteúdos livres/grátis; noutra, poderá interagir com um fornecedor de licenças, para obter a licença associada a um conteúdo previamente obtido. Depois de distribuídos, estes conteúdos protegidos podem ser reenviados a outros utilizadores por um canal diferente do canal de distribuição principal (o fornecedor de conteúdo), ou seja, de forma descentralizada. Contudo, para este ser usado é imprescindível que o utilizador final tenha obtido a respetiva licença (ou objeto digital correspondente) (Hwang, 2008) habilitando, assim, a superdistribuição (Löytynoja & Cvejic, 2003). Por isso, a solução de DRM a

implementar no contexto educativo deve ter em conta estes dois tipos de conteúdos, pois só assim poderá contribuir para satisfazer um vasto leque de necessidades: a dos criadores de conteúdos e detentores de direitos que pretendem que os seus direitos sejam obrigatoriamente respeitados aplicando medidas tecnológicas de proteção, e a dos criadores de conteúdos e detentores de direitos que, apesar de quererem que os seus direitos sejam respeitados, ou até prescindir desses direitos, não querem que sejam aplicadas essas medidas tecnológicas de proteção deixando o conteúdo ser partilhado sem qualquer constrangimento no acesso e uso. O modelo proposto, independentemente de o conteúdo desprotegido estar aqui previsto como uma possível variante, foca-se na proteção do conteúdo como forma de preservar a autoria do trabalho e o respeito pela sua integridade quando é partilhado.

3 Proposta de modelo

A existência de várias iniciativas comerciais e não comerciais na área do DRM, e o facto de muitas delas se basearem em especificações proprietárias contribui para que diversas funcionalidades implementadas as tornem incompatíveis. Por isso, torna-se conveniente a adoção de um modelo comum que descreva este tipo de sistemas e assim contribua para a sua harmonização (Llorente et al., 2004). As variadas soluções de DRM propostas na última década, podem sere classificadas por quatro dimensões (Yen, Liaw & Lo, 2014): integração e operação, proteção de privacidade, desenho de novos modelos de negócio e funcionalidades e gestão inovadora de fluxos. As tendências recentes no desenho de sistemas DRM concentram-se na inovação da gestão dos direitos (Yen, Liaw & Lo, 2014). Uma vez que o seu foco tem sido diversificado não contribuindo para o estabelecimento de um modelo de referência nem uma solução normativa para DRM que seja suficientemente abrangente, torna-se assim necessário, numa perspetiva funcional, identificar os fluxos, os principais participantes e componentes e a forma como o conteúdo e os direitos associados são partilhados para assim melhor entender como este tipo de sistemas funcionam num determinado contexto. Assim, poderemos conceptualizar e estabelecer um modelo genérico que pode ser aplicado no contexto académico.

3.1 Fluxo de conteúdo e DRM

Independentemente da extensão e da forma da cadeia de distribuição de conteúdo, as principais entidades envolvidas nesta cadeia podem ser categorizados como sendo o criador e detentor de conteúdo (que pode atuar como seu fornecedor a terceiros), o consumidor ou até ambos (Iannela, 2008; Marques & Serrão, 2011). Enquanto o fornecedor está envolvido na criação ou preparação/adaptação do trabalho protegido, o consumidor está envolvido na utilização deste

material de uma forma protegida. Apesar de a grande maioria dos utilizadores de um sistema de DRM serem só consumidores, nada impede que um utilizador seja consumidor de um recurso e produtor de outro (Marques & Serrão, 2011). Independentemente da perspetiva, o fluxo de conteúdo envolve sempre muitas e variadas entidades possuindo estas diferentes papéis (Marques & Serrão, 2012a). Neste caso, o consumidor não é o elemento final da cadeia pois as outras entidades podem partilhar conteúdos entre si (Jin, Lin, Liu, Zhao & Wu, 2006).

O fluxo de conteúdo presente na maior parte dos sistemas DRM pode ser separado em duas fases (Llorente et al., 2004): a proteção e a aquisição/consumo. A fase de proteção (Figura 25-1) descreve o modo como o detentor do conteúdo o protege com vista a permitir a sua obtenção e utilização de uma forma segura. A fase de aquisição/consumo (Figura 25-2) descreve o modo como um utilizador final pode obter um conteúdo protegido e a respetiva autorização sob a forma de licença para o poder utilizar de uma forma governada.

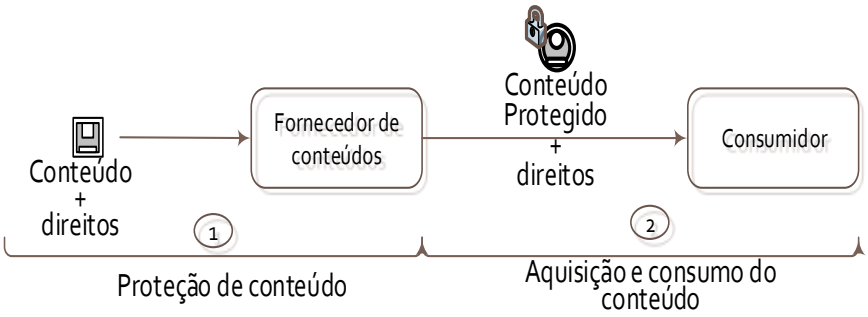


Figura 25 – Fluxo de conteúdo protegido

A fase de proteção de conteúdo envolve duas fases subsequentes (Figura 26 -1): a distribuição do conteúdo protegido e a geração dos mecanismos de proteção adequados para incorporar na licença (por exemplo a geração da(s) chave(s) de cifra a incorporar de forma protegida na licença). Estas fases estão separadas pois envolvem intervenientes com papéis diferentes, assim como informação independente (Llorente et al., 2004). A fase de aquisição e consumo, por outro lado, envolve três passos sequenciais aparentemente bastante simples (Figura 26-2); em primeiro a obtenção de conteúdo protegido, depois a aquisição da licença correspondente e finalmente a utilização do conteúdo protegido e governado (Llorente et al., 2004). O fenómeno da superdistribuição poderá levar a que o novo utilizador tenha de adquirir uma nova licença.

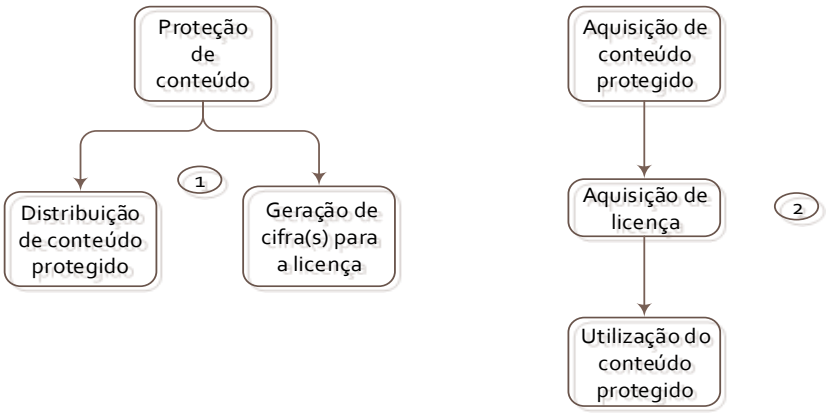


Figura 26 - Fluxo de conteúdo

①- Fase proteção de conteúdo ②- Fase de aquisição e consumo

Apesar destas fases serem distintas, várias entidades participam e assumem vários papéis no decurso do fluxo. No entanto, deve existir a flexibilidade suficiente para permitir que uma determinada entidade possa assumir papéis que estejam tipicamente atribuídos a outros.

3.2 Entidades e Papéis

Ao focarmos a análise nas principais partes envolvidas no fluxo de conteúdo, é possível encontrar os seguintes participantes, baseando-nos nos seus papéis (Nickolova & Nickolov, 2007; Collier, et.al., 2004a; Collier, et.al., 2004b):

- O **autor/detentor** do conteúdo ou **criado**r é/são a(s) pessoa(s) que cria(m) o conteúdo e possui(em) os direitos relacionados. Normalmente, é a entidade que possui direitos sobre o conteúdo estando na posse do mesmo. No caso de o detentor de conteúdos não ser, também, o seu criador, poderá adquirir direitos sobre o conteúdo a partir do seu criador original. O detentor de conteúdo, podendo usar tecnologia de proteção, desempenha um papel chave no sistema, pois é ele que seleciona individualmente o tipo de tecnologia de proteção e, assim, estabelece o nível de segurança e o modelo de negócio para a utilização do conteúdo. O legítimo detentor do conteúdo irá necessitar, na maioria dos casos, de negociar um acordo com o distribuidor dos conteúdos e o licenciador (que podem ser a mesma entidade), de modo a determinar as regras de utilização de conteúdos.
- O **editor** do conteúdo (quem o publica) oferece acesso ao conteúdo e é responsável pela sua distribuição, tendo uma relação direta com o criador de licenças. Normalmente, são-lhe atribuídas as seguintes funções:
  - Criar conteúdo num formato que esteja ajustado ao consumo;
  - Identificar individualmente os conteúdos, associando-os a um identificador único;

  - Facilitar a alteração de conteúdos de acordo com as preferências do consumidor, possibilitando o suporte destes em diferentes formatos de forma transparente;
  - Agir como intermediário em comunicações entre consumidores, autores/detentores do conteúdo, emissores de direitos, sistemas de autorização e processadores de pagamento eletrónico (caso envolva algum tipo de remuneração financeira).
- O **criador da licença** (quem vincula um conteúdo a uma licença) usa tecnologia DRM para conceder direitos aos utilizadores, oferecendo acesso personalizado ao conteúdo. Para além disso, é responsável por proteger o conteúdo de uso inadequado; daí associar cada cópia do mesmo a uma de licença, que especifica os direitos de acesso a um dado conteúdo disponíveis aos consumidores. Isto permite poupar os autores/detentores dos encargos subjacentes à negociação direta com os seus clientes. Ao garantir a oferta de uma alternativa legítima e de qualidade de obtenção de uma cópia legal, o criador da licença consegue estimular o uso legítimo. A maioria dos conteúdos difundidos desta forma fica sob o controlo do criador da licença.
- O **utilizador final**[9] (quem pretende aceder e utilizar um conteúdo) tem acesso ao conteúdo de acordo com as diretivas (regras de acesso) que foram estipuladas pelos autores/detentores e implementadas de acordo com o criador da licença que a emite. O utilizador final, para ter acesso ao conteúdo protegido tem de contactar o criador da licença responsável pela proteção deste (através de informação embutida na estrutura de metadados contida do pacote com o conteúdo). Uma outra vantagem que os sistemas DRM podem oferecer, reside na possibilidade de controlar o acesso a conteúdo académico restringindo-o exatamente àquilo que os estudantes mais desejam, mas onde existem direitos que os criadores/detentores (como por exemplo, os professores) querem controlar.

3.3 Conceptualização do modelo proposto

Considerando os quatro principais papéis envolvidos num sistema de DRM, é possível derivar um modelo genérico com os seguintes elementos participantes: o criador/detentor de conteúdos, o editor de conteúdos, o criador de licença e o utilizador final (Nickolova & Nickolov, 2007) ou consumidor. Os dois primeiros estão ligados ao criador de licença, que, por sua vez, está ligado ao utilizador final (Figura 27) (Nickolova & Nickolov, 2007). O que liga todos estes elementos são os diferentes tipos de licenças, que oferecem acesso legal a todos os conteúdos

[9] O termo "utilizador" será usado com outros termos comuns que têm o mesmo significado, como "utilizador final", "cliente", "comprador" e "consumidor".

protegidos respeitando as condições definidas através de uma linguagem de expressão de direitos.

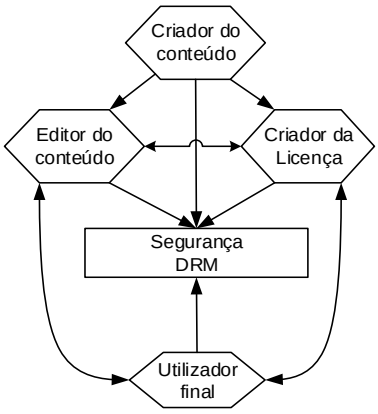


Figura 27 – Participantes e processos de segurança DRM (adaptado de Nickolova & Nickolov, 2007)

O criador do conteúdo é o utilizador que criou e/ou possui o conteúdo (detentor de conteúdo), atuando, normalmente, como detentor de direitos. O criador do conteúdo produz[10] ou fornece o conteúdo através do editor do conteúdo, ficando vinculado ao conteúdo através de uma licença. O editor de conteúdo fica então responsável pela sua legítima disseminação. Por sua vez, o criador da licença fica responsável pela emissão de licenças para o utilizador final, mas respeitando os direitos pré-definidos pelo criador e pelo editor do conteúdo (Nickolova & Nickolov, 2007).

A primeira melhoria do modelo anterior é fruto da constatação de que, no meio educativo, o editor de conteúdo e o criador da licença podem ser a mesma entidade. Isto resultou na concentração das duas entidades numa única com as mesmas funções: o fornecedor. A segunda melhoria derivou da compreensão de que o acesso a conteúdos protegidos está vinculado e governado por uma licença e resultou numa divisão do fornecedor em dois: o criador da licença (representando os direitos) e o empacotador que prepara e vincula o conteúdo à licença.

De referir que o modelo proposto é analisado na ótica do detentor de direitos. Nele, o criador ou o fornecedor mantem este papel sem perder qualquer clareza ao nível conceptual no que respeita à preservação de direitos pois estabelecem as regras (como proteção de propriedade, termos e condições de uso) que governam a utilização do conteúdo. Se o criador também for o detentor dos direitos e/ou do conteúdo, este terá de negociar um acordo com o fornecedor de conteúdo, tendo em mente a sua distribuição, bem como a sua proteção. Deste modo, o detentor

[10] Para garantir a correção e a simplicidade do modelo, o criador do conteúdo e o detentor do conteúdo são considerados a mesma entidade, sendo esta última a designação a prevalecer ao longo da tese.

de direitos atua como distribuidor de conteúdos. Para além disso, o utilizador final, para que possa aceder ao conteúdo e usá-lo, tem de estar equipado com uma aplicação DRM desenhada para executar dois tipos de processamento: o processamento do conteúdo e o processamento relativo à permissão de utilização do próprio conteúdo. Pode-se visualizar na Figura 28 interações entre os vários elementos.

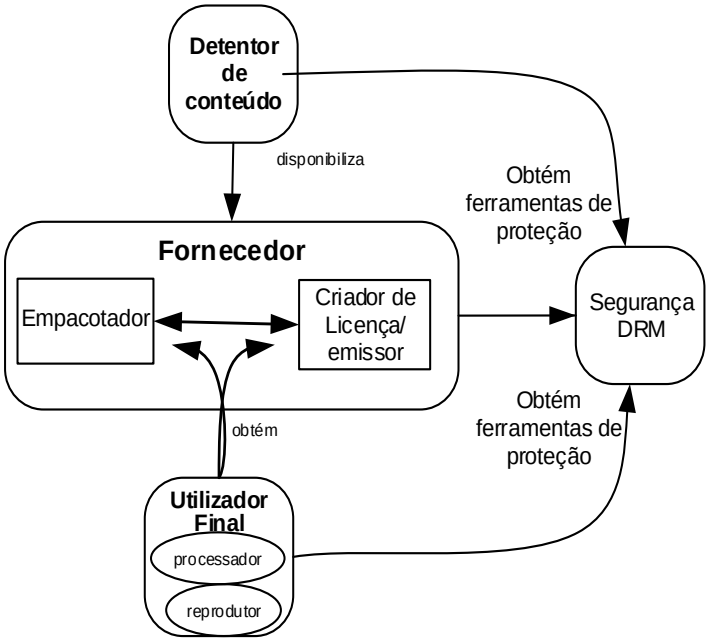


Figura 28 – Segurança e elementos participantes no modelo

As principais funções dos elementos participantes no referente à proteção passam pelo seguinte processo, em que:

- o detentor do conteúdo é quem o criou ou está na sua posse e permite o seu acesso por parte do fornecedor (empacotador);
- o criador da licença gera-a de acordo com as diretivas do criador do conteúdo;
- o empacotador codifica o conteúdo, protege-o e vincula-o a uma licença, podendo opcionalmente inserir quer o conteúdo quer a licença num pacote apropriado;
- o utilizador final obtém o conteúdo e a respetiva licença, que o processador usa para conseguir aceder ao conteúdo. De seguida, o conteúdo é acedido pelo respetivo reprodutor e utilizado de acordo com os direitos expressos na licença.

Ao longo do processo descrito é possível identificar dois tipos de objetos digitais (Sim, Oh & Lee, 2006) com que os participantes no modelo proposto devem lidar: (a) o objeto conteúdo que corresponde ao conteúdo codificado e a metadados empacotados e (b) o objeto de direitos que engloba o mecanismo de proteção do conteúdo devidamente protegido, metadados e os

termos de utilização expressos numa licença através de uma linguagem específica de expressão de direitos. Depois de identificados os elementos participantes e suas principais funções, podem descrever-se os processos nucleares a que estão associados (Figura 29):

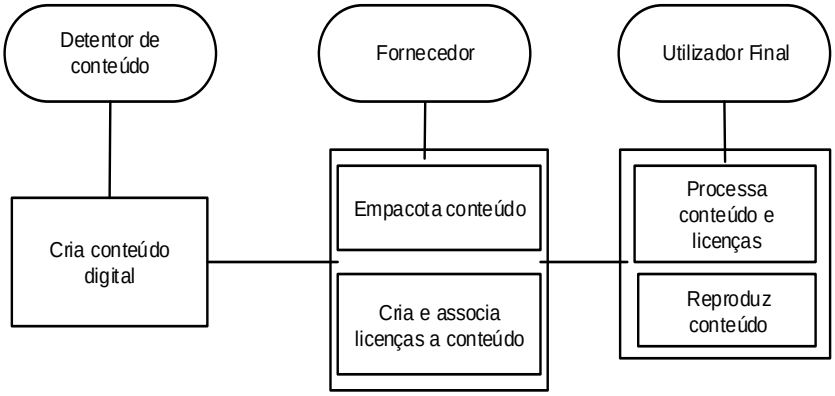


Figura 29 - Processos nucleares na proposta de modelo genérico

De forma sintética, de seguida, é descrita a execução dos processos pelos elementos participantes. O detentor do conteúdo carrega o seu conteúdo na plataforma do fornecedor. Depois, o conteúdo é codificado, empacotado e vinculado a uma licença gerada pelo criador da licença. Finalmente, o utilizador obtém o conteúdo a que já está associada uma licença. O utilizador final usa o processador do conteúdo e obtém a respetiva licença do criador de licenças para o conteúdo pretendido (Marques & Serrão, 2015a). Na posse da licença, o reprodutor acede ao conteúdo e executa a sua reprodução de acordo com os termos da licença (Figura 30).

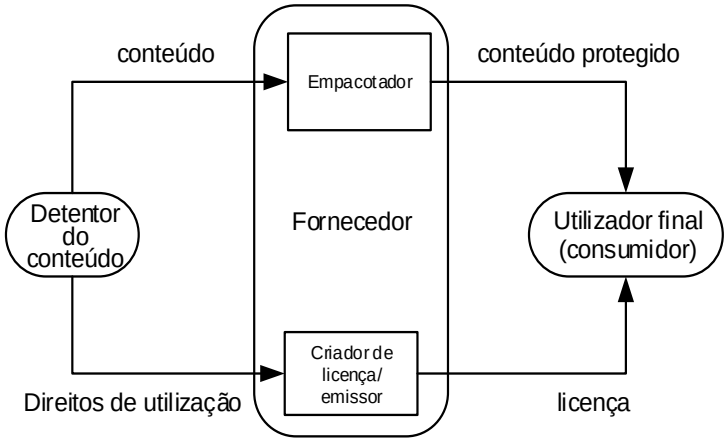


Figura 30 - Proposta de modelo DRM de referência

O empacotador de conteúdos e o criador da licença podem ser a mesma identidade ou, então, entidades diferentes. No último caso, precisam de ter um acordo que cubra os termos e condições de concessão de direitos sobre o conteúdo. Em ambos as situações, agem como distribuidores, mas no primeiro distribuem conteúdos e no segundo distribuem direitos.

3.3.1 Requisitos dos participantes

Os elementos participantes envolvidos nos processos de DRM têm diferentes expectativas, necessidades e requisitos que devem ser satisfeitos. De seguida são descritos as principais necessidades e requisitos do ponto de vista do detentor de conteúdo, fornecedor e utilizador.

- Detentor de conteúdo

O principal requisito deste participante relaciona-se com a necessidade de proteger o conteúdo de modo a conseguir garantir a preservação dos seus direitos. Assim, deve ser assegurado que o conteúdo permanece protegido quando está na posse de outras partes envolvidas. Ou seja, deve-se garantir a integridade do conteúdo.

Um outro requisito a considerar prende-se com a necessidade de o detentor poder ser capaz de definir os seus direitos e regras de utilização e de estes serem observados durante a redistribuição e utilização do conteúdo. Por fim, outro requisito a ter em conta relaciona-se com a necessidade de o sistema DRM suportar superdistribuição não só do conteúdo protegido, mas também da licença, assegurando a transmissão de direitos entre dispositivos clientes. O detentor de conteúdos pode assim, recurrer a um canal de distribuição eficiente e descentralizado para distribuir conteúdos, não podendo o conteúdo ser utilizado sem a respetiva licença. (Sachan, & Emmanuel, 2011; Yen, et.al., 2012; Löytynoja & Cvejic, 2003).

- Fornecedor

O fornecedor, além de poder disponibilizar o conteúdo num formato conveniente, deverá ser capaz de definir as regras de utilização na distribuição do conteúdo mas satisfazendo as regras primárias definidas pelo detentor. Podendo disponibilizar essas regras na forma de licença por um canal de comunicação diferente do canal conteúdo, acaba por subdividir-se em duas sub entidades: o empacotador (que prepara e disponibiliza o conteúdo ou objeto conteúdo) e o criador e emissor da licença que prepara e disponibiza as regras de utilização.

- Utilizador (consumidor)

Uma das necessidades que o utilizador final tem é que o consumo de conteúdo se realize da forma mais conveniente, ou seja, apesar dos fortes requisitos de segurança necessários à satisfação das necessidades de detentor e distribuidor, o consumidor deverá ser capaz de usar o conteúdo de um modo fácil. Uma outra necessidade relaciona-se com a preservação da privacidade do consumidor pois, o detentor e/ou distribuidor podem estar a coligir dados de utilização.

3.4 Componentes do sistema DRM

Qualquer arquitetura de um sistema DRM é composta por um conjunto normativo de diferentes componentes base (Abie, 2007) que disponibilizam as ferramentas necessárias à atividade dos participanrtes. Os participantes anteriormente identificados atuam sobre esses componentes com vista a que o conteúdo possa chegar ao utilizador final numa forma utilizável. Numa perspetiva arquitetónica, os principais componentes que asseguram as interações sobre os objetos digitais e que compõem o sistema DRM são os seguintes (Subramanya & Yi, 2006; Ku & Chi, 2004; Wang et al., 2005):

- Servidor de Conteúdos (SC)

A função principal do Servidor de Conteúdos (SC) é armazenar o conteúdo de forma protegida num repositório. O conteúdo localizado no repositório pode já estar no formato específico para a distribuição, mas, na maioria dos casos, é convertido para um formato específico de acordo com especificações standard ou proprietárias. O processo de preparação inclui cifrar e formatar o conteúdo assim como os dados relacionados, especificando direitos sobre o conteúdo, onde um módulo autónomo, normalmente designado por "empacotador" DRM, é o responsável por completar essas tarefas (Michiels et al., 2005). O pacote resultante corresponde ao objeto que contém o conteúdo e poderá conter metadados que pode corresponder a um número único de identificação para reconhecer o conteúdo e seguir a sua utilização, o conteúdo cifrado por algoritmos de chave simétrica e/ou até, simplesmente, uma ligação para o lugar onde se encontra o conteúdo protegido.

- Servidor de Licenças (SL)

As licenças contêm informações relativas à concessão de direitos, à identificação do conteúdo a que a licença se aplica e à identidade dos utilizadores ou dispositivos que pretendem atuar sobre o conteúdo. Um utilizador de um sistema DRM precisa de obter uma licença antes de aceder a uma parte específica do conteúdo ou ao seu todo. As licenças são emitidas por um gerador de licenças residente no servidor de licenças sendo normalmente inseridas no objeto de direitos que também incorpora o mecanismo de proteção do conteúdo (que pode ser uma ou múltiplas chaves criptográficas).

Ao empacotar o conteúdo, o SC redireciona o detentor do conteúdo para um módulo específico que permite definir direitos de utilização baseados na seleção efetuada por este detentor e gera um conjunto de mecanismos de proteção que são utilizados para posteriormente permitir o acesso a um determinado conteúdo. Estas definições e proteções são depois armazenadas em

bases de dados diferentes no servidor de licenças. Ambas as bases de dados contêm as identificações únicas dos conteúdos para que as definições de direitos e mecanismos de proteção possam ser associadas a itens de conteúdo específicos. Para além disso, o SL também armazena as identidades dos utilizadores, isto é, informação acerca dos utilizadores que possuem direitos sobre qualquer conteúdo protegido. A partir do pedido de licença e de informação relativa aos direitos selecionados por parte do utilizador, o criador da licença emite licenças específicas aos utilizadores legítimos e envia-as de volta para o utilizador que efetuou o pedido pela aplicação cliente do dispositivo do utilizador. Esta licença, ou o objeto digital onde está inserida, contém o mecanismo de proteção (por exemplo uma chave de decifra) que permite desproteger o conteúdo. Para que este mecanismo não seja facilmente acessível a qualquer utilizador, são utilizadas técnicas que permitem a sua ocultação, recorrendo, por exemplo, a mecanismos criptográficos de chave pública.

- Dispositivo do Utilizador

O dispositivo do utilizador contém *software* especificamente concebido para poder ser usado pelo utilizador final (ou por outros componentes ou aplicações a operar do lado do cliente) que é utilizado para aceder e usar o conteúdo. Este consiste num controlador DRM que recebe um pedido do utilizador, comunica com o servidor de licenças quando necessário (se é que esta comunicação é necessária) e está encarregue das aplicações que descodificam e processam o conteúdo num formato suportado. O controlador DRM pode ser um programa independente ou um simples módulo inserido numa aplicação de reprodução do conteúdo. As principais responsabilidades deste controlador DRM são:

(a) receber o pedido por parte do utilizador para executar operações sobre o conteúdo;

(b) recolher a informação identificativa do conteúdo e do utilizador e verificar a sua elegibilidade para obter uma licença do servidor de licenças (ou para aceder à licença embebida no próprio conteúdo);

(c) recuperar mecanismos de proteção da licença (ou objeto de direitos) e usar os mesmos para desproteger o conteúdo disponibilizando-o para o reprodutor;

d) assegurar que os direitos e condições especificados na licença são corretamente aplicados no decorrer da utilização do conteúdo.

A reprodução do conteúdo é conseguida através de uma aplicação de uso geral modificada para aceder e controlar o seu comportamento. As modificações podem ser conseguidas através do desenvolvimento e carregamento de módulos de extensão (*plugin)* ou através da interceção de

chamadas ao sistema ou da API subjacente criadas por aplicações originais (Michiels et al., 2005). As aplicações modificadas não alteram o ambiente de trabalho existente, mas podem ter um papel importante, já que verificam os direitos antes que alguma operação importante (abrir, imprimir, editar, entre outras) seja executada por qualquer utilizador (Yu & Chiueh, 2004).

3.4.1 Interação entre os diferentes componentes de um sistema DRM

Um sistema genérico de DRM que possa suportar as regras e os processos anteriormente descritos deve possuir um conjunto de componentes básicos que possibilitem o controlo da distribuição de conteúdo pelos fornecedores. Numa perspetiva de alto nível, a Figura 31 ilustra a interação dos componentes de um sistema DRM. Nesta interação importa ter em consideração o seguinte:

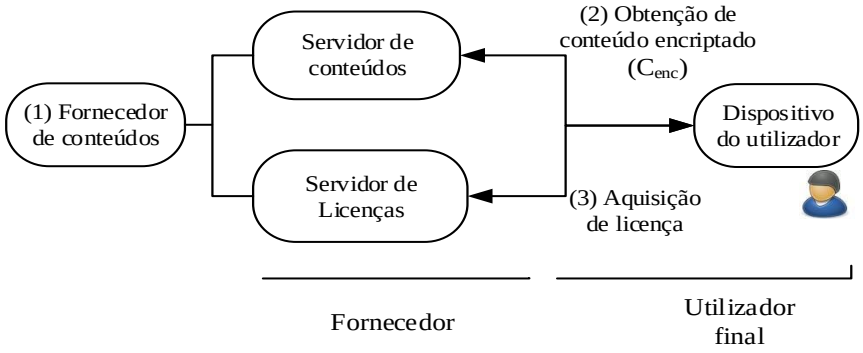


Figura 31 - Abstração das interações entre componentes de um sistema DRM

- O *Servidor de Conteúdos (SC),* responsável pela preparação, armazenamento, proteção e distribuição do conteúdo protegido ou objeto conteúdo (se for usada criptografia - C_{enc}).
- Um *Servidor de Licenças (SL)*, responsável pela criação de uma licença ou objeto de direitos para a entidade requerente. Uma licença ou objeto de direitos contém os direitos e os mecanismos de proteção necessários para decifrar o conteúdo protegido (C_{enc}), por exemplo a *Chave de Cifra de Conteúdo* (C_{EK}). Antes de emitir a licença para o cliente, o Fornecedor do conteúdo (1) deve assegurar:
  - que os direitos serão aplicados pelo cliente, ou seja que os mecanismos apropriados existem do lado do cliente para garantir a aplicação dos mesmos;
  - que o cliente irá expor a cifra ou o conteúdo decifrado apenas aos componentes com permissão para o fazerem. Por outras palavras, uma terceira entidade (neste caso o AC), que constitui uma parte de confiança aceite por todos, terá de garantir a confiabilidade do cliente perante os outros componentes.
- O fornecedor de conteúdos, é que iniciamente o podetém e normalmente tem controlo parcial sobre o SC e o SL;

- Um *Dispositivo do Utilizador*[11] é o componente que permite usufruir do conteúdo. Este é obtido numa forma protegida, por exemplo cifrado (C_{enc}) a partir de SC (2), embebido num objeto, produzido através de um processo criptográfico. Para além disso, o dispositivo DRM do utilizador obtém a licença ou objeto de direitos de SL (3) e é responsável por assegurar a aplicação dos direitos mencionados na licença. Esta licença contém o mecanismo necessário (por exemplo a chave de decifra do conteúdo -C_{EK}) para desproteger temporariamente o conteúdo e assim viabilizar a sua utilização.

No contexto desta tese e com base na proposta apresentada, iremos assumir que os mecanismos de proteção, quer de conteúdos, quer de licenças, serão baseados em mecanismos de criptografia simétrica e assimétrica. Existem, no entanto, um conjunto de outros mecanismos de proteção que podem ser utilizados no contexto deste trabalho e das suas propostas e contribuições.

Podendo os conteúdos ser de grande dimensão a criptografia de chave simétrica pode ser utilizada para cifrar o conteúdo. Nesta situação, este é o método mais adequado por razões de desempenho nos processos criptográficos de cifra e de decifra de conteúdos (Jeong, Yoon & Ryou, 2005). Para cada conteúdo é gerada uma chave diferente, podendo existir situações em que, para o mesmo conteúdo e para utilizadores diferentes, existem igualmente chaves diferentes. O conteúdo disponibilizado pelo detentor é cifrado usando uma chave de cifra de conteúdo (C_{EK}) e apenas os utilizadores a quem é fornecida uma licença válida contendo esta chave de cifra de conteúdo protegida o podem desencriptar e usar. Antes de emitir a licença ou objeto licença é ativado um mecanismo que verifica a elegibilidade do pedido de emissão e respetivas condições. A licença inclui termos e condições de acesso ao conteúdo num formato legível por mecanismos automáticos (software ou hardware) e inclui a chave de cifra do conteúdo (C_{EK}), a qual foi criptograficamente protegida para salvaguardar o acesso pelo seu legítimo destinatário. A criptografia assimétrica é aplicada para proteger a chave de cifra de conteúdo cifrando-a com a chave pública do destinatário (K^{pub}_{U}). Para garantir confiança entre as diferentes entidades do sistema, é utilizada uma infraestrutura de chave pública (*Public Key infrastructure* - PKI). Cada um dos componentes gera o seu par de chaves e envia a chave pública para a entidade certificadora (AC) de modo a obter um certificado que lhes vai garantir reconhecimento mútuo (Serrão et al., 2007; Jeong et al, 2005).

Do lado do utilizador, uma aplicação desenvolvida especificamente para o efeito e residente num dispositivo operado pelo utilizador final (muitas vezes designado *cliente DRM*) é usada

[11] *Dispositivo Cliente* ou *Cliente DRM* também é um nome comum.

para desproteger temporariamente o conteúdo e assim ser possível a sua utilização. Esta aplicação cliente está univocamente identificada e reconhecida pelos outros elementos com quem interage atuando como um componente de confiança. A componente é de confiança na medida em que é reconhecida pelos outros graças à confiança nos certificados digitais previamente emitidos pela AC e garante a aplicação das cláusulas estabelecidas pelo licenciador. Além disso, limita o acesso não só à chave de proteção do conteúdo (C_{EK}), como também à forma desprotegida do mesmo.

Depois de o objeto conteúdo ter sido distribuído uma primeira vez pelo SC, o utilizador pode então fazer um pedido para exercer operações sobre o conteúdo, por exemplo, escolhendo o item do menu numa aplicação de reprodução, executando os ficheiros do sistema ou fazendo duplo clique no ícone do objeto com o conteúdo formatado. A aplicação cliente, estando desenhada de modo a que o controlador DRM possa ser sempre ativado em resposta a um pedido (Rosenblatt et al, 2004), faz com que este comece a recolher a informação necessária para verificar a validade do pedido com vista a obter uma licença, incluindo a informação identificativa do utilizador e do conteúdo e quais os direitos que o utilizador pretende exercer. Se o utilizador estiver registado, o controlador DRM tentará encontrar informação relacionado com a licença desse conteúdo na base de dados do dispositivo. Se o utilizador não se tiver registado anteriormente no sistema DRM, o controlador ajudará a criar a informação que o identifique e envia-la-á para a base de dados de identidades do servidor de licenças.

Para o pedido válido de um utilizador autenticado, o gerador de licenças produz uma licença ou objeto licença que contém especificações de direitos, informação identificativa do cliente e a chave (ou chaves) de cifra/decifra devidamente protegidas do conteúdo, devolvendo depois a licença, ou o objeto que a contém, ao controlador DRM (Rosenblatt, 2004; Michiels et al., 2005). No entanto, para que a chave de cifra/decifra não possa ser facilmente acessível e transmissível por terceiros, recorre-se a criptografia assimétrica em que esta chave é encriptada com a chave pública do utilizador destinatário, e é inserida na nova licença ou objeto digital a ser obtido pelo utilizador. Quando finalmente, o controlador DRM do lado do cliente recebe o objeto, decifra a chave de cifra do conteúdo recorrendo à sua chave privada (do utilizador) que está na sua posse. Na posse da chave de cifra/decifra procede-se à desencriptação do conteúdo, sendo então possibilitada a execução de um conjunto de operações sobre o conteúdo por uma aplicação de reprodução de acordo com as condições expressas na licença (Rosenblatt, 2004).

Contudo, e no caso particular do meio académico, há a ter em conta um ponto importante antes do gerador de licenças emitir uma licença a pedido do utilizador final. Partindo do pressuposto

de que o utilizador é um membro da instituição educacional e que a licença somente poderia ser emitida para um utilizador com um perfil pré-estabelecido (por exemplo, um aluno que esteja devidamente inscrito num ciclo de estudos específico no atual ano letivo) então o servidor de licenças teria de verificar a elegibilidade deste utilizador perante estas condicionantes antes de emitir a licença. Na nossa abordagem, sempre que o utilizador final requeira uma licença de utilização de um conteúdo, o SL tem de saber se aquele é elegível para descarregar a mesma. Para tal irá contactar um Servidor de Validação (SV), obtendo dados para saber se o utilizador faz parte do domínio em causa e se obedece às condições com que a licença pode ser emitida.

No contexto académico, o processo habitual consiste em verificar se o utilizador é um membro da comunidade. Nesta situação, a plataforma onde residem todas as atividades dos membros da instituição designa-se por Plataforma de Gestão Académica (SGA)[12], podendo esta atuar como SV. Assim, o SL deve contactar o SGA da instituição para saber se o utilizador pertence ao domínio e se está autorizado a pedir a licença em causa. O gerador de licenças do SL solicita ao SGA estes dados e processa o pedido com os dados enviados, confirmando a legitimidade do pedido de licença do utilizador (Marques & Serrão, 2015a; Marques & Serrão, 2015b). Caso o resultado seja positivo, dá início à emissão da licença correspondente (Figura 32) para o utilizador que a requereu podendo este efetuar o descarregamento.

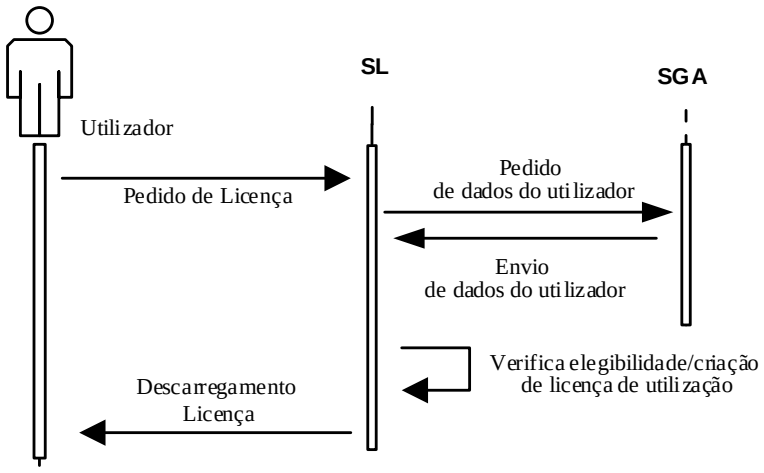


Figura 32 - Validação do pedido de emissão de licenças

Há a salientar neste cenário que, além de o utilizador requerente ter de ser um membro da comunidade académica, tem também de satisfazer algumas das condições que o detentor de

[12] SGA – Sistema de Gestão Académica – plataforma onde todas atividades académicas (cursos, aulas, matérias, membros, entre outros) relacionadas com a componente administrativa de uma instituição educacional são armazenados e geridos.

conteúdos especificou nas licenças de distribuição por ele criadas. Por exemplo, se um professor estipular como condição que somente os estudantes de um determinado ciclo de estudos de uma certa instituição universitária podem utilizar o conteúdo, então apenas os estudantes desse ciclo de estudos dessa instituição podem obter licença válida nas condições definidas. Ou seja, antes de emitir a licença o estudante será validado não só para verificar se pertence à comunidade académica como também se obedece às condições específicas expressas nessa mesma licença. Os outros estudantes, apesar de serem membros da mesma instituição, não podem obter essa licença, porque não estão devidamente inscritos nesse ciclo de estudos. Aqui o SL terá um papel importante na verificação da elegibilidade do pedido de licença. Para tal valida esse pedido através de um mecanismo específico que procede à análise e comparação dos dados retornados pelo SGA e os da informação constante na licença de distribuição do conteúdo previamente criada pelo detentor do conteúdo. Se o resultado final for positivo, então o SL pode proceder para o passo seguinte: a emissão de uma licença de utilização obedecendo às condições especificadas na licença de distribuição. Deste modo, com a aplicação do mecanismo apropriado torna-se possível controlar a distribuição de licenças dentro do meio académico não só sabendo a quem a licença é dirigida, mas validando a elegibilidade do utilizador perante as condições estabelecidas pelo detentor de direitos. A grande vantagem relativamente a outro tipo de emissão de licenças que requerem a validação da elegibilidade dos membros de um grupo (por exemplo através de licenças certificado MPEG-21 REL (Yang et al., 2008; Wang et al., 2005; Sheppard & Safavi-Naini, 2006a), ou de licenças agregadas (Sachan et al., 2010; Sachan & Kankanhalli, 2012) está no processo de simplificação da emissão da licença. Esta simplificação é resultante de não ser necessária a posse adicional de comprovativos que validam a elegibilidade do utilizador perante as condições definidas inicialmente pelo detentor de direitos. Desta forma pode-se simplificar a emissão de licenças aplicando os mecanismos de controlo adequados que garantem que os direitos são respeitados ao longo da linha sucessória.

3.4.2 Proteção do conteúdo e chaves

Tendo em conta o modelo proposto, iremos assumir que no decurso da proteção o utilizador faz uso de um dispositivo, que, para além de conter as ferramentas adequadas que lhe permitem atuar sobre o conteúdo, está devidamente registado e autenticado perante o sistema DRM, sendo os seus pedidos de emissão de licença considerados, a*priori*, válidos.

Consideremos C_n como sendo o conteúdo, e C_{EK} a chave de cifra secreta usada por um algoritmo de cifra simétrico S_k para encriptar o conteúdo. Quando se aplica S_k com a chave C_{EK} sobre o conteúdo C_n o resultado obtido é o conteúdo encriptado C_{enc}.

- $S_k (C_n, C_{EK}) = C_{enc}$

  S_k é um algoritmo de cifra simétrica que cifra o conteúdo com uma chave de cifra C_{EK}.
  C_{EK}*: é a chave de cifra do conteúdo; chave secreta usada na cifra do conteúdo (pode ser obtida por cálculo do resumo (hash) sobre o conteúdo).*

  C_{enc}: é o conteúdo cifrado; conteúdo protegido resultante da aplicação de S_k sobre o conteúdo.

Assumindo que o utilizador possui um par de chaves, uma pública e outra privada (K^{pub}_{U1},K^{priv}_{U1}) armazenadas de uma forma segura no seu dispositivo e que o emissor de licenças (Distribuidor D) possui igualmente um par de chaves (K^{pub}_{D}/K^{priv}_{D}) então, para proteger a C_{EK}, o emissor de licenças cifra-a com a chave pública do utilizador U que a requereu (K^{pub}_{U1}), usando um algoritmo A_k de criptografia de chave assimétrica.

K^{pub}_{U} e K^{priv}_{U} são as chaves pública e privada de um utilizador U*, utilizadas pelo algoritmo de criptografia assimétrica.*
A_K é um algoritmo criptográfico de chave assimétrica que utiliza o par de chaves K^{pub} e K^{priv} do utilizador U

- $A_K (K^{pub}_{U1}, C_{EK}) \rightarrow C_{EK}^{P}$ (C_{EK} protegida pela chave pública do destinatário)

De seguida o emissor de licenças D gera uma licença (*lic*) incorporando direitos, metadados e a C_{EK} protegida (C_{EK}^{P}), e gera uma assinatura digital sobre essa licença usando a sua chave privada (K^{priv}_{D}). A licença assinada é então enviada ao utilizador final pelo emissor de licenças.

D_{sig} é o algoritmo de assinatura digital*;*

signature $D_{(lic)}$ é o resultado obtido quando D aplica *D_{sig}* sobre *lic* com a sua chave privada *K^{priv}_{D};*
signature $D_{(lic)}$= D_{sig} (K^{priv}_{D}, lic);

A licença assinada digitalmente por D, (Lic (D_{sig}D)), corresponde a:

- Lic (D_{sig}D) = *lic* + *signature $D_{(lic)}$*

Logo:

- Lic (D_{sig}D) = *lic* + *Dsig (K^{priv}_{D}, lic)*

Sendo *lic* = $A_K (K^{pub}U_1, C_{EK})$ + direitos

Então a licença assinada é:

- Lic (D_{sig}D) = $A_K (K^{pub}U_1, C_{EK})$ + direitos + Dsig (K^{priv}_{D}, *lic*)

Quando o utilizador recebe a licença assinada, a primeira coisa que faz é verificar a integridade desta aplicando o algoritmo de assinatura digital e verificando a conformidade de acordo com a assinatura do emissor da licença.

D_{sig} (K^{pub}_{D}, (*signature* $D_{(lic)}$))

D_{sig} (K^{pub}_{D}, (Dsig (K^{priv}_{D}, *lic*)))

Se a assinatura for válida, então:

- D_{sig} (K^{pub}_{D},(*signature* $D_{(lic)}$)) = D_{sig}(*lic*)

O utilizador pode então prosseguir obtendo a C_{EK} protegida (C_{EK}^{P}) extraindo-a da licença. De seguida aplica o algoritmo de chave assimétrica A_K, com sua chave privada K^{priv}_{U1} (correspondente da chave pública K^{pub}_{U1}) sobre a C_{EK} protegida (A_K ($K_{priv}U_1$, C_{EK}^{P})). O resultado obtido é a C_{EK} desprotegida.

- A_K ($K^{priv}U_1$,A_K ($K^{pub}U_1$, C_{EK})) = C_{EK}

De seguida, o utilizador procede à decifra do conteúdo protegido C_{enc}, aplicando o algoritmo de cifra simétrico com a C_{EK} previamente obtida (pressupõe-se a utilização de apenas uma chave para cifrar o conteúdo).

- S_k (C_{enc}, C_{EK}) = C_n

O resultado obtido é o conteúdo desprotegido, podendo então o reprodutor (*player*) residente no dispositivo do utilizador usar este conteúdo de acordo com os termos e condições especificados na licença. O esquema que suporta a encriptação do conteúdo é baseado numa (ou múltiplas) chave(s) de cifra de encriptação, $C_{EK,}$ aplicada pelo distribuidor de conteúdo, e num conjunto de chaves de cifra, (K^{priv}_{U}/K^{pub}_{U}), do utilizador, que personaliza o acesso ao conteúdo por parte do utilizador. A C_{EK} permite proteger o conteúdo prevenindo, através da encriptação, o acesso não autorizado ao conteúdo e o par de chaves K^{priv}_{U}/K^{pub}_{U} previne o acesso à C_{EK}. Somente um utilizador legítimo utilizando um dispositivo considerado de confiança poderá desencriptar temporariamente o conteúdo usando a chave privada do seu conjunto de chaves de cifra para obter a C_{EK} que permite o acesso ao conteúdo. A aplicação de mecanismos criptográficos vem permitir que o conteúdo possa ser protegido de forma segura e que possa ser acedido de forma controlada. A criptografia permite que o respeito pela confidencialidade e integridade do conteúdo seja observado, assim como o respeito pela autoria (através das assinaturas digitais).

3.5 Estrutura do sistema proposto

Na atual proposta, o canal de distribuição do conteúdo protegido pode envolver qualquer sistema computacional corrente que proporcione o envio de conteúdos, desde um simples servidor *Web* até à entrega em mão do conteúdo numa *flash drive*. O servidor de licenças é utilizado pelo dispositivo cliente somente para obter o objeto licença com a chave de cifra que protege o conteúdo e as licenças necessárias ao consumo. Existindo dois canais de transmissão de objetos independentes, um para o objeto conteúdo e outro para o objeto de direitos, passa a haver uma grande liberdade para modelar as operações do sistema DRM.

Podemos assim conceptualizar a estrutura do sistema de DRM capaz de suportar o modelo proposto tendo em conta o fluxo de informação desde o fornecedor de conteúdos até ao consumidor. No momento de disponibilizar o conteúdo, o fornecedor carrega o conteúdo e informação relacionada. O sistema DRM faz o processamento desta informação e produz o objeto de direitos e de objetos conteúdo. Quando se realiza o consumo do conteúdo, o dispositivo do utilizador extrai a informação adequada do objeto de direitos para poder decifrar o conteúdo inserido no objeto conteúdo. Com o conteúdo já desprotegido o dispositivo do utilizador faz vigorar os termos e condições inseridos na licença extraída do objeto de direitos podendo então o utilizador realizar o consumo. A Figura 33 ilustra o fluxo de informação ao nível conceptual sendo aí possível verificar o seu alinhamento com o modelo proposto.

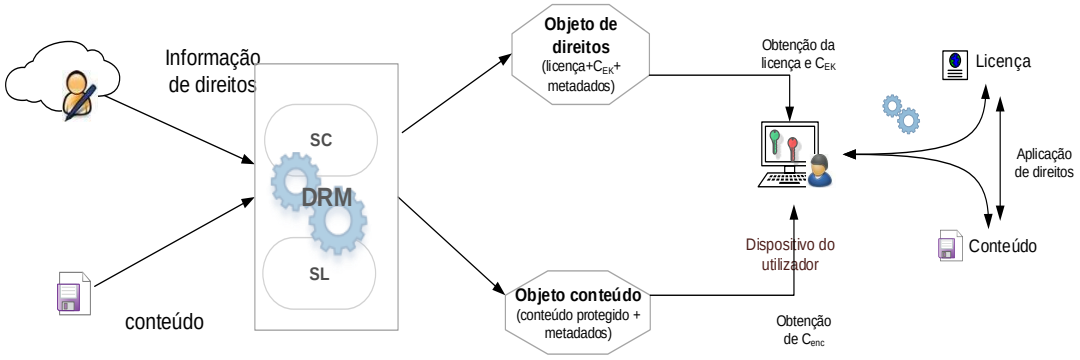


Figura 33 – Fluxo de conteúdos, direitos e informação,

No esquema proposto a abordagem considera:

- A utilização de um sistema de PKI capaz de garantir confiança a participantes e componentes;
- A utilização de um sistema capaz de executar mecanismos de criptografia de chave-pública (assinatura digital e cifra);

- A utilização de mecanismos criptográficos de geração de resumo para criar automaticamente a cifra C_{EK};
- A utilização de criptografia de chave simétrica na cifra do conteúdo pelo SC com a chave de cifra C_{EK} (recorrendo por exemplo ao AES), inserindo-o protegido num objeto digital conjuntamente com metadados;
- A utilização de criptografia de chave assimétrica (K^{priv}, K^{pub}) para proteger a C_{EK};
- A emissão de licenças personalizadas para cada cliente elegível, embebidas num objeto digital conjuntamente com a C_{EK} cifrada e metadados;
- A verificação da elegibilidade do pedido para obtenção de licença através de uma entidade externa (SV);
- Os componentes do sistema de DRM que têm acesso à C_{EK} são o SC, o SL e o utilizador final que usa um dispositivo cliente seguro com uma licença válida para o conteúdo;
- A utilização de assinaturas digitais nos objetos conteúdos e objetos de direitos e respetiva licença como meio de garantir a sua integridade.

Do ponto de vista da transferência de objetos, assume-se o seguinte:

- A transferência do objeto de direitos ocorre entre dois componentes de confiança: o emissor da licença (SL) e o dispositivo cliente ou entre dispositivos cliente;
- Os utilizadores possuem uma par de chaves (K^{priv}, K^{pub}) e estão autenticados perante o sistema DRM. A chave privada está armazenada em local seguro no dispositivo cliente, de modo a que o utilizador não tenha acesso direto à mesma;
- O objeto de direitos que contém a licença e a chave de cifra de conteúdo (C_{EK}) protege esta última criptograficamente de forma a garantir a sua confidencialidade. Para garantir a autenticidade e comprovar a integridade da licença por terceiros, esta é assinada digitalmente pelo emissor;
- A aplicação que utiliza o conteúdo residente no dispositivo cliente sendo executada num ambiente seguro torna incapaz a revelação da cifra de proteção do conteúdo e do conteúdo desprotegido quando este ficar decifrado para ser consumido.

A proposta de arquitetura está desenhada com vista a suportar a superdistribuição de conteúdos. Os canais de distribuição de conteúdos protegidos podem ser múltiplos, variando desde servidores *Web* até redes ponto-a-ponto, mas a obtenção do objeto de direitos terá de ser efetuada a partir do servidor de licenças. As licenças ficam ligadas ao utilizador de modo a permitir que este aceda ao conteúdo a partir de dispositivos vulgares (computadores, tablets,

smartphones, entre outros). A ligação à Internet só é necessária quando o utilizador obtém a licença pela primeira vez a partir de um servidor. As licenças são baseadas em XML podendo definir direitos de utilização simples que viabilizam o consumo de conteúdos protegidos desde que sejam válidas. A obtenção das licenças é realizada em observância com o modelo anteriormente proposto tendo em conta a interação com o SGA a fim de validar a elegibilidade do utilizador face ao pedido de emissão da licença. Assume-se que o objeto conteúdo, além do conteúdo protegido, contém meta informação relacionada. O dispositivo do utilizador onde reside a aplicação cliente identifica o conteúdo protegido e obtém a licença respetiva a partir do servidor de licenças. Nesta arquitetura é assumida a existência de uma infraestrutura de chave pública que disponibiliza serviços típicos como a criação, revogação e atualização de certificados, entre outros. A autoridade certificadora (AC) faz parte da infraestrutura de chave pública tendo por tarefa ligar as identidades dos utilizadores aos seus pares de chaves de encriptação através dos certificados. A arquitetura permite a disponibilização de diferentes ferramentas de proteção correspondentes a variados métodos e versões de algoritmos. De um ponto de vista estrutural foi desenhada a seguinte estrutura (Figura 34) do sistema que atuará como base de referência arquitetónica para o modelo proposto.

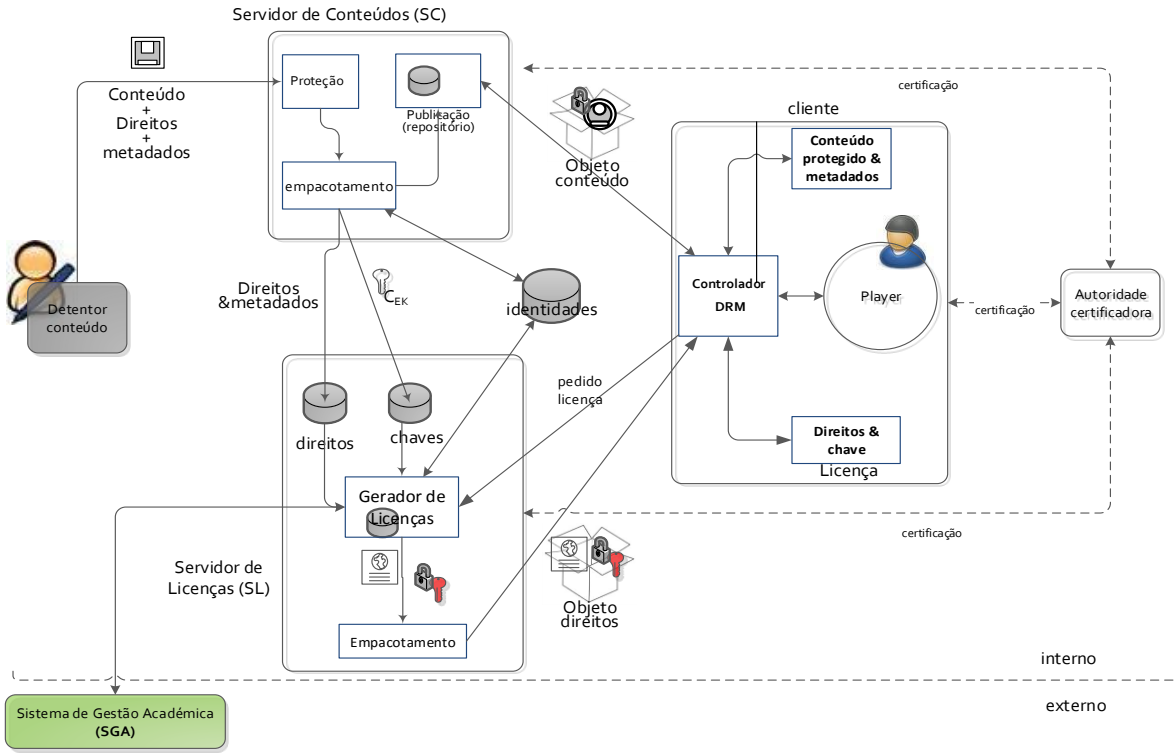


Figura 34 – Arquitetura proposta do sistema DRM

Ao analisar as várias soluções de DRM aqui apresentadas é possível notar que uma grande maioria envolve, quase sempre, os mesmos intervenientes atuando do mesmo modo e seguindo

um padrão bastante similar. A nossa abordagem tenta ser o mais neutra possível em termos tecnológicos (por exemplo, não fica restrita a um único tipo de mecanismo de proteção) e descreve em termos arquitetónicos e funcionais a proposta de solução de DRM orientada para a proteção de direitos dobre conteúdos educacionais. Nesta arquitetura é possível perceber a presença das três principais entidades típicas de um sistema DRM (Rosenblatt et al., 2004): o servidor de conteúdos (*SC*), o servidor de licenças (*SL*) e o cliente (utilizador final). De forma a verificar a legitimidade dos utilizadores no meio académico, foi acrescentada uma quarta entidade: o sistema de gestão académica (SGA). Esta entidade, ao permitir estabelecer integração com o sistema DRM (por exemplo através de serviços *Web)*, possibilita a validação e legitimação do utilizador nesse meio e nas condições pré-definidas pelo detentor de direitos de modo a que a validação de direitos transmitidos em conformidade com a linha sucessória seja realizada antes da emissão da licença.

De um ponto de vista arquitetónico, na solução está sempre subjacente uma infraestrutura de PKI capaz de disponibilizar capacidades de proteção e funcionalidades de autenticação. A razão para tal é justificada pela necessidade de estabelecer confiança entre os componentes. A integração de uma autoridade de certificação (AC) é crucial de modo a garantir as funcionalidades de PKI nas suas operações internas. A AC vem permitir o reconhecimento entre participantes e componentes através dos pares de chave pública e certificados digitais atribuídos. Na arquitetura, os principais componentes interagem mutuamente tendo por base protocolos específicos de DRM. O autor/detentor de conteúdo cria-o e envia-o ao fornecedor usando canais de comunicação seguros (SSL/HTTPS) não havendo, por isso, grandes preocupações com a segurança no que respeita à aplicação de medidas de proteção nesta fase.

Na solução proposta, os canais de distribuição podem ser desde simples servidores *Web* até redes ponto a ponto, sendo o servidor de licenças usado para adquirir as licenças necessárias à utilização do conteúdo. Apesar de haver uma grande liberdade de conceber as operações, o seu desenho depende da lógica do negócio e do contexto em causa: o académico. Por isso, a integração do SGA, como componente externo necessário à verificação da elegibilidade do pedido dos utilizadores para emissão de licença no contexto em causa é de primordial importância na estrutura, viabilizando o licenciamento neste contexto.

De um ponto de vista funcional, pode-se sintetizar o fluxo de conteúdo e informação associada através das seguintes fases (considere-se que os utilizadores estão registados e autenticados).

1 – Criação do conteúdo, direitos e metadados

O detentor do conteúdo cria e gere conteúdo usando aplicações e ferramentas específicas que incorporam tecnologia capaz de garantir a proteção do conteúdo. Em termos básicos o conteúdo é codificado num formato de transporte neutro (por exemplo em *Base 64*), encriptado e empacotado sendo gerado o identificador do conteúdo (IDc), metadados (M) e a chave de proteção do conteúdo (C_{EK}). Após realizar a preparação do conteúdo e o seu empacotamento num objeto digital, a informação associada é preparada pelo SC para publicação (metadados, descrição do conteúdo, detalhes do licenciamento, entre outros). Para garantir a integridade e autenticidade o objeto será assinado digitalmente.

2 – Geração de chaves

As chaves usadas na encriptação do conteúdo e metadados relacionados são disponibilizadas ao servidor de licenças (SL). Ao mesmo tempo o SL permite ao detentor do conteúdo definir as condições em que este poderá ser distribuído apresentando-lhe um formulário com vários itens relativos a permissões e restrições.

3 – Pedido de emissão de licença

Após obter o conteúdo desejado, o utilizador U interage com SL através do cliente e faz um pedido de emissão de licença especificando condições em que pretende utilizar o conteúdo IDc e envia o seu certificado (CERT_C). O SL, para legitimar o pedido, contacta o SGA pedindo informação sobre o utilizador. Esta informação permite validar a elegibilidade do pedido (qual o utilizador e condições) e, caso seja aceite, irá preparar uma licença de utilização para emitir.

4 – Informação de licenciamento

Nesta fase, o SL depois de verificar se o utilizador é legítimo perante o SGA (verificando se está aí registado), verifica internamente a elegibilidade do pedido de licença. Para tal, o SL verifica se o pedido do utilizador obedece às condições de distribuição definidas pelo detentor do conteúdo processando e comparando com os dados provenientes do SGA relativos ao utilizador (por exemplo, se o utilizador está matriculado no curso) e efetua a ativação do mecanismo adequado de validação de licenças (ver nos capítulos 9 e 10). Caso a validação seja positiva o SL gera uma licença assinada digitalmente com os direitos de utilização para o utilizador que a pediu.

5 – Geração do objeto de direitos

De seguida, o SL procede à geração de um objeto de direitos contendo a informação necessária e os metadados, direitos e a chave de proteção do conteúdo encriptada com a

chave pública do utilizador, (K^{pub}_{U}), que fez o pedido. O SL disponibiliza ao cliente o URI correspondente deste objeto. Refira-se que para garantir a confidencialidade da chave de proteção do conteúdo esta é encriptada. Para garantir a integridade e autenticidade o objeto é assinado digitalmente.

6 – Aquisição da licença e utilização do conteúdo

A utilização do conteúdo só é possível após o cliente autenticar o objeto conteúdo e o objeto direitos e, de seguida, efetuar a desencriptação da cifra de proteção. Adicionalmente terá de desproteger o conteúdo com a cifra ficando o seu uso condicionado aos termos e condições especificados na licença. Como todos os objetos trocados entre o cliente, SL e SC são assinados digitalmente, pode-se garantir o seu não-repúdio por quem os emitiu. Após a extração da informação destes objetos, o conteúdo pode ser utilizado, assegurando o cliente a correta vigência dos termos e condições expressos na licença.

A interação entre os vários componentes DRM assenta em transações seguras, minimizando a exposição da utilização do conteúdo a utilizadores fora do domínio académico. Para tal, é de referir que uma das principais contribuições fica materializada nas interações com o SGA para assinalar ao SL que somente utilizadores legítimos no domínio académico podem obter licenças. Deste modo, a emissão de licenças fica limitada aos utilizadores que foram aprovados previamente. Estes utilizadores podem ser desencorajados de partilhar as suas chaves privadas e certificados digitais com terceiros pois qualquer utilização irregular de conteúdo poderá ser-lhes atribuída indevidamente. Ao lidar com cada pedido de emissão de licença de forma autónoma realizando a sua validação prévia, consegue-se obter um nível de controlo bastante elevado no que se refere à segurança na transmissão do objeto de direitos e com isso uma maior capacidade de gestão dos utilizadores, e pedidos de licenciamento por eles realizados.

3.5.1 Requisitos na transferência da licença

Os requisitos do procedimento da transferência da licença, quando esta transita do distribuidor para o dispositivo do utilizador ou entre dispositivos de utilizadores sob a forma de um objeto digital, podem ser enumerados da seguinte forma:

- A transferência deve assegurar que somente os utilizadores autorizados têm acesso à licença;
- A transferência deve assegurar que somente os utilizadores pertencentes ao domínio académico são elegíveis para que a licença lhes seja emitida;

- O objeto de direitos, quando residente no dispositivo do utilizador deve manter sempre protegida a chave de cifra de proteção do conteúdo (C_{EK});
- No decorrer da transação do objeto de direitos este deve ser mantida protegida de modo a que não possa ser modificada, intercetada ou adulterada sob qualquer forma.

3.5.2 Funcionalidades do modelo proposto

As operações relacionadas com a proteção e partilha de conteúdos com direitos de PI podem ser delineadas de acordo com a implementação de várias funcionalidades. Estas podem ser sistematizadas da seguinte forma:

- Pedido de certificado e registo**:** esta fase é a inicial e é obrigatória. Todas as entidades (participantes e componentes) com papéis essenciais, devem estar registados perante a AC e possuírem certificados digitais e respetivos pares de chaves K^{pub}/K^{priv}. Após o registo e uma autenticação com sucesso no sistema, o detentor do conteúdo pode fazer o carregamento do conteúdo C_n.
- Preparação do conteúdo e metadados: nesta fase, os detentores de conteúdo, após estarem registados e autenticados no sistema, já são considerados de confiança e podem então proceder à preparação e gestão do conteúdo protegido. Para tal, usam aplicações e ferramentas específicas de autoria que fazem recurso a tecnologia de proteção DRM. A proteção do conteúdo é conseguida através de aplicações e de ferramentas específicas de proteção como as de marca de água e de criptografia de chave simétrica. Nesta fase é gerado o identificador do conteúdo (ID_C), metadados do conteúdo (C_M) e a chave de cifra secreta de proteção do conteúdo (C_{EK}). De modo a gerar uma chave diferente por cada conteúdo, a C_{EK} pode ser gerada a partir da função resumo $Hash_{SHA1}\big(Hash_{SHA1}(C) + Hash_{SHA1}(Author_{ID})\big)$ sobre o resumo do conteúdo e do resumo do identificador do detentor.
- Empacotamento do conteúdo e contentores: nesta fase, no SC é utilizada uma chave de cifra específica C_{EK} para um conteúdo específico com uma identidade ID_c para executar a cifra do conteúdo C_n, dando origem a um contentor seguro C_{enc}. O conteúdo protegido é de seguida empacotado num formato específico (recorrendo a um "item digital" especificado na norma MPEG-21) conjuntamente com a sua identificação (ID_C) e metadados e disponibilizado para ser descarregado pelo SC sob a forma de objeto digital. A integridade e não repúdio serão assegurados pela assinatura digital do fornecedor do conteúdo inserida no objeto.

- Chaves de encriptação, metadados e licenciamento de direitos: as chaves são usadas para a cifra do conteúdo e conjuntamente com outra informação relevante são disponibilizadas ao SC. Após acabar de realizar a preparação e empacotamento do conteúdo toda a informação necessária será enviada ao SL (C_M, C_{EK}, ID_c, metadados, detalhes de licenciamento, entre outros dados opcionais). A definição de direitos é realizada pelo detentor de conteúdos através de ferramentas apropriadas do SC que especificam os direitos a serem concessionados, assim como a metadados relacionada. Toda esta informação é então transmitida ao SL, que a armazenará para mais tarde poder emitir licenças.
- Distribuição de conteúdo e licenças: o processo de distribuição de conteúdos pode ser desdobrado em duas partes. Na primeira um fornecedor distribui o conteúdo e a licença associada a um consumidor U_1, numa segunda o consumidor U_o redistribui o conteúdo protegido a outro consumidor U_N. Um outro canal de distribuição pode existir quando o consumidor U_N recebe conteúdo protegido através de meios independentes como o correio eletrónico, P2P ou mensagens. O U_N poderá usar o conteúdo se tiver uma licença válida usando o seu dispositivo. Caso não a tenha, terá de a adquirir usando o dispositivo cliente para selecionar o conteúdo e a licença pretendida. Para tal, envia o seu pedido de licença a SL relativo ao conteúdo ID_c conjuntamente com o seu certificado (*CERT_n*).
- Armazenamento da licença: nesta fase os direitos previamente especificados pelo detentor do conteúdo sobre o conteúdo com identidade ID_c, assim como outros metadados são guardadas no SL. Assim que um utilizador elegível pedir uma licença, esta é personalizada de acordo com o seu perfil, guardada e transmitida sob a forma de objeto de direitos.
- Autorização e elegibilidade no licenciamento: nesta fase o SL verifica o pedido do cliente/consumidor identificado por CERT_n e autoriza-o a prosseguir para a obtenção da licença referente ao conteúdo ID_C, caso as suas credenciais sejam válidas. O serviço de licenciamento analisa o pedido de emissão da licença verificando a sua elegibilidade contactando o SGA. A elegibilidade baseia-se em dois critérios: se o utilizador pertence ao domínio (no meio académico basta verificar se o utilizador faz parte da instituição) e se o pedido de licença é elegível para o utilizador em causa, isto é, se se enquadra nos termos e condições definidos previamente pelo detentor do conteúdo (por exemplo, se o mesmo matriculado num determinado ciclo de estudos ou unidade curricular). O SL, através do gerador de licenças, solicita esta informação ao SGA, processa-a e verifica se o pedido é ou não elegível. Consoante o resultado, prossegue (ou não) para a fase correspondente à geração e emissão da licença.

- Distribuição e aquisição da licença: nesta fase, depois de o SL contactar o SGA, obtendo os dados para saber se o pedido de licença é elegível, e verificar se pode emitir uma licença, o utilizador especifica os direitos de utilização através de uma REL, assim como a informação criptográfica necessária para se aceder ao conteúdo protegido. Para tal, o SL procura a C_{EK} para o conteúdo identificado com ID_c previamente enviada pelo SC. A C_{EK} é cifrada através de um algoritmo de chave assimétrica com a chave pública do utilizador, K^{pub}_U, e o SL gera uma licença contendo metadados e os respetivos direitos embebidos numa licença. Esta licença é assinada digitalmente pelo SL de modo a que a integridade e não-repúdio desta possam ser confirmados. A licença pode então ser empacotada com a C_{EK} cifrada e com os metadados relacionados num objeto digital, de acordo com um formato XML específico assinado digitalmente pelo emissor, o SL.
- Interpretação e utilização da licença: o consumo de conteúdo só é possível depois de o cliente autenticar os objetos digitais, autenticar a licença, desencriptar a C_{EK} inserida no objeto licença coma chave privada do utilizador, K^{priv}_U, aplicá-la para decifrar o conteúdo e finalmente obter as regras de utilização definidas na licença não deixando de verificar previamente a legitimidade do utilizador validando se este é a pessoa se enquadra dentro dos termos e condições definidos pelo distribuidor. Como todas as mensagens entre SL, SC e o cliente são cifradas e estes componentes são autenticados, podem usar-se as assinaturas digitais com o propósito de estabelecer o não repúdio. O cliente agirá sobre o conteúdo de acordo com a interpretação das expressões definidas na licença através da REL.
- Consumo de conteúdo: depois de toda a informação estar na posse do cliente (chaves, direitos de utilização e conteúdo) pode dar-se seguimento à utilização do conteúdo. Nesta fase as medidas de segurança implementadas internamente no subsistema da aplicação cliente devem garantir a proteção adequada no decurso da decifra do conteúdo protegido e da sua utilização, sendo impraticável:
  - a extração de conteúdo desprotegido de modo a evitar a sua distribuição ilimitada sem necessidade de o acompanhar e utilizar com a respetiva licença;
  - a extração das chaves criptográficas que iriam assim permitir o acesso não autorizado ao conteúdo e serviços de distribuição.

4 Análise das propriedades de segurança na proposta

Um dos conceitos mais importantes no desenho de sistemas DRM modernos está relacionado com a separação entre conteúdos protegidos e direitos associados (Hwang, 2008). A separação permite que o conteúdo protegido possa ser distribuído livremente, não podendo contudo ser

consumido sem a presença da respetiva licença válida (Hwang, 2008). Por outro lado, esta separação vem permitir que o conteúdo possa ser associado a termos e condições de utilização que podem variar consoante a forma como o mesmo pode ser consumido, fornecendo uma grande flexibilidade e facilidade de gestão no uso do conteúdo e direitos associados (Hwang, 2008). No modelo proposto este conceito é observado havendo separação entre o canal de distribuição do conteúdo protegido e empacotado e o canal de distribuição de direitos. Isso significa que, quando um utilizador pretende usufruir de novos direitos ou renovar direitos sobre conteúdos que já possui, bastará renegociar os novos direitos e solicitar a emissão de uma nova licença, podendo continuar a usar os mesmos conteúdos. Esta questão é particularmente relevante quando o tamanho dos conteúdos é muito grande e estes requerem muito tempo para descarregar.

O conteúdo e a chave que cifra o conteúdo (C_{EK}) contida no objeto de direitos devem ser protegidos no dispositivo do utilizador depois de estarem decifrados, como complemento à proteção implementada no decorrer da fase de transmissão. Um sistema de DRM fornece este tipo de proteção emitindo a licença e respetivo objeto que a contém somente a dispositivos em observância com as regras de segurança que estejam em conformidade. Para tal, o dispositivo deverá ser de confiança possuindo um certificado que o confirme. Para obter este certificado o dispositivo deve estar em conformidade com as regras definidas pela entidade reguladora de confiança no modelo. Este certificado garante ao sistema que o utilizador final não irá comprometer o sistema por fugas na proteção do conteúdo e na licença.

Na proposta apresentada podemos ter duas camadas de cadeias encriptadas que originam diferentes níveis de proteção consoante a perpetiva no fornecedor de conteúdos, no dispositivo dos utilizadores e no canal de comunicação. Esses níveis de proteção visam garantir segurança ponto a ponto, pelo que a segurança global do sistema tenderá a ser avaliada pelo seu elo mais fraco. De seguida, são explicados estes níveis de proteção.

- Proteção da Licença e do Conteúdo no Fornecedor de Conteúdos

  Um fornecedor de conteúdos atua sobre dois servidores: um de licenças e um de fornecimento de conteúdos. As políticas de segurança física são aplicadas para a proteção destes, que vão ao encontro das regras de conformidade e robustez definidas por uma entidade de confiança no modelo testado. Consequentemente, o fornecedor do conteúdo não torna públicos o conteúdo desprotegido nem as chaves.

- Proteção do Conteúdo no Canal de Comunicação

  O conteúdo é normalmente cifrado com uma C_{EK} usando um algoritmo de cifra simétrico (como, por exemplo, o AES). O conteúdo cifrado é enviado ao utilizador final através de um canal de comunicação e o sistema DRM assume que esse algoritmo de cifra simétrica é seguro o suficiente para garantir a confidencialidade e integridade do conteúdo, por isso o conteúdo está sempre sob proteção no canal de comunicação.

- Proteção da Licença no Canal de Comunicação

  A licença desempenha um papel importante pois contém a informação secreta necessária para decifrar o conteúdo, que é enviada à entidade requerente durante a fase de aquisição da mesma. Não sendo um requisito primordial a confidencialidade da licença mas sim a da chave de proteção de conteúdo, C_{EK}, somente esta será cifrada para ser protegida no canal de comunicação. Para isso, é cifrada com a chave pública da entidade requerente, e assinada com a chave privada do emissor. Preservando a confidencialidade da $C_{EK,}$ cifrando-a, e a integridade da licença através de assinatura digital, conclui-se que as licenças são protegidas no canal de comunicação.

- Proteção de Conteúdo e da Licença no Dispositivo do Utilizador Final

  O conteúdo e a licença têm de ser protegidos no dispositivo do utilizador final, como complemento da proteção realizada durante a fase de transmissão. Um sistema DRM fornece um determinado tipo de proteção, criando a licença apenas para os dispositivos que respeitam as regras de conformidade e robustez definidas por uma entidade de confiança num modelo testado. Se isso se verificar, um dispositivo obtém um certificado de uma autoridade reconhecida, certificado esse que assegura ao servidor que o utilizador é de confiança e que não divulgará o conteúdo nem a informação da licença, daí que estes estejam protegidos no dispositivo do utilizador final desde que este obedeça às regras de computação segura.

A aplicação de criptografia garante a confidencialidade do conteúdo assegurando desta forma um nível de proteção satisfatório. Estando o conteúdo devidamente protegido e inserido no objeto conteúdo este último necessita de se manter íntegro. Para tal, a incorporação da assinatura digital do emissor no objeto visa garantir a confirmação dessa integridade levando a que o dispositivo do utilizador rejeite qualquer objeto que a não respeite. O objeto de direitos ao conter a licença e a chave de cifra de proteção do conteúdo torna-se na peça mais importante de todo o sistema pois permite desbloquear o acesso ao conteúdo protegido. Por isso é necessária uma especial atenção ao processo de transferência deste objeto.

De acordo com os requisitos enunciados de transferência de licenças na secção anterior, é possível concluir que:

- O primeiro requisito é satisfeito pois mesmo que terceiros possuam uma licença emitida para um recetor específico, somente este a poderá usar, uma vez que é quem pode fazer prova de que a licença lhe é endereçada já que possui a chave privada correspondente. Ou seja, como a licença está personalizada, esta somente tem utilidade para o utilizador a quem foi endereçada. Além disso, e adicionalmente, a chave de cifra que protege o conteúdo (C_{EK}) inserida no objeto é enviada numa forma cifrada usando a chave pública do recetor. Mesmo que terceiros obtenham a chave cifrada, só o utilizador legítimo para quem foi emitido o objeto digital o poderá utilizar, pois é este que possui a chave privada correspondente da chave pública que encripta a C_{EK}. Ou seja, somente os utilizadores autorizados podem desencriptar a C_{EK} e assim ter acesso ao conteúdo.
- O segundo requisito é igualmente satisfeito pois, ao assumir a incorporação do SGA na arquitetura, o SL poderá verificar a elegibilidade do pedido do cliente para emissão de licença solicitando informações ao SGA sobre o perfil académico de quem faz o pedido e assim validá-lo.
- O terceiro requisito também é satisfeito, pois assume-se aqui que o dispositivo é de confiança e que obedece às regras de segurança estabelecidas e em conformidade com a proteção de conteúdos. Deste modo, assegura-se que chave de proteção do conteúdo é mantida protegida no dispositivo do utilizador, e assim, só o utilizador do dispositivo a pode desencriptar com a sua chave privada não a revelando, exceto para reproduzir o conteúdo.
- Finalmente, o quarto requisito também é satisfeito, pois qualquer modificação não autorizada ou falsificação será detetada, já que a integridade da licença é sempre verificada de acordo com a assinatura digital do emissor da licença.

5 Conclusão

Apesar de a complexidade da proteção de conteúdos abrangidos por direitos de PI no contexto académico ser significativa, foi possível delinear a proposta de solução coerente com o modelo e alinhado com o fluxo de conteúdos no contexto académico. Essa proteção implica a aplicação das medidas corretas com vista a garantir a confidencialidade e integridade dos objetos envolvidos, de modo a preservar os direitos associados, nomeadamente o de atribuição. Tendo por base o modelo proposto por (Nickolova & Nickolov, 2007) foi desenhada uma arquitetura

de referência de um sistema de DRM que possa acomodar o modelo proposto. De acordo com o modelo de gestão de direitos aqui apresentado, a chave (ou chaves) que encripta(m) o conteúdo encontra(m)-se embebida(s) num objeto digital que contém a licença e que está protegida com a chave privada do recetor. Assim, é possível garantir a confidencialidade do conteúdo pois se o recetor enviar este objeto digital contendo a licença a um outro recetor este não poderá aceder ao conteúdo, já que não possui a chave privada do recetor original. Ao oferecer o suporte criptográfico à autenticação de entidades e à proteção dos conteúdos e direitos garante-se assim o controle de acesso ao conteúdo. Ao mesmo tempo a combinação de assinatura e certificados digitais permite verificar a integridade dos objetos e a sua autoria.

Numa perspetiva de segurança é essencial a existência de interações de confiança entre o fornecedor do conteúdo, o emissor de licenças e o sistema de gestão académica. Esta última entidade tem a responsabilidade do envio de dados que permite ao serviço de licenciamento assinalar a elegibilidade de um pedido de licença. Desta forma não só os pedidos de utilizadores legítimos de um determinado domínio são validados (por exemplo, só utilizadores do meio académico podem obter licenças), como também são verificadas condições específicas a que os utilizadores desse domínio devem obedecer antes de a licença ser emitida (por exemplo, estarem matriculados num determinado ciclo de estudos). Este modelo fornece, assim, uma enorme vantagem no que diz respeito à gestão de direitos de PI sobre conteúdos de âmbito académico, pois permite verificar e validar os pedidos de utilização de conteúdo verificando internamente e de forma autónoma a elegibilidade desse pedido.

A análise efetuada ao modelo na perspetiva dos requisitos de transferência de licenças permite concluir que a proposta satisfaz todos os requisitos enunciados, reunindo as condições de segurança para poder ser implementada num sistema de DRM adequado ao contexto educacional. A aplicação de técnicas criptograficas na proteção de conteúdos, num ambiente seguro e de confiança proporcionado pelo DRM, consegue satisfazer as pretensões de grande parte dos participantes relativas à integridade do conteúdo e da satisfação do direito de atribuição. Assim, esta proposta vai ao encontro dos requisitos básicos de segurança (Schneier, 2007) na proteção do conteúdo com vista a garantir confidencialidade, integridade, autenticação e controlo de acesso. A proposta de modelo apresentada fica assim alinhada em conformidade com as pretensões enunciadas nos estudos de (Gadd et al., 2007; Bates et al., 2007) no que se refere às principais necessidades de preservação de direitos no contexto em causa. Mais ainda, vai ao encontro da pretensão de estabelecer um ambiente de confiança, capaz de assegurar a transmissão de direitos respeitando a linha sucessória, como iremos ver de seguida.

Capítulo 5

Proteção de conteúdos e transmissão de direitos

Resumo

Ao longo deste capítulo será dada particular atenção à proteção dos conteúdos e aos seus fundamentos, mas o seu foco incide essencialmente sobre a transmissão de direitos entre participantes no fluxo de conteúdo com o privilégio de emissão de licença. Através de um caso de uso genérico definido, faz-se uma análise do processo de licenciamento no contexto académico. A problemática da aquisição e transferência da licença e consequente transmissão de direitos, assim como o rastreio do licenciamento são os temas aqui analisados exemplificando-se a sua aplicação, sempre que possível, em situações comuns ao meio académico. Além de um novo método de emissão de licenças que permite verificar a elegibilidade dos utilizadores do domínio académico, é proposto um novo mecanismo de retransmissão de licenças entre os utilizadores finais utilizando técnicas de reencriptação. Além deste contributo em que se recorre à reencriptação da chave protetora do conteúdo através da interação com um *proxy*, é também proposto um outro mecanismo baseado em assinaturas digitais que permite rastrear as várias licenças emitidas ao longo da linha sucessória da cadeia de distribuição.

1 Introdução

Os sistemas de gestão de conteúdos mais comuns, ao basearem-se somente em mecanismos de autenticação para que os utilizadores acedam ao conteúdo, não conseguem assegurar que uma vez estabelecido o acesso aos conteúdos, os mesmos sejam utilizados e distribuídos na forma que foi definida pelos seus criadores e distribuidores. Uma vez obtido o conteúdo desprotegido pelo utilizador, o detentor original do conteúdo perde o controlo/governação sobre a forma como este pode ser usado num contexto de utilização potencialmente hostil (Hwang, 2008). Deste modo, para evitar possíveis violações sobre direitos de PI, a utilização e a circulação não autorizadas de conteúdos devem ser evitadas (ou pelo menos controladas e governadas). Um dos aspetos a ter em consideração como forma de garantir o que foi referido anteriormente consiste na utilização de técnicas de proteção, nomeadamente as criptográficas, que permitam

cifrar o conteúdo e "esconder" de terceiros a respetiva chave de cifra que protege o conteúdo (Schreiner, 2011), assegurando que esta só pode ser acedida por quem está credenciado para tal. A robustez do sistema DRM assenta na força do método de ofuscação da chave de proteção do conteúdo (Etinger, et al., 2009), sendo por isso necessário utilizar técnicas que a permitam proteger de forma eficaz.

Para obter uma licença, o utilizador, através do dispositivo, faz um pedido de licença explícito participando ativamente no processo de aquisição (preenche alguns formulários e fornece informação relevante). O emissor da licença usa a informação do utilizador recebida em conjunto com metadados mais relevante para criar um objeto de direitos (licença). De seguida, envia-a para o dispositivo do utilizador. A licença obtida pode ser transmissível para outro utilizador mas não tem qualquer utilidade porque a chave que cifra o conteúdo (C_{EK}) foi cifrada com a chave pública do utilizador (K^{pub}) destinatário original. Para obter a chave de proteção de conteúdo desprotegida aplica-se a chave privada do utilizador (K^{priv}), e então poder-se-á utilizar o conteúdo tendo em conta as regras estipuladas na licença (Figura 35).

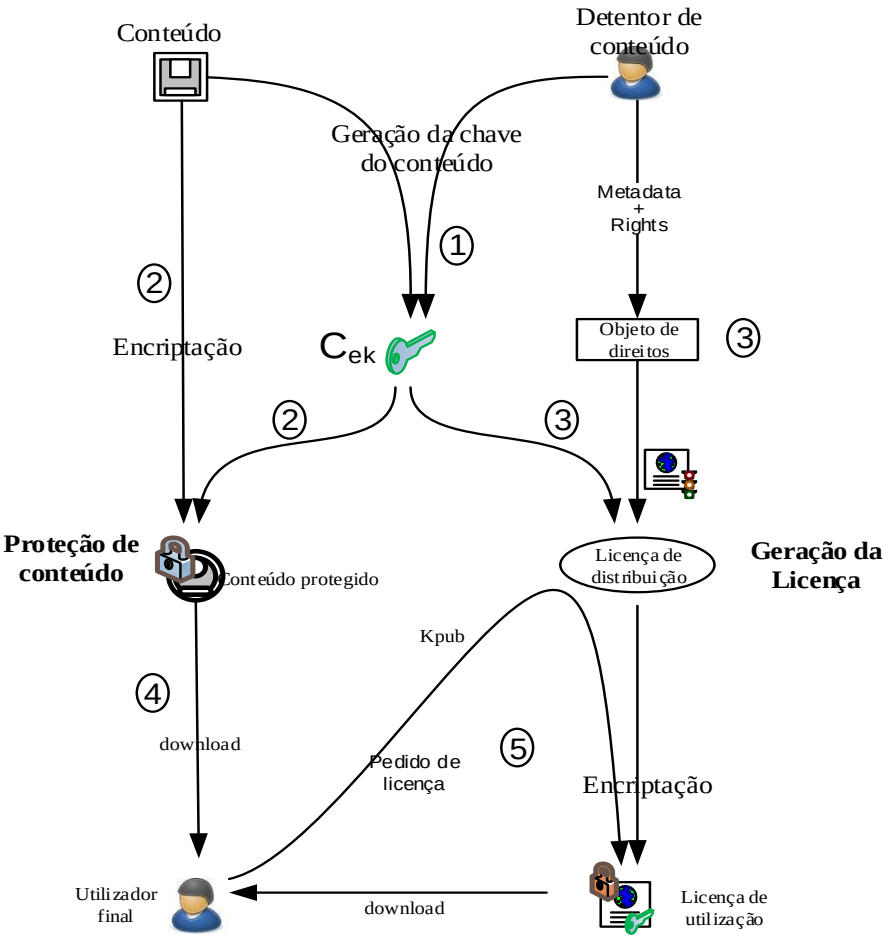


Figura 35 - Utilização de chaves na proteção de conteúdo e geração de licenças

O detentor de conteúdos procede à proteção utilizado mecanismos criptográficos (1) e (2)e adicionalmente define as condições de utilização numa licença de distribuição (3). O utilizador poderá então descarregar o conteúdo para o seu dispositivo (4). Do ponto de vista do utilizador, para este poder adquirir os direitos que pretende, tem de o fazer perante um fornecedor de direitos, o servidor de licenças (5) (Wang et al., 2005). A partir de um leque de possíveis opções definidos pelo detentor do conteúdo, tais como o custo da opção, o domínio em causa e/ou o tipo de utilização, é emitida uma licença ou objeto licença.

No modelo de referência proposto no anterior capítulo, a licença está associada ao utilizador final em vez de um dispositivo. Depois de o utilizador ser autenticado, é-lhe garantido o acesso ao conteúdo se possuir a chave criptográfica de proteção do conteúdo na licença que adquiriu. Nesta perspetiva, o utilizador é que possui um papel de relevo e não o dispositivo, o que implica que o conteúdo possa estar acessível ao utilizador em qualquer dispositivo após a autenticação. A distribuição do conteúdo pode, então, ser feita, mas outros utilizadores não o podem utilizar, porque precisam de adquirir uma licença personalizada em que a chave de proteção do conteúdo (C_{EK}) está "protegida" com a sua própria chave (Marques & Serrão, 2015b). Sem essa licença personalizada não podem usar o conteúdo distribuído por outros utilizadores, mesmo que já estejam autenticados no sistema.

2 Conteúdos e licenças no DRM: caso de uso

Para avaliar um sistema de DRM genérico existente e as hipóteses de convergência em uso geral iremos descrever um caso de uso que será utilizado como base de referência. Assumem-se os seguintes pressupostos:

- O dispositivo do utilizador é inerentemente seguro. Isto é, assume-se que o dispositivo não irá revelar nenhuma chave e que apenas divulgará o conteúdo de acordo com as regras da licença;
- O dispositivo assegura a aplicação dos direitos definidos na licença;
- Todos os utilizadores finais são elegíveis e, consequentemente, autorizados a requerer uma licença desde que estejam devidamente registados e autenticados no sistema;
- Todos os componentes são autenticados por uma terceira entidade;
- A licença (ou objeto de direitos) contém a chave de cifra do conteúdo que, por sua vez, está cifrada com a chave pública do utilizador armazenada no dispositivo (K^{pub}) podendo ser decifrada com a respetiva chave privada (K^{priv}). Para além disso, é assumido que o conteúdo

é cifrado com uma (C_{EK}) e que os algoritmos de cifra são seguros, de modo a garantir confidencialidade e integridade ao (C_{EK}) e ao conteúdo nos seus canais de comunicação;

- O servidor de licenças (SL) e o servidor de conteúdos (SC) são considerados robustos em termos de segurança no respeitante a comunicação com outros componentes.

O caso de uso apresentado está deliberadamente simplificado e baseia-se na versão mais frequente e usual de descarregamento de conteúdo. Para melhor se perceber foi dividido em três possíveis cenários distintos que se apresentam de seguida.

2.1 Aquisição de licença

Neste cenário, um utilizador obtém o conteúdo protegido (com a informação da aquisição de licença) de um Servidor de Conteúdos (SC) através de um dispositivo credenciado. Sempre que pretende usar o conteúdo e não possuir a respetiva licença armazenada é redirecionado para o Servidor de Licenças (SL). Com a informação de aquisição, o utilizador inicia o processo de obtenção da licença correspondente. Para tal, o dispositivo envia uma mensagem de *requisição* ao servidor de licenças e espera pelo resultado. Se o pedido for validado e o utilizador preencher todas as condições pré-definidas, o resultado é enviado (Figura 36), permitindo ao dispositivo descarregar a licença.

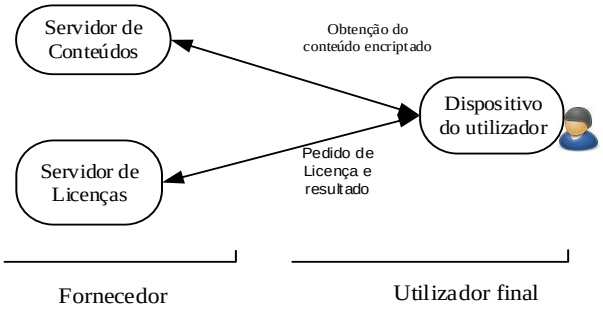


Figura 36 – Cenário de aquisição de licença

O pedido de aquisição de licença é realizado pelo utilizador U a SL enviando o respetivo certificado Cert_U, e a identificação do conteúdo ID_C.

- U => LS: Cert_U ; $K^{priv}_U(ID_C)$

O SL valida o pedido de licença e dá início à geração da licença personalizada para o utilizador U, de acordo com uma estrutura predefinida incorporando metadados e a chave de proteção do conteúdo encriptada, C_{EK}. Antes de autorizar o utilizador a descarregar a licença, o SL confirma a identidade deste e da assinatura do pedido de licença, valida o pedido e, caso haja

confirmação, procede à emissão da licença (*lic*) para o utilizador U. Contudo, antes de a emitir, esta é assinada digitalmente por SL para garantir a integridade e não repúdio da licença.

2.2 Transferência de conteúdo e licença

Um utilizador, via dispositivo credenciado, descarrega conteúdo de um Servidor de Conteúdos (SC) sendo redirecionado para o Servidor de Licenças (SL). De seguida, com a informação da aquisição obtida, obtém do SL a licença correspondente, o que ocorre da mesma forma que no cenário de "Aquisição de Licença". Se o dispositivo do utilizador transferir o conteúdo para um outro dispositivo, o processo repete-se, tal como no cenário da "Aquisição de Licença" (Figura 37), devendo o novo recetor adquirir uma nova licença ao SL. Contudo, se transmitir a licença a terceiros o conteúdo permanece sem qualquer utilidade para o recetor.

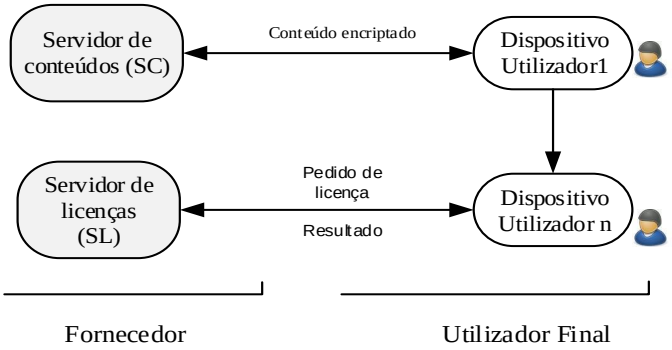


Figura 37 – Aquisição e transferência de conteúdo e licença

O detentor de conteúdo, caso não tenha a licença respetiva, terá de a obter diretamente do distribuidor. Esta característica de "interrupção de seguimento" da licença pode dar suporte a vários modelos de negócio para o detentor de conteúdos, inclusive no contexto académico onde os membros, podendo pertencer ao mesmo grupo, (departamento, ciclo de estudos, unidade curricular) podem ter interesse em controlar a circulação de licenças nesse grupo. Este aspecto é interessante no contexto educativo, pois a noção de membro de um determinado grupo está bastante enraizada no contexto académico (departamentos, ciclos de estudos, turmas) e podendo esses mesmos grupos obter essas licenças de uma forma fácil, mas ao mesmo tempo controlada pelo fornecedor, tal pode ajudar ao estabelecimento do DRM no contexto académico.

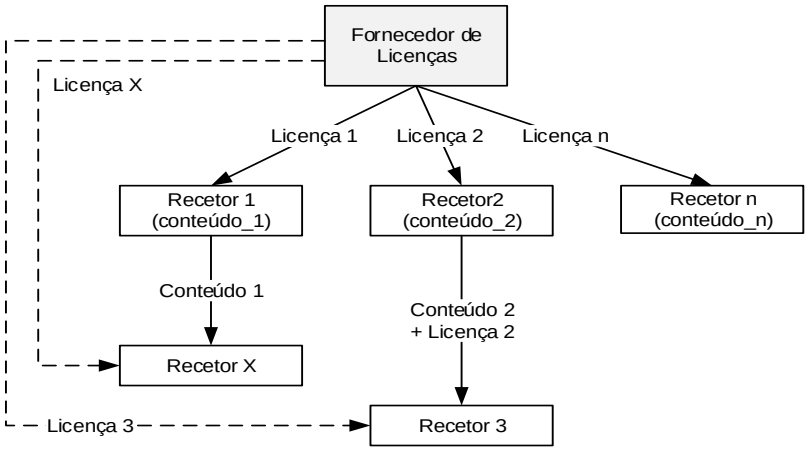


Figura 38 – Fluxo de informação na obtenção de licenças

Contudo, nada impede que o fornecedor possa distribuir licenças entre os seus membros, mas concedendo direitos entre eles de uma forma que não coloque em causa o princípio de posse nem os direitos originais definidos pelo detentor de direitos, desde que implemente mecanismos específicos que preservem a autenticidade da licença.

2.3 Transmissão de direitos entre utilizadores

O facto de as licenças emitidas para os utilizadores estarem personalizadas torna o seu valor nulo quando a licença é transmitida de utilizador para utilizador. Este tipo de sistemas baseados na identidade do utilizador, ou seja, na individualização da licença, arrasta consigo um outro problema: a portabilidade da licença. Para contornar este problema terão de ser implementados mecanismos específicos que permitam a emissão de licenças de um utilizador final para outro desde que seja observado o princípio de posse, pois só assim se garante uma utilização legítima do conteúdo. Independentemente do problema da portabilidade da licença, e para que um utilizador possa transmitir direitos a terceiros, este terá de estar previamente autorizado. Essa autorização depende de o detentor progenitor de direitos na linha sucessória ter definido a concessão de direitos a terceiros na licença. Desta forma, o retransmissor de direitos atua como um delegado autorizado a operar como licenciador de outras licenças secundárias tendo por base os direitos originais definidos na licença primária. Contudo, os direitos concessionados expressos na licença secundária não devem exceder os direitos concedidos na licença primária (Sachan, & Emmanuel, 2011), cuja linha sucessória tem origem no detentor de conteúdo.

Um delegado pode ser definido como "a pessoa autorizada a atuar como representante de outra". Na delegação de direitos encadeados, o licenciador delega no licenciado a autoridade de atuar como licenciador de um conjunto de direitos. Se possível, o licenciador deverá ser capaz de controlar qualquer parte da licença de utilização para delegação. A delegação é, assim,

importante, pois permite ao detentor de direitos original controlar a delegação ao longo da linha sucessória de transmissão de direitos. A emissão de licenças só será interrompida se a licença expirar ou se as condições que exprimem o privilégio de emitir licença o indicarem. Deste modo, pode-se concluir que qualquer participante no ciclo de vida do conteúdo pode atuar indiscriminadamente no papel de detentor de conteúdo, distribuidor ou consumidor.

Ao construir uma licença para distribuir a terceiros, o emissor da mesma deve possuir Privilégios de Emissão da Licença (PEL), ou seja, de concessão de direitos. Se estes privilégios forem incluídos, então o recetor desta licença primária pode emitir uma licença secundária para outro requerente sem que este consulte o progenitor da licença primária. Para tal deve existir um elemento especial na estrutura da licença que represente o PEL atribuído ao emissor da licença. Tal pode viabilizar a transmissão de direitos facilitando a distribuição de conteúdos a uma escala sem precedentes, pois evita que os utilizadores tenham de contactar diretamente o autor, ou múltiplos progenitores da cadeia de distribuição (Wenqing, Wanting & Di, 2005), mantendo-se ao mesmo tempo o controlo sobre a governação dos direitos.

Podemos exemplificar considerando o caso de um Professor que emite uma licença que permite aos seus alunos visualizar o conteúdo e também o possam distribuir aos seus colegas (alunos) nas mesmas condições. Assumindo que o professor atribuiu ao servidor de licenças (SL) o direito de distribuir as suas licenças, e que todos os participantes estão registados e autenticados no sistema, podemos considerar os seguintes passos na aquisição da licença (Figura 39):

1. O Aluno 1 interage com o servidor de licenças (SL) e faz um pedido de uma licença com PEL para um conteúdo C_{enc} identificado por ID_c (a) ;
2. O servidor de licenças (SL*)* verifica se o Aluno 1 é elegível. Para tal, contacta um servidor de validação (SV) que aloja dados do aluno (por exemplo, o sistema de gestão académica) e pede-lhe o envio de dados (b);
3. LS recebe os dados de SV, processa-os, e se o resultado for positivo então LS verifica se a licença padrão definida pelo detentor do conteúdo (por exemplo, Professor A) permite emitir licenças do tipo PEL. Caso a verificação seja positiva, valida-os de acordo com os direitos da linha sucessória e procede à emissão da licença PEL. O Aluno 1 descarrega a licença e armazena-a no seu dispositivo (c);
4. O Aluno 2 na posse do conteúdo C_{enc} identificado por ID_c pede então uma licença com PEL ao Aluno 1 (d);
5. Ao receber o pedido, o Aluno 1 contacta o SV solicitando dados referentes ao Aluno 2 (e);

6. Se o resultado do processamento dos dados da resposta do SV for positivo, o dispositivo do Aluno 1 verifica se a licença permite emitir licenças PEL. Caso a resposta seja positiva, emite uma licença PEL de acordo com os direitos da linha sucessória e envia-a para o Aluno 2, que a armazena (f);

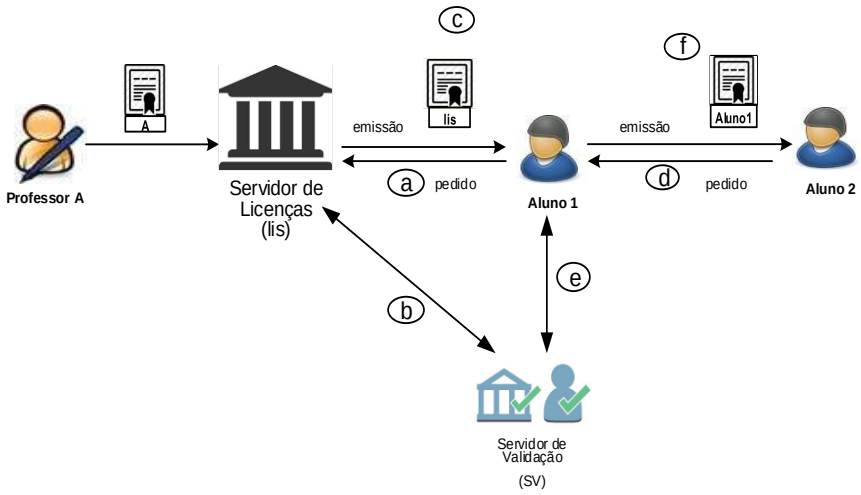


Figura 39 – Transmissão de licenças entre utilizadores

Caso um outro aluno requeira uma licença ao Aluno 2 os passos repetem-se. Assim, desta forma um aluno (ou até mesmo um professor se estiver habilitado para tal) pode facilmente disseminar conteúdos (através da concessão de direitos) usando uma licença PEL, delegando os direitos que lhe foram concessionados. O processo apenas será interrompido quando:

- na licença emitida exista alguma condição que o impeça (como, por exemplo, o número de delegações, o prazo de validade, entre outros).
- o SV enviar dados que não autorizam o licenciado (por exemplo, o aluno não pertence à instituição)
- a licença primária não permitir a emissão de licenças para o perfil do licenciado (por exemplo, a licença primária define que a licença deve ser emitida só a alunos do Curso_x)
- a integridade da licença estiver comprometida.

No decorrer da transmissão de licenças entre os utilizadores convém referir que os direitos do detentor têm de ser preservados ao longo da linha sucessória de direitos. Essa preservação, ao ser concretizada na proteção de conteúdos, pode definir a forma de transmissão da licença. Essa forma deve ter em conta as seguintes situações:

- Impedimento de uso – o utilizador pode não ser capaz de usar uma licença depois de esta lhe ter sido retransmitida;

- Prevenção do uso continuado – o utilizador pode não ser capaz de continuar a usar a licença depois de a retransmitir a terceiros;
- Impedimento de retransmitir a licença a terceiros – o utilizador só poderá emitir uma licença se possuir privilégios de emissão da licença;
- Prevenir licenciamento não autorizado – somente quem for definido como licenciador é que pode retransmitir a licença;
- Não repúdio – o utilizador que retransmite a licença não poderá negar que o fez;
- Rastreabilidade – o detentor deve ser capaz de rastrear os re-emissores da licença.

Apesar de serem utilizados mecanismos criptográficos robustos que realizam a proteção de conteúdos com grande fiabilidade, nem sempre se consegue dar resposta a todas estas situações. No modelo proposto, a inserção da componente que permite verificar a elegibilidade dos pedidos dos utilizadores para emissão de licença contribui significativamente para dar algumas respostas a estas situações, pois a licença só é emitida se o recetor pertencer ao domínio académico e se se verificarem os requisitos iniciais do detentor. Contudo, existem muitas outras situações em que somente através da utilização de uma REL suficientemente versátil se conseguirá dar resposta a esta situação (por exemplo, impedir que não haja mais que uma única retransmissão de licença). Nos capítulos 9 e 10 iremos abordar essa questão propondo soluções e exemplificando através de casos de uso recorrendo a uma REL baseada na norma MPEG-21.

2.3.1 Licença emitida entre utilizadores e assinaturas digitais

Um outro problema relacionado com a transmissão de direitos entre utilizadores relaciona-se com a transmissão da chave de proteção do conteúdo e com a assinatura digital da licença. No caso de uso descrito, uma vez que a licença contém uma chave cifrada com a chave pública do recetor, se este transmitir esta licença a terceiros, nunca estes poderão decifrá-la a menos que possuam a chave privada desse mesmo emissor. Ou seja, só este utilizador pode usar o conteúdo depois de obter a chave secreta que cifra o conteúdo aplicando a sua chave privada. O mesmo acontece com a assinatura digital da licença. Para solucionar este problema, é proposta uma solução baseada na reencriptação da chave de proteção do conteúdo a qual pode passar por duas abordagens distintas: a reencriptação pelo dispositivo ou a reencriptação através de *proxy*.

2.3.1.1 Reencriptação pelo dispositivo

Uma primeira abordagem para desenhar uma solução passaria pela proposta de reencriptação da chave de proteção do conteúdo pelo utilizador final emissor no dispositivo antes de este a

enviar na nova licença para outro utilizador. Para que esta seja válida, esta deve ser compatível com a licença padrão progenitora do detentor de direitos ou distribuidor autorizado de forma a respeitar a linha sucessória de emissão de direitos. Ou seja, em cada passo de emissão de licenças o emissor envia uma licença onde os direitos são condicionados pelos que foram originalmente definidos na licença progenitora. Se a licença obedecer ao padrão, então a chave criptográfica pode ser transferida para a nova licença. Assim, pode-se garantir que o princípio de posse é observado. Para tal, propõe-se a implementação de um mecanismo que contemple a seguinte sequência de operações, na emissão da licença.

Pressupõe-se que os utilizadores estão registados e devidamente autenticados no sistema possuindo um par de chaves (K^{pub}_{U}, K^{priv}_{U}) armazenadas no dispositivo cliente. Além disso, o utilizador que vai distribuir direitos ($U_{\mathbf{1}}$) está na posse de uma licença com os direitos sobre um determinado conteúdo e que lhe permite delegar direitos a terceiros (U_n) através da emissão de uma licença.

O utilizador final $U_{\mathbf{1}}$ extrai da licença a chave de proteção do conteúdo C_{EK} usando a sua chave privada (K^{priv}) num algoritmo de chave assimétrica A.

- $A_K\,(K^{priv}U_1, A_K\,(K^{pub}U_1\,, C_{EK}\,)) \Rightarrow C_{EK}$

O utilizador final ($U_{\mathbf{1}}$) cifra novamente a chave de proteção (C_{EK}) com a chave pública do utilizador recetor ($U_{\mathbf{n}}$) para quem pretende emitir a nova licença.

- $A_K\,(K^{pub}{}_{U\mathbf{n}}\,,\, C_{EK}\,) \Rightarrow C_{EK}$

A licença é então reconstruída tendo por base a licença do utilizador emissor U_1 e assinada por este com a sua chave privada.

- $\text{Lic}(D_{\mathbf{sig}}U_1) = \text{lic}U_1 + \text{signature}_{U1} = \text{Lic}\,(D_{sig}D) - A_K(K^{pub}{}_{U1}, C_{EK}) + A_K(K^{pub}{}_{Un}, C_{EK}) + \text{signature}_{U1}$

onde:

$\text{Lic}\,(D_{sig}D) = \textit{lic} + \text{signature}_{\mathbf{D}} = \textit{lic} + \text{Dsig}\,(K^{priv}{}_{D}, \textit{lic})$

$\text{signature}_{U1} = \text{Dsig}\,(K^{priv}{}_{U\mathbf{1}}, \text{lic}\,U_1)$

Pode-se inferir que a nova licença é constituída por:

- $\text{Lic}\,({}_{Dsig}U_1) = \textit{lic} + \text{Dsig}\,(K^{priv}{}_{D}, \textit{lic}) - A_K(K^{pub}{}_{U1}, C_{EK}) + A_K[K^{pub}{}_{Un}, C_{EK}) + \text{Dsig}\,(K^{priv}{}_{U\mathbf{1}}, \text{lic}U_1)$

Esta licença é então enviada para o outro utilizador final (U_n) que, por sua vez, verifica a assinatura digital com a chave pública de U_1 (as chaves públicas ficam armazenadas na autoridade de autenticação no ato de registo dos utilizadores no sistema). Para que a comparação seja positiva, os resumos devem ser iguais (*digest1=digest2*).

- $Dsig\ (K^{pub}_{U1}, signature_{U1}) = Dsig\ (lic + Dsig\ (K^{priv}_{D}, lic) - K^{pub}_{U1}\ (C_{EK}) + K^{pub}_{Un}\ (C_{EK})$

Se a comparação for positiva, procede-se então à desencriptação do conteúdo com a cifra obtida do resultado da operação de desencriptação utilizando a sua chave privada sobre a chave do conteúdo encriptado por U_1.

- $A_K\ (K^{priv}_{Un}\ ,\ A_K(K^{pub}_{Un}\ , C_{EK}\ )) \Rightarrow C_{EK}$

Daqui em diante o utilizador final poderia proceder do mesmo modo e distribuir a licença recebida para outros utilizadores, caso esta não tenha restrições de distribuição que o impeçam.

2.3.1.2 Reencriptação por *proxy*

Uma segunda abordagem passaria pela proposta de utilização de um *proxy*. A abordagem seguida passa pela adoção de técnicas de *re-cifra* (Ateniese & Hohenberger, 2005; Schmidt et al., 2004) e de *re-assinatura* (Ateniese & Hohenberger, 2005; Libert & Vergnaud, 2008) através de um *proxy*. O esquema de *re-cifra* através de um *proxy* permite que uma entidade mediadora transforme um texto cifrado com a chave pública do utilizador A (K^{pub}_A) num outro que pode ser decifrado com a chave privada de B (K^{priv}_B) de tal modo que a entidade mediadora não obtém qualquer informação acerca do conteúdo do texto cifrado. Por outras palavras e aplicando-o ao contexto do DRM, o *proxy* não consegue saber qual é a chave secreta (C_{EK}) que encripta o conteúdo. No esquema de *re-assinatura* por *proxy*, uma entidade mediadora (*proxy*) atua como tradutor entre duas partes convertendo uma assinatura válida e publicamente verificável de A sobre uma mensagem *m*, DsigA(*m*), numa assinatura de B sobre a mesma mensagem DsigB(*m*) (Blaze, Bleumer & Strauss, 1998; Libert & Vergnaud, 2008). Contudo, o *proxy* não necessita de saber qualquer chave da assinatura e não pode assinar mensagens arbitrárias como sendo A ou B (Blaze et al., 1998; Libert & Vergnaud, 2008).

Se esta entidade mediadora ficar incorporada no sistema DRM, mais propriamente no servidor de licenças, pode-se então delinear um mecanismo de transferência de licenças entre utilizadores recorrendo a estas técnicas. Uma vantagem de usar re-assinaturas através de *proxy* está na possibilidade de construir as assinaturas de licenças de tal modo que estas sejam verificadas usando a chave pública do fornecedor. Para tal, o utilizador B usando o dispositivo

D_B pode verificar uma assinatura convertida usando somente a chave pública do fornecedor de licenças.

A incorporação de um módulo que atue como *proxy* permite que não só a C_{EK} possa ser re-cifrada, mas também a licença primária que a contém e que está assinada pelo emissor original possa ser re-assinada pelo utilizador emissor da nova licença a outro utilizador. Ou seja, o SL poderá assim re-assinar a nova licença contendo a $C_{EK,}$ mas protegida pela chave pública do utilizador recetor. Este mecanismo permite assegurar a manutenção do nível de segurança do sistema DRM sem que exista uma grande alteração na sua arquitetura, pois a execução é realizada no SL. Para formalizar o conceito de re-cifra através de *proxy*, podemos considerar os seguintes passos de acordo com Blaze, et.al., (1998):

1) Geração de Chaves: $G(_K)$;
2) Este algoritmo gera uma chave pública K^{pub} e uma chave privada K^{priv};
3) Geração da chave de re-cifra: $ReK_{A=>B} = ReKey\ (K^{priv}_A, K^{pub}_B)$;
4) Para uma chave privada de A e uma chave pública de B, este algoritmo cria a chave $ReK_{A=>B}$ que permite re-cifrar um texto cifrado por A num outro cifrado por B;
5) Cifra: $A_k\ (K^{pub}_B, m)$:

   Para um recetor B da mensagem *m* com a chave pública (K^{pub}_B), o algoritmo produz uma mensagem cifrada *m1* que pode ser re-cifrada com a chave de re-cifra apropriada;

6) Re-cifra: ReEnc ($ReK_{A=>B,}$ *m1*):

   Este algoritmo toma como parâmetros a chave de reencriptação $ReK_{A=>B}$ e a mensagem cifrada *m1* com a chave pública de A, para produzir um mensagem cifrada, *m2*, com a chave pública de B;

7) Decifra: $D_k(K^{priv}_I, mi)$:

   Este algoritmo toma como parâmetros uma chave privada K^{priv}_I de uma entidade I e a mensagem cifrada *mi* encriptada com a sua chave pública K^{pub}_I, para produzir a mensagem *m*.

Além disso, para qualquer mensagem e qualquer par de chaves (K^{pub}_A, K^{priv}_A), (K^{pub}_B, K^{priv}_B), os algoritmos devem satisfazer as seguintes condições de exatidão:

- $D_k(K^{priv}_A, A_k(K^{pub}_A, m)) = m$
- $D_k(K^{priv}_B, ReEnc(ReKey(K^{priv}_A, K^{pub}_B), A_k(K^{pub}_A, m))) = m$

No mecanismo proposto, faz-se recurso a uma entidade intermediária (*proxy*) facilitadora da transferência segura de direitos entre os utilizadores. Este *proxy*, sendo capaz de executar funções de *re-cifra*, incorpora-se no modelo proposto através da sua implementação no SL de acordo com as interações da Figura 40.

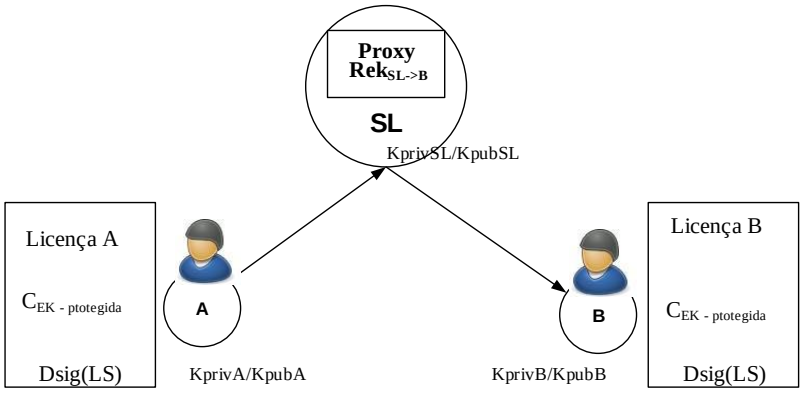


Figura 40 – Integração do *proxy* na estrutura proposta

A integração do *proxy* na estrutura do sistema DRM proposto permite ir ao encontro dos seguintes requisitos:

- suportar modelos de licenciamento suficientemente flexíveis e eficazes e possuir uma baixa complexidade computacional;
- suportar o conteúdo encriptado de modo a que o utilizador final não o possa extrair e armazenar numa forma não encriptada.

Para melhor percebermos o modo de funcionamento do *proxy* na estrutura DRM, iremos assumir que os utilizadores estão registados e devidamente autenticados, e que possuem o respetivo par de chaves (K^{priv}_U, K^{pub}_U), armazenados num dispositivo de confiança certificado, sendo a aplicação de controlo DRM resistente a adulterações. O utilizador (U_1), que pretende distribuir direitos, está na posse de uma licença emitida por um servidor de licenças SL, devidamente assinada por este, que lhe permite conceder direitos a terceiros (U_n) através de PEL. Assume-se também que o dispositivo emissor da licença e o que a recebe têm a capacidade de reproduzir o mesmo formato de conteúdo e que os seus algoritmos de cifra são iguais.

Consideremos então que o utilizador U_n requer uma licença *lic* ao utilizador U_1 para o conteúdo identificado por ID_c. O dispositivo do utilizador U_1 verifica o PEL e, se o resultado for positivo, direciona o pedido para o servidor de licenças SL e envia-lhe conjuntamente a licença referente. Este verifica a elegibilidade do pedido face às condições expressas na licença perante o Servidor de Validação (SV). Caso a resposta seja positiva, extrai a chave do conteúdo protegido,

($K^{pub}_{U1}(C_{EK})$), gera a respetiva chave de re-cifra, $ReK_{SL=>B} = ReKey(K^{priv}_{SL}, K^{pub}_{Un})$, e envia-os ao *proxy* através de um canal seguro (por exemplo, via SSL). O *proxy* procede então à re-cifra da chave do conteúdo protegido para obter uma nova chave cifrada com a chave pública do requerente U_n.

- $ReEnc(ReK_{SL=>B,} K^{pub}_{U1}(C_{EK})) = ReEnc(ReKey(K^{priv}_{SL}, K^{pub}_{Un}), K^{pub}_{U1}(C_{EK})) = K^{pub}_{Un}(C_{EK})$

O *proxy* envia esta nova chave protegida com a chave pública do utilizador que a requereu para o servidor de licenças (SL), que então procede à geração e emissão de uma nova licença (*lic')* contendo a chave re-cifrada. Esta licença será assinada digitalmente pelo SL, de modo a que se possa observar a sua integridade e não repúdio. Finalmente, a licença é enviada ao utilizador emissor U_1, que por sua vez autoriza o utilizador requerente U_n a proceder ao descarregamento (Figura 41).

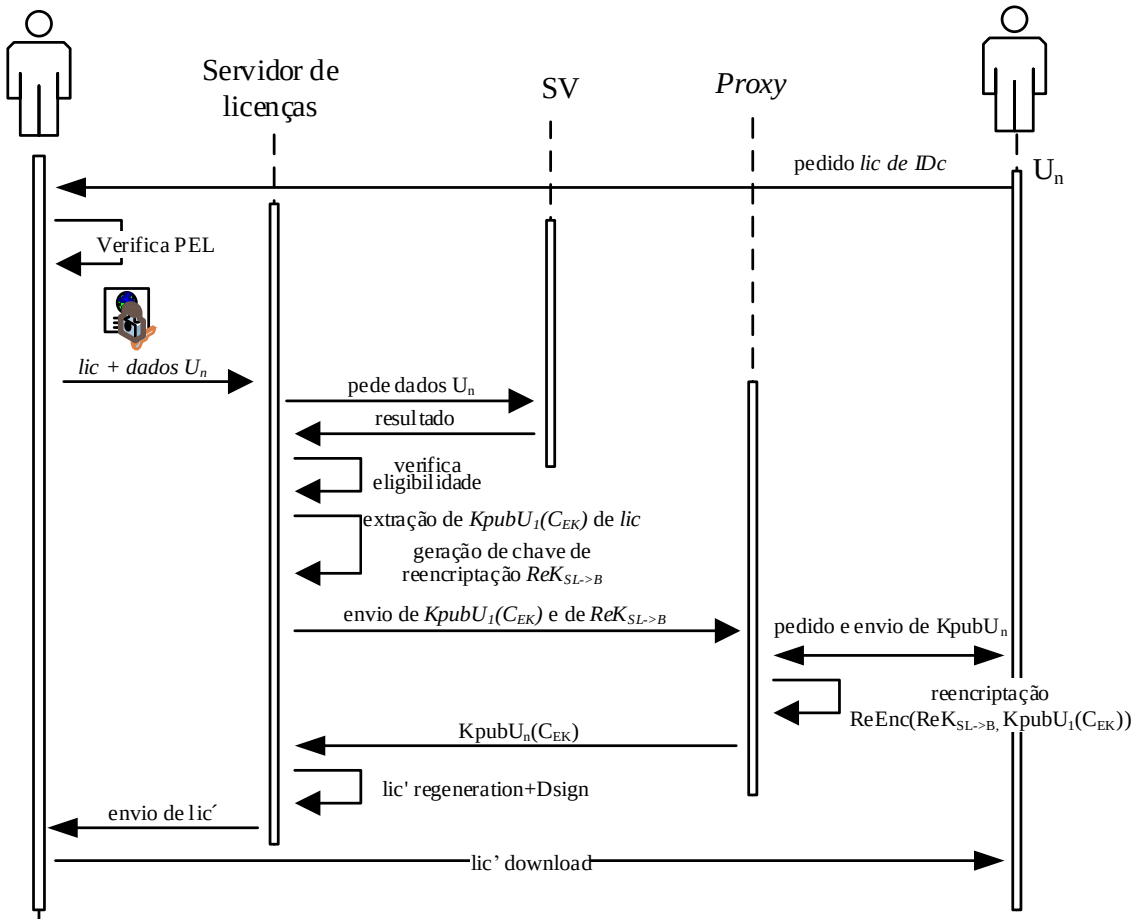


Figura 41 – Reencriptação por *proxy*

De referir que, estruturalmente, a integração do módulo *proxy* também se poderia efetuar fora do servidor de licenças, mas isso traria maior complexidade ao sistema no que diz respeito a segurança e número de interações.

2.4 Rastreio do licenciamento

Uma das particularidades da abordagem proposta na solução anterior reside na possibilidade de traçar um rasto da utilização do conteúdo à medida que as licenças são distribuídas entre os utilizadores. Visto a licença final incorporar a assinatura digital do emissor da licença progenitora, é possível então estabelecer toda a linha sucessória em termos de emissão de licenças ao longo da cadeia de distribuição. Suponha-se o caso de um Professor que emite uma licença que permite que os alunos só possam visualizar o conteúdo e o possam também distribuir aos seus colegas nas mesmas condições. Assim, temos um professor (Professor A) que permite a um servidor de licenças (SL) emitir licenças de utilização para os seus alunos e estes, por sua vez, poderão redistribuí-las por outros alunos. Inserindo a identificação do progenitor na licença emitida podemos facilmente saber quem já utilizou aquele conteúdo com aquela licença. A Figura 42 tenta ilustrar este cenário correspondente ao fenómeno de superdistribuição (Wang, Liu & Lee, 2007) nos sistemas de DRM.

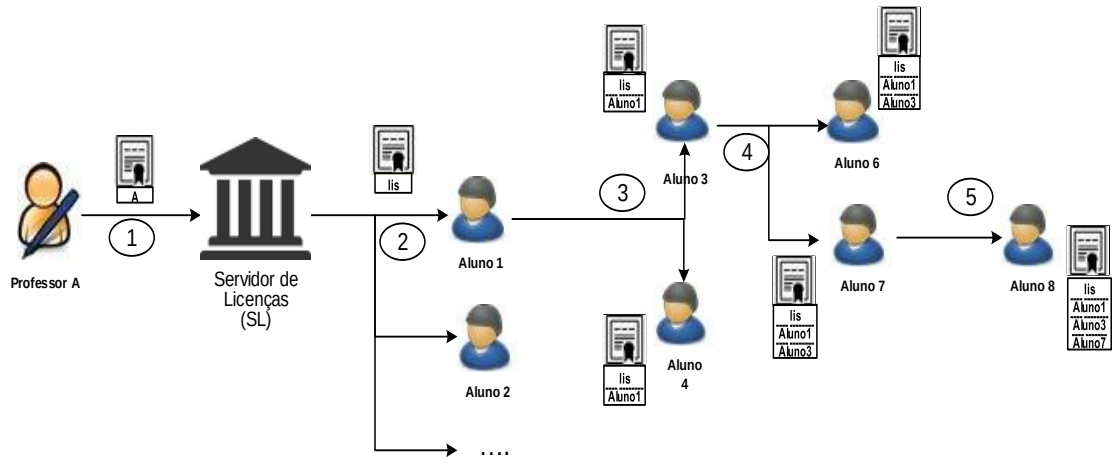


Figura 42 – Distribuição de licenças entre utilizadores no meio académico

Tomando por exemplo o cenário ilustrado na Figura 42 podemos inferir que a licença do Aluno 8 foi emitida pelo Aluno 7. Por sua vez, a licença do Aluno 7 foi emitida pelo Aluno 3. A do Aluno 3 foi emitida pelo Aluno 1 e este tem, por sua vez, uma licença emitida pelo servidor de licenças SL, que a obteve do Professor A. Por outro lado, e tomando por referência a segunda proposta de solução, sendo o SL a emitir a respetiva licença, podemos assim efetuar um rastreio e monitorização das licenças uniformemente a partir de um ponto central no sistema. Deste

modo, e independentemente da linha sucessória de direitos ficar registada na licença, podemos estabelecer centralmente a linha sucessória dos direitos transmitidos, pois qualquer licença emitida pelo servidor central ficará registada com o respetivo destinatário. No Capítulo 7 iremos verificar como se pode materializar esse rastreio recorrendo à norma MPEG-21 REL.

Qualquer uma das soluções requer sempre a ligação à Internet de modo a haver a validação do pedido de licença para o domínio em causa (neste caso o académico) e verificar se o utilizador requerente se enquadra dentro do perfil com que os direitos foram inicialmente definidos na licença principal ao longo da linha sucessória.

3 Conclusão

No modelo de gestão de direitos anteriormente proposto, a proteção da PI sobre o conteúdo fica assegurada pela utilização de mecanismos criptográficos no empacotador, na aplicação cliente e no gerador de licenças. O empacotador gera pacotes cifrados individuais, usando uma chave secreta diferente para cada conteúdo a cifrar. Cada uma dessas chaves é embebida nas licenças referentes ao conteúdo desse pacote, o que significa que só o possuidor destas licenças poderá decifrar e usar os conteúdos do pacote. A chave secreta que decifra o conteúdo por criptografia de chave simétrica encontra-se embebida na licença, estando protegida com a chave pública do recetor. Se um utilizador final enviar esta licença a um outro recetor, este não poderá aceder ao conteúdo, pois não possui a chave privada do recetor original. Para obviar a tal e potenciar a disseminação de licenças, o modelo inicial é estendido propondo-se um mecanismo que permite transmitir licenças e conceder direitos entre utilizadores. É assim proposto um mecanismo que recorre a reencriptação da chave protetora do conteúdo através da interação com um *proxy*, assim como um outro mecanismo baseado em assinaturas digitais que permite rastrear as várias licenças emitidas ao longo da linha sucessória da cadeia de distribuição.

Para garantir o sucesso da solução, o sistema de DRM interage com o sistema de gestão académica da instituição, de modo a verificar a elegibilidade dos utilizadores finais na obtenção das licenças de utilização dos conteúdos. Tal permite verificar se um utilizador faz parte do domínio académico em causa e se obedece às condições em que a licença pode ser emitida, através da valição dessa mesma licença a ser emitida através de dados provenientes da interação com um Servidor de Validação, (o SGA). Na proposta apresentada, é possível realizar, desta forma, a proteção de conteúdos e direitos associados recorrendo a uma solução com vários mecanismos onde os conceitos e tecnologia de DRM são aplicados ao contexto académico.

Capítulo 6

OpenSDRM adaptado ao contexto educacional e académico

Resumo

Neste capítulo é demonstrado o alinhamento de uma plataforma "aberta" DRM, o OpenSDRM adaptado ao contexto académico, com o modelo proposto anteriormente. Assim, é possível enquadrar o modelo proposto com uma solução DRM já existente com caraterísticas capazes de ter sucesso no contexto académico, nomeadamente o facto de se apresentar como tecnicamente "aberta" e por isso poder adaptar-se ao contexto em causa. O contributo dado passa assim pela apresentação de uma plataforma adaptada ao contexto académico capaz de contribuir para uma solução do problema de partilha de conteúdos e direitos associados abrangidos por PI. Tendo por base uma abordagem baseada numa arquitetura orientada por serviços *Web* que a torna bastante flexível, esta plataforma é capaz de suportar as interações de validação de emissão de licenças com o sistema de gestão académica normalmente existente nas instituições educacionais, com vista à realização da transferência de direitos entre participantes no domínio educacional.

1 Introdução

Apesar da existência de um número variado de sistemas e arquiteturas de gestão de conteúdos protegidos, a grande maioria corresponde a sistemas proprietários com especificações de acesso privado com pouca aderência a normas internacionais. Tal não só condiciona qualquer análise comparativa (Delgado et al., 2005a), como também a implementação de interfaces com aplicações externas ou até outros sistemas de DRM. Tal como anteriormente foi mencionado, a alternativa mais viável são soluções abertas suportadas por especificações de domínio público, assentes em normas internacionais, capacitadas para fornecer interfaces de conectividade com outras plataformas e cuja implementação seja baseada em código aberto.

Na sua génese o OpenSDRM foi concebido como uma plataforma de DRM orientada a serviços, independente do tipo de conteúdo, onde os vários módulos que o constituem foram desenhados para serem implementados usando a abordagem interoperável baseada numa arquitetura orientada por serviços (SOA, Servise-Oriented Architecture) (Figura 43) suportada por serviços

Web recorrendo ao protocolo SOAP (Serrão, Dias & Delgado, 2005b). Isto faz com que tenha uma grande flexibilidade no que respeita ao desenvolvimento de módulos num ambiente distribuído, permitindo manter as funcionalidades básicas independente da plataforma e linguagem de programação (Serrão, Dias & Delgado, 2005a). Por outro lado, oferece suporte a todo o ciclo de vida dos conteúdos, e permite adaptar-se aos mais variados modelos de negócio (*download*, superdistribuição, *streaming* e *broadcasting)* (Serrão et. al, 2005a) onde diferentes e variados intervenientes estão envolvidos.

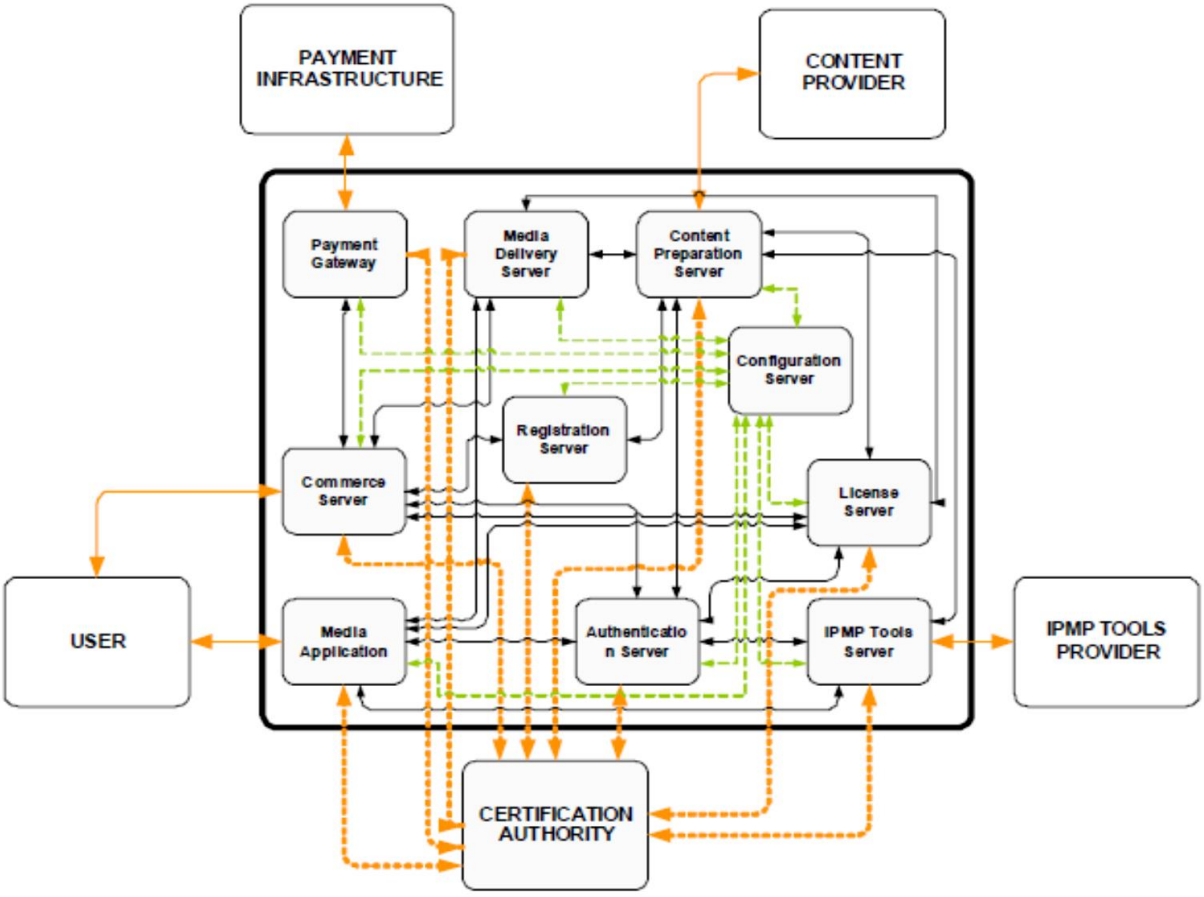


Figura 43 – Arquitetura orientada a serviços do OpenSDRM (Serrão, Dias & Delgado, 2005b)

O OpenSDRM implementa uma solução de DRM tradicional para a proteção de direitos sobre os conteúdos digitais, a qual pode ser aplicada na publicação e negociação/comercialização dos mesmos (Serrão & Siegert, 2004). Pela análise realizada anteriormente a diversas soluções "abertas" de DRM, foi possível identificar o sistema OpenSDRM (Delgado et al., 2005a; Serrão, Fonseca, Dias, & Delgado, 2006a) como uma solução de DRM suficientemente flexível para poder ser utilizada em qualquer ambiente, não sendo por isso de estranhar a possibilidade de esta se adaptar ao contexto académico.

A estrutura do OpenSDRM e as funcionalidades disponibilizadas através de uma arquitetura orientada por serviços tornam-na suficientemente flexível para poder ser facilmente adaptada ao contexto académico tendo em conta o modelo proposto. A sua arquitetura, suportada por especificações de tecnologia ”aberta”, vem permitir uma incorporação facilitada de alguns dos mecanismos das normas MPEG-21 com vista à proteção e partilha de conteúdos e direitos associados abrangidos por PI. A segurança, independentemente do domínio de aplicação de qualquer sistema de DRM, é um fator a ter em consideração e no caso do contexto académico não é exceção, pois a preservação de direitos como os que estão mais relacionados com a integridade do conteúdo e o direito de atribuição requerem a aplicação de medidas de proteção. O OpenSDRM não descura este aspeto sendo um dos seus aspetos fortes como vimos no Capítulo 3.

2 OpenSDRM – características, funcionalidades e serviços

As operações disponibilizadas por cada um dos serviços fundamentam-se em serviços baseados no protocolo SOAP. Uma das muitas vantagens das funcionalidades proporcionadas por este tipo de serviços reside na possibilidade de os desdobrar por diferentes subsistemas de acordo com as necessidades das diferentes aplicações a serem implementadas. Tal proporciona uma maior modularidade ao sistema, pois diferentes subsistemas (ou módulos) podem ser implementados consoante a funcionalidade requerida (Serrão, Fonseca, Dias, & Delgado, 2006a). Ao mesmo tempo, podem ser partilhados serviços comuns a diferentes módulos com requisitos diferentes, com a consequente redução de custos. Alguns exemplos das funcionalidades dos serviços relacionam-se com:

- Distribuição – relacionada com a funcionalidade de transferência de conteúdo e licenças;
- Segurança – relacionada com a funcionalidade de licenciamento e proteção de conteúdo e licenças;
- Gestão – relacionada com a funcionalidade de registo e localização do conteúdo.

De forma sucinta podem citar-se algumas das características mais importantes do OpenSDRM:

- Mecanismo automático de registo dos seus componentes e procedimentos de certificação baseados em certificados X.509 para cada componente;
- Processo de autenticação mútuo de componentes e atores baseados em certificados digitais. O mesmo processo é utilizado por atores e componentes, interrogando a servidor de autenticação (AUS) pelo estado das credenciais utilizadas. Mas, no caso da autenticação de um ator, o componente Agente DRM é o principal responsável que lida

com a autenticação. No mecanismo de autenticação o OpenSDRM recorre sempre às credenciais completas para assegurar que o processo de autenticação é bastante robusto;

- A aplicação de direitos sobre o conteúdo sempre que o utilizador o consome é assegurada pelo Agente DRM do OpenSDRM. Este *middleware* pede e gere as licenças e executa as autorizações localmente, sendo contudo agnóstica relativamente à REL utilizada. As autorizações de acesso dos utilizadores são baseadas nos direitos especificados nesta licença ao utilizador. Um único agente DRM pode ser usado no mesmo dispositivo por diferentes aplicações de reprodução;
- O OpenSDRM fornece um servidor de preparação de conteúdos, que recebe o conteúdo original, codifica-o e embebe-o num formato específico ao mesmo tempo que o protege e adiciona metadados;
- O OpenSDRM fornece um interface específico para ligar a plataformas externas de pagamentos.

Independentemente das diferenças existentes nas múltiplas arquiteturas de DRM, existem contudo pontos comuns entre elas que permitem a identificação dos principais atores e serviços, os quais contribuem para a definição de um sistema genérico de DRM. De um modo geral, independentemente do domínio de aplicação em que se posicionam, qualquer sistema DRM é direcionado para agir sobre as atividades exercidas no conteúdo quer haja a intervenção do utilizador final, detentor de conteúdo ou fornecedor de conteúdo, oferecendo mecanismos de governação do mesmo (Grzonkowski, S., 2010). Para tal, tem de oferecer um conjunto de funcionalidades que permitam a estes atores conduzir as suas operações sobre o conteúdo. Tal como foi referido anteriormente (Capítulo 2), estas funcionalidades são disponibilizadas pelo sistema DRM sob a forma de um conjunto de serviços com vista à gestão dos direitos. Cada um dos serviços anteriormente mencionados estabelece relações entre si de modo a garantir níveis de proteção concordantes com o domínio em que se posicionam. A grande diferença do OpenSDRM relativamente a outras implementações DRM reside na capacidade de lidar com diferentes serviços chave de gestão de direitos como serviços distribuídos, escondendo os detalhes da implementação dos diferentes atores ao mesmo tempo que disponibiliza as suas funcionalidades, expondo-as para poderem ser utilizadas (Serrão et al., 2006a). Esta abordagem permite que estes serviços chave fiquem disponíveis em redes abertas como a Internet, ao mesmo tempo que viabiliza que outros serviços possam ser implementados em consonância com os serviços já mencionados. Para além disso, vários outros fornecedores de soluções de DRM poderão implementar interfaces específicos expondo as suas funcionalidades básicas a

outros serviços sem revelar detalhes de implementação. A integração entre todos estes serviços permite estabelecer ambientes suficientemente adaptáveis a um domínio de aplicação específico, possibilitando a implementação de diferentes modelos de negócio (Serrão et al., 2006a).

Tendo por base de referência o modelo anteriormente proposto pode-se observar que os vários componentes do OpenSDRM se enquadram aí consoante a função desempenhada. Por outro lado, tendo por base de referência a arquitetura de DRM generalista e tendo em conta a estrutura referida em (Yang et al., 2008; Patriciu, et. al., 2011), não é difícil verificar a compatibilidade do OpenSDRM relativamente aos quatro componentes base desta arquitetura. A presença dos principais blocos é notória sendo somente de realçar a falta de um componente relacionado com a verificação da elegibilidade do utilizador no meio académico, ou seja, o servidor de validação (SV). Contudo, sendo esta componente uma entidade externa gerida autonomamente (o Sistema de Gestão Académica - SGA), pode ser facilmente considerada na estrutura do OpenSDRM com vista à sua aplicação no meio académico, disponibilizando os serviços necessários para se verificar a elegibilidade dos utilizadores neste meio. Podemos assim estabelecer as seguintes equivalências (com a exceção da componente *Authentication and Accounting*) entre componentes OpenSDRM e a estrutura funcional do DRM (Capítulo 2).

OpenSDRM		Blocos da estrutura funcional DRM
"End User System"	↔	Bloco de Utilização (verificação de aplicação de direitos, rastreio e monitorização)
"Content Management System"	↔	Bloco de Gestão/Distribuição (repositório)
		Bloco de Criação (preparação do conteúdo, atribuição de direitos)
"License Service"	↔	Bloco de Gestão/Distribuição (licenciamento, transação)
"Payment system"	↔	Bloco de Gestão/Distribuição (transação)
"Protection Tools System"	↔	Bloco de Criação (preparação de conteúdos)

Tabela 6 – OpenSDRM e estrutura funcional DRM

Podemos também estabelecer os seguintes relacionamentos entre componentes OpenSDRM e as funcionalidades no modelo proposto (Capítulo 4).

OpenSDRM		Funcionalidades do modelo proposto
"Authentication and Accounting System" e CA	↔	Pedido de certificado e registo
"Content Management System"	↔	Preparação do conteúdo e metadados
"Content Management System"	↔	Empacotamento do conteúdo e contentores
"License Service" e "Protection Tools System"	↔	Chaves de encriptação, metadados e licenciamento de direitos
"Content Management System" e "License Service"	↔	Distribuição de conteúdo e licenças
"License Service"	↔	Armazenamento da licença
"Payment system" e "License Service"	↔	Autorização e elegibilidade no licenciamento
"License Service" e "End User System"	↔	Distribuição e aquisição da licença
"End User System"	↔	Interpretação e utilização da licença
"End User System"	↔	Consumo de conteúdo

Tabela 7 – OpenSDRM e funcionalidades do modelo proposto

Tendo em conta os vários serviços disponibilizados pela plataforma OpenSDRM, podemos observar que os sete serviços básicos comuns a qualquer sistema de DRM (Serrão, 2008) também se encontram presentes (o serviço de pagamentos é realizado através de uma entidade externa).

OpenSDRM		Serviço
"Content Management System"	↔	Serviço de conteúdos
"License Service"	↔	Serviço de licenças
"Authentication and Accounting System"	↔	Serviço de controlo de acesso
"License Service"	↔	Serviço de rastreio
"Payment system"	↔	Serviço de pagamentos/financeiro
"Protection Tools System" e "Content Management System"	↔	Serviço de importação
"Authentication and Accounting System"	↔	Serviço de identificação
Entidade externa ao OpenSDRM (CA)	↔	Serviço de certificação (opcional)

Tabela 8 – OpenSDRM e serviços

Desta análise pode-se concluir da existência de um forte relacionamento entre o modelo proposto e o OpenSDRM que, salvo ligeiras diferenças, não impedem a existência de equivalências entre atores participantes e componentes. Além disso, e não estando restrito a um tipo de norma pré-estabelecido, o OpenSDRM é suficientemente flexível e adaptativo para poder fazer uso das mais recentes normas atuais, nomeadamente aquelas que estão relacionadas com a norma MPEG-21, de forma a satisfazer os requisitos contemporâneos de controlo de utilização de conteúdos. A sua adaptação ao contexto académico teve sempre em vista a incorporação dos cenários de utilização mais correntes neste meio com o intuito de facilitar a disseminação de conteúdos onde os direitos de PI fossem respeitados de acordo com a proposta de modelo de DRM. Para além de poder incorporar as novas técnicas/tecnologias assinaladas na norma internacional MPEG-21, fornece as bases para a implementação de todo um sistema de autenticação, gestão de eventos ocorridos, licenças reconhecíveis e interpretáveis pelos sistemas computacionais e métodos de proteção de conteúdo a ser partilhado, capazes de dar o suporte aos requisitos dos intervenientes na proteção de conteúdos abrangidos por PI no meio académico. Sendo suficientemente flexível para se adaptar às normas MPEG-21, o OpenSDRM permite que o conteúdo possa ser embebido em "itens digitais", independentemente do seu formato, assim como as licenças expressas através da REL específica do MPEG-21, contribuindo assim para o estabelecimento de uma solução capaz de realizar a gestão de conteúdos abrangidos por PI.

2.1 Aspetos de segurança no OpenSDRM

Sendo o DRM uma agregação de tecnologias de segurança, esta acaba por ser um dos requisitos mais importantes a ter em conta em qualquer sistema deste tipo (Ku, et. al., 2004). Em termos de segurança, o OpenSDRM assegura a coexistência de duas camadas: uma para o nível aplicacional e outra para o nível de comunicação (Serrão et. al.,, 2005b). A sua interdependência é mútua sendo o nível global definido pela segurança da camada mais fraca. No nível de comunicação são usados certificados X.509 e o protocolo SSL/TLS instalados em servidores que permitem viabilizar a autenticação e encriptação (Serrão, et.al., 2005b). Este nível permite assegurar canais de comunicação autenticados e seguros para que os componentes possam comunicar entre si. O nível aplicacional é estabelecido de forma a assegurar que mecanismos de integridade e não repúdio possam ser estabelecidos. Este nível corresponde à permuta interna de mensagens SOAP de forma segura entre os serviços disponibilizados no OpenSDRM e entre atores externos e esses serviços (Serrão, et.al., 2005b).

Cada um dos serviços que fazem parte do OpenSDRM usa este modelo de segurança em duas camadas (Serrão, et.al., 2005b). Pelo nível de comunicação, o OpenSDRM pode assegurar a autenticidade dos servidores HTTP e a confidencialidade do canal de comunicação entre esses servidores, enquanto, ao nível aplicacional, pode garantir a autenticação, integridade e não repúdio dos diferentes serviços e atores que interagem na plataforma, que até podem ser independentes do serviço *Web*. A plataforma OpenSDRM tem sido usada e testada em diversos cenários de utilização (Serrão, Dias & Delgado, 2005a) dando por si garantias suficientes no respeitante à proteção aplicada. O OpenSDRM fornece um ambiente seguro na realização das operações típicas de um sistema DRM fazendo uso, sempre que necessário, de ferramentas de criptografia simétrica e assimétrica, credenciais digitais e protocolos seguros, dando assim realce às funcionalidades relacionadas com a proteção de conteúdos (Serrão, 2008; Serrão & Siegert, 2004). Além de preencher os requisitos básicos de qualquer sistema DRM, o facto de se apresentar como uma arquitetura de especificações e código aberto torna-a fortemente atrativa para poder incorporar especificações de normas internacionalmente reconhecidas como o MPEG-21, assim como garantir a sua adaptação para outros cenários. Os requisitos básicos de segurança (Schneier, 2007) que o OpenSDRM tem de observar atuando em conjunto com o MPEG-21 terão de ir ao encontro de proteção do conteúdo com vista a garantir confidencialidade, integridade, autenticação e o controlo de acesso.

- Confidencialidade - Os dados armazenados e transmitidos devem ser convenientemente protegidos contra possíveis revelações não autorizadas. Este critério é satisfeito no OpenSDRM, pois não só o conteúdo é armazenado de forma encriptada, como também é transmitido entre componentes por canal seguro. A especificação dos componentes MPEG-21 IPMP (MPEG-21:IPMP, 2006) permite assegurar um elevado nível de confidencialidade, fazendo recurso a diversas ferramentas criptográficas que podem ser incorporadas no OpenSDRM para proteção do conteúdo assegurando uma forma fácil de transmissão graças a documentos XML DID (MPEG-21:DID, 2005);
- Integridade - Os dados transmitidos devem ser genuínos não sendo alteráveis no decurso da transmissão. O suporte que o MPEG-21 IPMP (MPEG-21:IPMP, 2006) fornece relativamente a tecnologias de resumo e de assinaturas digitais garante a confidencialidade dos dados transmitidos pela plataforma OpenSDRM;
- Autenticação - A identificação mútua entre os intervenientes no decorrer de uma transação deve ser assegurada. O OpenSDRM assegura a utilização de vários tipos de autenticação como os baseados em criptografia de chave pública e assinaturas digitais, os quais têm suporte pelo MPEG-21;

- Controle de acessos - Somente utilizadores legítimos devem ter acesso a recursos específicos. Este é um dos objetivos básicos da arquitetura OpenSDRM que é atingida através do MPEG-21 IPMP quando se define objetivamente o utilizador com acesso ao conteúdo. A forma como este o poderá usar dependerá dos direitos a ele atribuídos na licença expressa através da MPEG-21 REL (MPEG-21:REL, 2005).

3 MPEG-21, modelo proposto e adaptação do OpenSDRM

O OpenSDRM define uma arquitetura capaz de suportar uma plataforma de gestão de direitos sobre conteúdos protegidos que é bastante abrangente, já que esta não é dirigida é um domínio de aplicação específico, e também pode ser adaptada para suportar uma grande diversidade de tecnologias e mecanismos com suporte em normas internacionais. O OpenSDRM, sendo tecnologicamente neutro, pode suportar os mecanismos das normas MPEG-21 o que o torna suficientemente adaptativo e flexível para que quer o conteúdo (independentemente do seu formato) quer as licenças possam ser embebidos em itens digitais MPEG-21.

A abordagem aqui proposta é orientada para a criação de mecanismos que protejem o conteúdo partilhado e os direitos associados, possibilitando a partilha de conteúdos ao utilizador final nas condições definidas pelos termos de utilização, oferecendo mecanismos de governação do conteúdo ao longo da cadeia de distribuição no contexto académico. Para poder ser utilizada no contexto académico não comercial em que se faz recurso às especificações da norma MPEG-21 na proteção e transporte de conteúdo abrangido por PI terá necessariamente de ser adaptada. Na proposta, essa adaptação passa em primeiro lugar pela incorporação de uma entidade externa independente que forneça o serviço de dados conveniente capaz de possibilitar a verificação da elegibilidade do utilizador no meio académico respeitante à emissão de licenças para um determinado conteúdo. Essa adaptação pode ser realizada de duas formas: acompanhando o ciclo de vida do conteúdo ou considerando os dois lados em que o ciclo tem existência nos sistemas DRM, o lado servidor e o lado cliente do consumidor/utilizador.

Do lado servidor há a considerar duas vertentes: a primeira vertente considera a incorporação de serviços *Web* num servidor de gestão académica (SGA), que disponibilize os dados referentes ao perfil do requerente da licença quando o servidor de licenças (SL) lhos solicite a pedido do cliente. A segunda vertente considera a incorporação de um módulo de preparação de conteúdo protegido num objeto digital pelo servidor de conteúdos (CPS) e outro no servidor de licenças (SL) para gerar objetos de direitos de acordo com as especificações MPEG-21, com as ferramentas de proteção suportadas. Através da incorporação de um módulo especial no SL

que cruze dados disponibilizados pelos serviços do SGA com os do requerente da licença previamente autenticado, torna-se possível verificar a sua elegibilidade. Esta verificação pode ser realizada em duas fases. Numa primeira fase, o servidor de licenças recebe os dados do SGA e verifica se o requerente da licença pertence ao meio académico. Numa segunda fase, o servidor de licenças verifica se os direitos expressos pelo detentor de direitos (por exemplo, o autor) sobre o conteúdo numa licença modelo estão em conformidade com os direitos pedidos pelo utilizador e a serem emitidos na licença de utilização. Caso estas condições se verifiquem, então o SL procede à emissão das licenças empacotando-as num objeto digital (documento DID), contendo a chave de proteção do conteúdo encriptada com a chave assimétrica do utilizador e respetivos metadados. Um procedimento semelhante é usado no CPS na preparação do conteúdo, incorporando um módulo semelhante que através do SGA verifica se o detentor do conteúdo está inserido no domínio académico. Assim, podemos controlar a emissão de licenças para utilizadores legítimos dentro do domínio académico.

Do lado cliente, independentemente de outras funcionalidades de proteção, o Agente DRM do OpenSDRM terá de desempacotar o objeto digital correspondente ao documento que embebe o conteúdo e o que embebe a licença e a chave de proteção de conteúdo. Na posse destes objetos poderá dar início à utilização do conteúdo. Independentemente de outros critérios anteriormente citados, do ponto de vista tecnológico, podemos enunciar os requisitos básicos a que o OpenSDRM terá de responder, de modo a integrar-se com o MPEG-21 e com o modelo de gestão de direitos anteriormente proposto.

- Possibilidade de interação com um servidor que disponibiliza dados sobre o perfil académico dos utilizadores. Só depois de os utilizadores estarem autenticados no sistema se deverá executar a verificação de elegibilidade dos detentores de conteúdos e dos utilizadores finais para preparar e consumir conteúdos, respetivamente.
- O servidor de preparação, empacotamento e encriptação de conteúdos, CPS, deverá atuar em conformidade com a norma MPEG-21, possuindo módulo(s) que permita(m) a proteção do conteúdo e empacotando-o(s) num objeto conteúdo de acordo com uma estrutura predefinida.
- O servidor que armazena e prepara as licenças para emissão, o SL, deverá atuar em conformidade com a norma MPEG-21 possuindo módulo(s) que permita(m) a criação de objetos de direitos de acordo com uma estrutura predefinida, contendo a chave de proteção do conteúdo, metadados e licenças expressas através de linguagem MPEG-21 REL. Este servidor somente emitirá licenças se o pedido do utilizador obedecer aos

termos da licença padrão criada no ato de preparação do conteúdo, devendo para isso fazer uma validação prévia antes de emissão.

- O módulo cliente deverá ser capaz de interpretar e decifrar os objetos digitais, correspondentes ao objeto conteúdo e objeto de direitos contendo o conteúdo protegido e a licença embebida segundo a norma MPEG-21, respetivamente. Este módulo deve ser capaz de extrair a chave de proteção do conteúdo embebida no objeto de direitos e interpretar e fazer aplicar os direitos expressos na licença sobre o conteúdo.

4 OpenSDRM e a arquitetura orientada por serviços *Web*

A abordagem seguida no OpenSDRM baseada em serviços *Web* vem tornar possível o interface com sistemas externos como, por exemplo, sistemas de gestão de conteúdos, plataformas de comércio eletrónico e inclusive os sistemas de gestão académica (SGA) existentes nas instituições académicas e educacionais. O nível de integração irá assim depender dos interfaces implementados e consequente integração de serviços disponibilizados pelo SGA. A implementação de um módulo específico no SGA que assegure a ligação ao OpenSDRM, disponibilizando serviços *Web* é aqui de enorme importância. A figura seguinte (Figura 44) ilustra a arquitetura global do OpenSDRM e as interações com componentes externos via serviços *Web*.

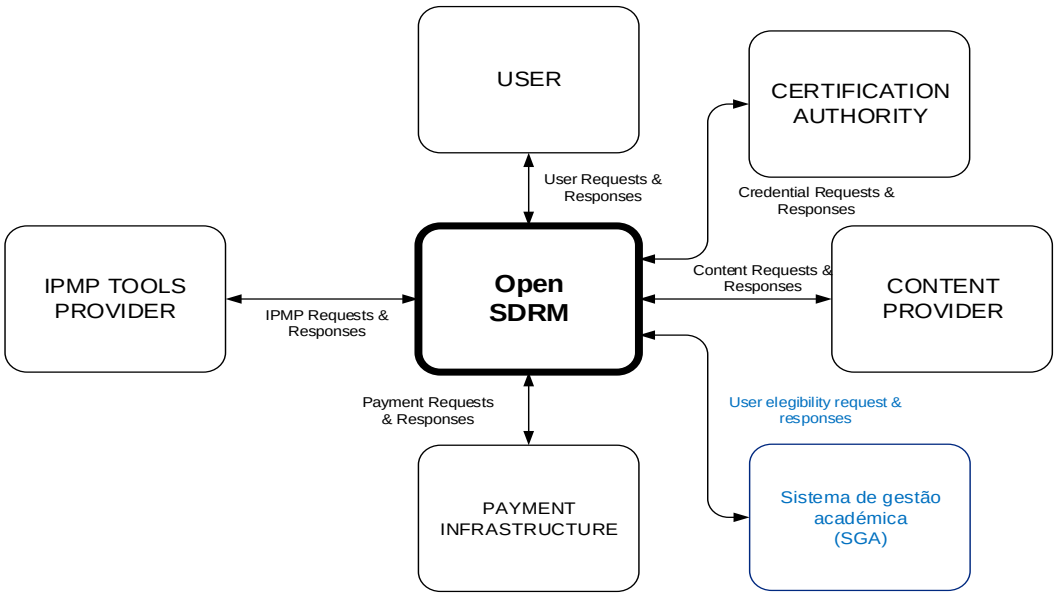


Figura 44 - OpenSDRM e interação com componentes externos (adaptado de Serrão, 2008)

A arquitetura detalhada do OpenSDRM, ilustrando os seus principais serviços, foi adaptada para poder suportar as interações com a plataforma SGA, o que envolve a alteração de alguns

serviços já existentes e a introdução de novos, e pode ser visualizada através na seguinte figura (Figura 45). Foi introduzida uma nova entidade (SGA) que vem permitir através dos interfaces adequados a obtenção de informação necessária e complementar o OpenSDRM para que este possa garantir o correto funcionamento quer na proteção quer na gestão de direitos de PI.

Ao existir uma integração ao nível de serviços disponibilizados entre a plataforma de gestão académica (SGA) e a plataforma de gestão de direitos OpenSDRM, torna-se possível a permuta de informação, de modo a validar toda informação necessária à concessão de direitos. Ou seja, sempre que o OpenSDRM necessita de informação relacionada com o perfil académico de um utilizador, este solicita os dados ao SGA pelo interface adequado, através do serviço apropriado. A informação retornada é avaliada pelo componente OpenSDRM que a pediu dando-se seguimento ao procedimento seguinte, de modo a validar a concessão dos direitos a quem os solicitou.

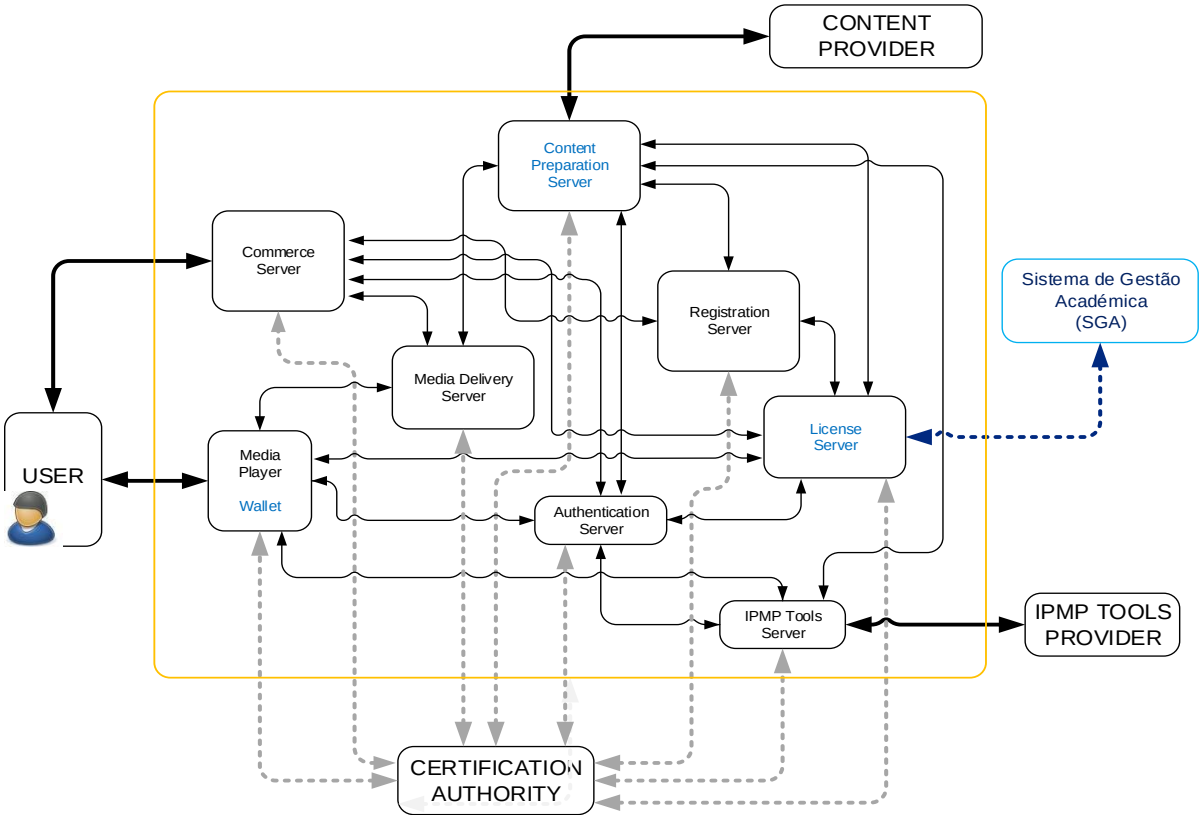


Figura 45 - Arquitetura do OpenSDRM adaptado (adaptado de Serrão, 2008).

Os serviços mais diretamente ligados ao SGA localizam-se no License Server (LIS), no CPS e no Authentication Server (AUS). O SGA possui um interface que implementa um serviço, em que sempre que é solicitado autentica a sua origem dando a respetiva resposta. A informação solicitada é posteriormente enviada a quem a solicitou no OpenSDRM. Todas as mensagens

trocadas entre os componentes e o SGA são baseadas em SOAP sobre SSL. Desta forma, e perante um pedido efetuado por um utilizador, a elegibilidade do pedido em si (por exemplo, verificar se o aluno está matriculado numa determinada Universidade) e também de certos direitos sobre conteúdos (por exemplo, verificar se o aluno pertence ao ciclo de estudos em que o conteúdo pode ser distribuído) pode ser imediatamente verificada. Os principais momentos em que há uma forte interação entre o OpenSDRM e o SGA ocorrem durante o registo do utilizador e do conteúdo, definição de direitos sobre o conteúdo e o pedido de emissão de licença. A integração do SGA com o OpenSDRM resume-se essencialmente a serviços relacionados com:

- Pesquisa de identidades: serviço que disponibiliza a procura de entidades (por exemplo, utilizadores, ciclos de estudos, anos escolares, unidades curriculares, entre outros) retornando os respetivos dados LIS.
- Gestão de utilizadores: serviço que possibilita o registo e manutenção de informação relacionada com utilizadores no OpenSDRM a partir do SGA e aplica os mecanismos apropriados de mapeamento para estabelecer correspondências com vista à compatibilização dos dois sistemas.

O serviço que disponibiliza a pesquisa de identidades pode envolver o retorno de informação com diferentes níveis de complexidade. Um nível bastante simples corresponde a um cenário em que um componente OpenSDRM pede informação sobre se um utilizador está matriculado na Universidade para verificar se o utilizador é elegível dentro do domínio académico da instituição. Um outro mais complexo corresponde a um cenário em que o utilizador, depois de passar o primeiro nível, e ao fazer um pedido de emissão de licença para um determinado conteúdo, tem de satisfazer as condições expressas na licença progenitora. Se as condições forem específicas ao domínio académico e se forem satisfeitas (através da verificação com os dados retornados pelo SGA), então o nível mais complexo fica também ultrapassado, o que permite validar o pedido de emissão de licenças do utilizador dentro do domínio académico. Para limitar o número de serviços disponíveis referentes à pesquisa de identidades, o SGA incorpora um serviço que disponibiliza toda a informação relevante do perfil académico do utilizador (identidade, ciclos de estudos, unidades curriculares, ano escolar, propinas, entre outros). Com a informação retornada do SGA, o módulo do LIS pode dar continuidade à operação em curso, desde uma simples verificação da elegibilidade do utilizador até uma validação da emissão de licenças (Figura 46).

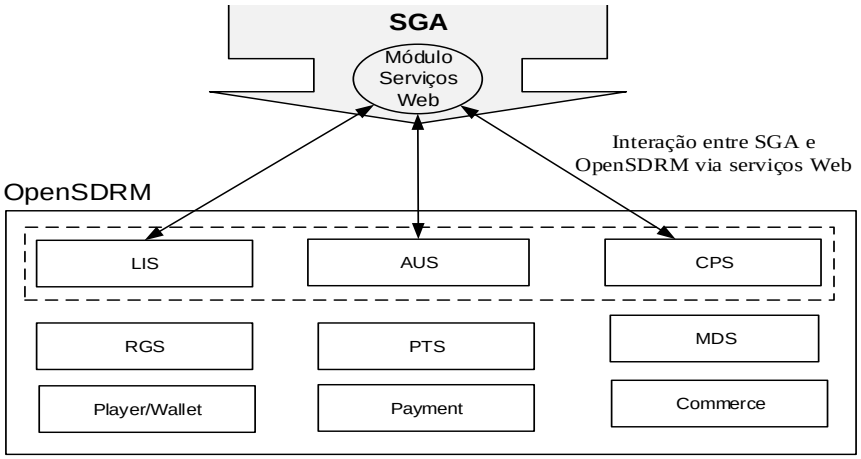


Figura 46 – Integração dos componentes OpenSDRM com os serviços *Web* do SGA

As licenças de uso no contexto académico podem ser solicitadas preenchendo a informação necessária apresentada no formulário relacionado com a licença de distribuição. Isto inclui informação suficiente sobre a instituição, assim como informação que identifica o estudante ou professor não só perante o sistema OpenSDRM, como também perante o SGA, informação essa, que poderá incorporar parâmetros específicos que permitem uma ligação a um contexto educativo específico, de acordo com a licença a emitir. Assim, se o autor de conteúdo, ao interagir com a licença modelo, definir que as licenças a emitir futuramente só poderão ser geradas para uma determinada instituição, ciclo de estudos e/ou unidade curricular, então o utilizador final pode ser filtrado consoante o seu perfil obedecer, ou não, a estas condições. Para tal, o LIS interage com o SGA e, com os dados recebidos verifica se o requerente é elegível e se as condições de âmbito académico (por exemplo, o ciclo de estudos ou unidade curricular) estão em conformidade com o perfil do aluno aí registado. Caso seja elegível, então uma licença específica para esse utilizador será criada. Para garantir a aplicação de direitos sobre o conteúdo expressos na licença através da REL, o mesmo é efetuado por um Agente DRM, que integra a solução OpenSDRM, num componente que opera do lado do utilizador.

De um ponto de vista de segurança torna-se necessário que o sistema DRM, assegure que os novos serviços adicionados fiquem registados e certificados como válidos antes de interagirem com quaisquer dos outros serviços. Visto cada um dos serviços residirem num servidor Web o processo de certificação dos mesmos envolve, do ponto de vista do transporte, a utilização de uma infraestrutura de PKI que suporta a geração e emissão de certificados digitais. Do ponto de vista aplicacional, o SGA é registado como um serviço da plataforma de DRM, processo descrito em Serrão, Torres, Delgado, & Dias (2006d), e permite estabelecer um ambiente de confiança entre o SGA e os restantes serviços (como por por exemplo, o LIS). O servidor de

autenticação (AUS) é aqui um serviço central que permite o registo e autenticação de atores e de novos serviços constituintes do sistema (Serrão,et al., 2006d).

Tal como para os serviços tradicionais do OpenSDRM, a confiança entre o SGA e o LIS é garantida pela implementação dos mesmos mecanismos de segurança baseados em certificados digitais X.509 que fazem parte da infraestrutura PKI. O processo de registo e autenticação do SGA é idêntico ao dos outros serviços do OpenSDRM sendo o AUS a entidade que executa essa função garantindo assim a autenticação do novo componente.

Tendo em atenção que grande parte dos sistemas de gestão académica possuem uma arquitetura baseada em serviços Web suportada pelos protocolos SOAP e REST, tal vem viabilizar a comunicação e a troca de informação realizada entre o LIS e o SGA. Com vista a obter informação académica dos utilizadores (informação tal com o nome, o curso, as unidades curriculares, a escola e o departamento a que pertencem, entre outros) necessária para a geração de licenças, a comunicação entre estes componentes irá basear-se num desses protocolos sobre um canal seguro de comunicação (por exemplo, SSL). Assim, com os serviços web implementados, o pedido do utilizador para emissão de licença irá fazer com que o SGA envie um ficheiro XML contendo os dados académicos referentes a quem os solicitou para o LIS, que assim, os irá interpretar dando então seguimento ao procedimento de geração da licença de utilização.

Havendo diferença nos métodos de autenticação dos utilizadores entre a plataforma que dá suporte ao SGA e o ARMS torna-se necessário garantir a sua harmonização. A implementação de serviços de autenticação de *Single Sign On* podem contribuir para tal. A sincronia entre os dois sistemas será garantida através de sincronização regular de equivalência entre os utilizadores autenticados nessas plataformas. A diferença na autenticação de utilizadores poderá assim ser ultrapassada pela extração do identificador único do utilizador das credenciais de autenticação do ARMS que terá uma equivalência com a identificação dos utilizadores no SGA.

5 Conclusão

A integração entre o modelo proposto de gestão de direitos, as especificações MPEG-21 e o OpenSDRM encontram-se alinhadas, permitindo realizar a sua adaptação ao contexto académico estabelecendo um ambiente seguro e de confiança entre as partes envolvidas na referente proteção de conteúdos e no respeito pelos direitos. O OpenSDRM, através da sua adaptabilidade, suportada por uma enorme diversidade de serviços disponibilizados pelos seus

componentes, torna possível a adição de novos serviços e incorporação de novos componentes. A implementação desta plataforma, ao basear-se em ferramentas de código aberto, interfaces e tecnologias seguindo normas abertas, compatibiliza-se com um leque bastante alargado de cenários de proteção e posterior utilização de conteúdos. Para o contexto académico em análise, a alteração mais significativa na sua estrutura prende-se com a interação com um servidor de validação, SGA, que permita ao OpenSDRM verificar da elegibilidade dos pedidos de emissão de licença pelo utilizador. A incorporação das especificações MPEG-21 arrasta consigo o desenvolvimento de novos módulos com funções específicas (empacotamento/extração, encriptação/ desencriptação), a serem inseridos no CPS, SL e Cliente DRM. O OpenSDRM, sendo suficientemente aberto para poder incorporar as especificações de normas, é assim capaz de fornecer as funcionalidades que proporcionam a proteção adequada de conteúdo ao mesmo tempo que suporta a sua transmissão e distribuição, assim como a preservação de direitos ao longo da linha sucessória no domínio académico. A nova estrutura, consequência destas adaptações, designar-se-á por ARMS (Academic Rights Management System).

Parte III

Transmissão de conteúdos e direitos no OpenSDRM adaptado

Capítulo 7

Proteção do conteúdo recorrendo à norma MPEG-21

Resumo

Ao longo deste capítulo é analisada a transmissão e mobilidade dos objetos digitais, quer do conteúdo quer da licença, assim como das respetivas estruturas capazes de viabilizarem o seu transporte. É ainda analisado o enquadramento da estrutura de conteúdos e licenças com algumas partes da norma ISO/IEC 21000 (MPEG-21:VTS, 2004) (conhecida por MPEG-21), com vista a perceber o seu modo de funcionamento no respeitante à transferência de direitos entre os intervenientes que tomam parte na transação num sistema DRM. Dá-se um especial enfâse na análise dos métodos de proteção de conteúdos e transmissão de direitos proporcionados por esta norma, analisando-se, no final, o seu alinhamento com o modelo anteriormente proposto. Este capítulo apresenta como contributo a definição de uma estrutura genérica de conteúdos e licenças baseada na norma MPEG-21 que permite o seu transporte entre os intervenientes num sistema DRM adaptado ao contexto académico: o ARMS. São aqui analisados alguns casos de utilização envolvendo este sistema, nomeadamente o descarregamento e superdistribução de conteúdos.

1 Introdução

É prática comum no meio académico os utilizadores descarregarem conteúdos livres a partir da *Web* para mais tarde os utilizarem (Banzato, 2012), sendo estes em larga percentagem conteúdos textuais (ficheiros em formato Word, PDF, entre outros) (Bates et al., 2007; Banzato, 2012). Por isso, iremos dar especial ênfase aos sistemas DRM orientados para um cenário de descarregamento de ficheiros, visto serem estes os mais usados no meio académico no processo de partilha de conteúdos.

Os sistemas de DRM, ao permitirem que a informação protegida possa ser transmitida sobre canais inseguros e armazenada em dispositivos com armazenamento inseguro, sem comprometer a integridade e confidencialidade da informação, estão a dar uma resposta ao problema da transmissão de forma controlada (Safavi-Naini & Sheppard., 2010). Sucintamente,

do ponto de vista de proteção de direitos, o problema da partilha de conteúdos, não só no contexto académico, pode ser descrito em dois patamares distintos face ao contexto em que se insere. Por um lado, ao nível da eficácia da proteção do conteúdo, e por outro lado, nos mecanismos que permitem a distribuição e posterior partilha do conteúdo e direitos associados (Michiels et.al., 2005). Para que possa ter sucesso, o sistema deve ter em conta a interação entre estes patamares de modo a aumentar a conveniência dos utilizadores. Assim, não só se devem identificar as tecnologias de proteção, mas também as tecnologias e mecanismos apropriados que suportam a transmissão de conteúdos e respetivas licenças que são inerentes ao ciclo de vida do conteúdo. O conteúdo é normalmente protegido usando técnicas criptográficas, e através de uma licença o detentor de direitos especifica quais os direitos que os utilizadores possuem sobre esse conteúdo. A licença existe, normalmente, separada do conteúdo protegido e é concebida de acordo com uma linguagem de expressão de direitos (REL), sendo que o conjunto de direitos aí expresso é definido de acordo com um dicionário de dados de direitos (*Rights Data Dictionary* - RDD). A cada um desses direitos corresponde uma ação, sendo a sua execução verificada pela aplicação que interpreta o conteúdo (aplicação de *reprodução*). Somente esta aplicação é capaz de lidar com a proteção do conteúdo ao aplicar a ação em causa sobre esse conteúdo, devendo por isso ser um componente de confiança resistente a alterações. Contudo, quer o conteúdo quer a licença, ao serem transmitidos entre os participantes do sistema DRM, e independentemente da tecnologia e dos mecanismos de proteção aplicados, devem assegurar a mobilidade e garantir que a proteção aplicada é persistente ao longo do ciclo de vida do conteúdo (Safavi-Naini & Sheppard., 2010; Lee, Park & Kim, 2010).

O conteúdo transacionado entre as entidades de sistemas DRM, normalmente não é interoperável entre diferentes plataformas de DRM (Safavi-Naini & Sheppard., 2010). A definição de uma entidade única (por exemplo um ficheiro) que encapsule o conteúdo conjuntamente com informação relacionada necessária para a sua utilização iria facilitar a transfêrencia e reutilização de recursos de aprendizagem promovendo o desenvolvimento de procedimentos e formatos de empacotamento (Anido-Rifón, et al., 2014). Atualmente nos vários sistemas de DRM não há um único formato de conteúdo cuja preferência seja indiscutível. Várias técnicas para representar objetos digitais têm aparecido nos últimos tempos, sendo de especial interesse técnicas de representação de bens digitais como documentos XML, (Bekaert, Hochstenbach & Van de Sompel, 2003). Exemplos disso são as especificações *Metadata Encoding and Transmission Standard* (METS, 2014) e IMS *Content Packaging Specification* (IMS, 2009), as quais, conjuntamente com a proliferação de tecnologias como o

RDF (RDF, 2014) (Rodríguez, Gallego & Delgado, 2007c) e Dublin Core (DCMI, 2013a), têm contribuído para um cada vez maior interesse da comunidade científica em usar *objetos digitais complexos.* Um objeto complexo pode agregar dados, metadados e por vezes serviços numa entidade digital única (Nelson & Sompel, 2006) e pode ser visto como um artefacto que se pode decompor em conteúdos, metadados, relações com outros objetos e comportamento. Por exemplo, um objeto digital complexo pode agregar um ficheiro, os seus metadados, a sua proveniência e direitos associados, ligações a serviços de identificação e proteção e qual o comportamento perante uma determinada situação.

A norma MPEG-21 direciona-se com vista a dar uma resposta nesta área através de múltiplas especificações (igualmente designadas por partes). Para tal, faz recurso a um tipo de dados organizados em ficheiros XML que descreve a estrutura e relação entre os vários componentes agregados numa entidade com o nome de "Item Digital" (DI - *Digital Item*) (MPEG-21:DID, 2005). Este DI é essencialmente um contentor virtual de conteúdos e metadados (Burnett, Davis & Drury, 2005). A descrição dos elementos constituintes é realizada através de uma linguagem específica nesta norma, a *Digital Item Declaration Language* (DIDL), que permite descrever, através de um método normalizado, objetos de dados complexos (Bekaert, De Kooning & Van de Walle, 2005) como coleções com múltiplos componentes de conteúdos.

Ao definir um modelo baseado em XML para expressar a estrutura de objetos complexos e descrever os seus componentes (conteúdos e/ou descrições), o MPEG-21 permite que esses componentes não tenham um formato específico de codificação e também que as descrições não sigam obrigatoriamente um modelo de metadados estabelecido (Bekaert, De Kooning & Van de Walle, 2006). Existe assim uma grande liberdade de incluir no DI qualquer tipo de componente, e qualquer tipo de componente incluído é descrito no documento XML através da linguagem baseada no DIDL (Shao B., et. al., 2008). Deste modo, o DIDL e o W3C XML *Schema* em que se baseia fornecem uma flexibilidade e extensibilidade bastante alargadas no que se refere à representação de objetos digitais complexos (Bekaert et al., 2005), como aqueles que normalmente encontramos no meio académico (relatórios, livros, artigos científicos, vídeos de aulas, apresentações, entre outros), que podem combinar diferentes tipos de conteúdos.

2 Representação de objetos digitais usando o MPEG-21

Como foi referido anteriormente (Capítulo 4), o DRM no contexto académico deve considerar o suporte a dois tipos de conteúdos: o conteúdo protegido e o conteúdo desprotegido ou livre. O termo livre não significa que não existam direitos sobre esse conteúdo, simplesmente o seu

detentor prescindiu de os exercer. O cenário de utilização de um conteúdo livre poderá envolver a utilização de licenças, mas aqui o seu significado será meramente informativo, descrevendo ao utilizador os termos e condições de utilização, não havendo porém, qualquer garantia de que este irá respeitar essas condições. Neste cenário não se faz uso de medidas tecnológicas de proteção para garantir que a aplicação de direitos sobre conteúdo é respeitada, podendo dizer-se, por isso, que está desprotegido ou livre. Face a esta situação, pode-se considerar que a mobilidade do conteúdo protegido ou livre entre entidades DRM pode ser efetuada de duas formas: em conjunto com a licença ou em separado (Rodríguez, Gallego & Delgado, 2007c).

Se a licença existir em separado do conteúdo desprotegido, o utilizador poderá ter de contactar adicionalmente um servidor de licenças para obter uma licença para saber quais os termos de utilização. A sua consciência ética de respeito pelos direitos de PI será o único garante de que os direitos expressos na licença serão respeitados, não havendo nada que o obrigue a utilizar a licença e a respeitar as condições nela expressas (Etinger et al., 2009). Por outro lado, se a licença ficar empacotada em conjunto com o conteúdo desprotegido, então o utilizador receberá informação sobre os termos e condições sem ter que estabelecer ligações adicionais ao servidor de licenças para obter uma licença. Apesar de ser a solução com menor complexidade na distribuição de conteúdo desprotegido, nada impede o utilizador de desrespeitar os termos e condições expressos na licença exceto a sua consciência ética de respeito pelos direitos de PI. Em caso de infração, qualquer disputa será regulada pela lei vigente (Hietanen & DeRosnay, 2006).

Independentemente de o conteúdo ser protegido ou não, o requisito mais importante a observar por qualquer regime de PI reside numa efetiva comunicação ao recetor de conteúdo de que um conjunto de direitos foi reservado (Guibault & Angelopoulos, 2011). A comunicação desses direitos pode assentar em mecanismos tecnológicos. Estes mecanismos podem evoluir de passivos para ativos, dependendo a evolução da aplicação de medidas tecnológicas de proteção que asseguram a aplicação de direitos sobre os conteúdos (Kwok & Chi., 2006). De qualquer das formas, será sempre de considerar no ciclo de vida do conteúdo a intervenção dos participantes e componentes nucleares de um sistema DRM. A preparação e empacotamento do conteúdo, protegido ou não, e da respetiva licença, é um aspeto crucial, pois condiciona a sua forma de transmissão (Bekaert et al., 2005).

Para facilitar a mobilidade quer do conteúdo (protegido ou não) quer da licença entre os vários componentes de um sistema de gestão de conteúdos e direitos associados estes podem ser embebidos num ficheiro facilmente transportável entre as partes integrantes do sistema. Uma

das formas consiste em recorrer a ficheiros do tipo XML de modo a inserir não só o conteúdo como a informação relacionada e direitos associados, embebendo-os na sua estrutura. O MPEG-21, e o conceito que conceptualiza relativo aos DIs, faz recurso a este tipo de ficheiros sendo por isso um forte candidato para a proposta apresentada.

2.1 Empacotamento de conteúdos e de licenças

A base de suporte de qualquer estrutura de conteúdo nos sistemas DRM baseados na norma MPEG-21 é o típico objeto digital (Bekaert, et al., 2003; Kahn & Wilensky, 1995) (que pode conter texto, imagem, som, metadados, entre outros) encapsulado num pacote de dados usando o formato XML. Esta estrutura pode conter múltiplos objetos, que podem ficar embebidos num contentor/pacote DRM com uma estrutura definida, servindo o empacotamento do conteúdo para descrever as agregações do mesmo. Segundo as especificações da norma MPEG-21, cada recurso pode ser representado e inserido num DI (Burnett et al., 2005; Bekaert et al., 2005). Além disso, é possível alocar metadados a cada recurso e especificar o método da proteção de direitos de forma individualizada, o que facilita a partilha e o armazenamento de conteúdos em sistemas de gestão de conteúdos que possam oferecer suporte a esta norma (Bekaert et al., 2005).

A aplicação desta norma, nos dois possíveis cenários de distribuição de conteúdos no contexto educativo (conteúdo desprotegido/livre e conteúdo protegido), torna possível identificar várias combinações entre conteúdos, licenças e chaves de encriptação do conteúdo.

2.1.1 Conteúdo desprotegido

Nesta situação, cada licença pode ser vista como uma declaração, informando o consumidor acerca das permissões de utilização do conteúdo. Não sendo só do interesse do consumidor aceder a esta informação, mas também do detentor, é essencial declarar explicitamente a licença usada. O detentor pode definir a sua licença com condições individualizadas ou escolhendo uma licença genérica predefinida como, por exemplo, no caso da iniciativa *Creative Commons*. Assim, tudo vai depender da forma como se define a licença no DI e o modo como o consumidor acede à mesma. As possíveis combinações entre conteúdo desprotegido e licença agregadas num DI podem ser, resumidamente, visualizadas na Tabela 9.

DI = Item Digital L = Licença C = Conteúdo

Conteúdo desprotegido			
	Cenário	Combinação C + L	Nº DIs
1	Conteúdo desprotegido empacotado num DI e a Licença noutro DI.	DI [(C)]+ DI [(L)]	2
2	Conteúdo desprotegido agregado com a licença no mesmo DI.	DI [(C + L)]	1

Tabela 9 – Combinações de conteúdo desprotegido e licenças

Analisando a Tabela 9 para o conteúdo desprotegido, verifica-se que o segundo cenário é aquele que envolve um menor número de DIs, sendo, por isso, aquele que oferece uma menor complexidade na gestão de conteúdos e licenças, pois não obriga a uma procura constante da licença no sistema DRM, sempre que se queira utilizar o mesmo conteúdo. Podendo o DI com o conteúdo desprotegido ser enviado em conjunto com a licença, o utilizador não necessita de contactar o servidor de licenças para adquirir a licença, e pode então limitar-se à utilização do conteúdo (inclusive em modo *offline*) respeitando os termos e condições estipulados na licença empacotada no DI. Caso pretenda obter novos direitos, terá de obter o objeto contendo o mesmo conteúdo e uma nova licença, o que pode causar um maior volume de dados a ser transmitido.

Num cenário de distribuição de conteúdo desprotegido, existem três formas de efetuar a declaração de direitos numa licença:

- Através da inserção de texto – neste caso, o texto do licenciamento é incluído como metadados, em que o mesmo texto expressa os termos e condições da concessão devendo ser usado pelo consumidor para saber quais as permissões/restrições e condições. A sua leitura e a interpretação das permissões/restrições pode ser bastante subjetiva;
- Através da indicação de um *Uniform Resource Identifier* (URI) – neste caso, é inserido a um URI contendo um identificador global único que declara a licença e a versão da licença utilizada. Por exemplo, um URI deste tipo pode ser "http://creativecommons.org/licenses/by/3.0/", que é o identificador de uma das licenças definidas pela iniciativa *Creative Commons*;
- Através da indicação de uma página *Web* - o identificador é em simultâneo o URL de uma página *Web* onde o consumidor pode encontrar informação adicional acerca da licença e suas propriedades, assistindo-o na interpretação desta.

Independentemente da forma como a licença é declarada, torna-se necessária a identificação do conteúdo de uma forma única, de modo a que futuramente o mesmo possa ser reconhecido. O MPEG-21 *Digital Item Identification* (DII) (MPEG-21:DII, 2005) permite especificar os métodos de identificação de DI, esquemas descritivos e o relacionamento com outros DIs ou esquemas de identificação. Os identificadores especificados são independentes do tipo de conteúdo e baseiam-se num URI que permite a identificação de recursos abstratos ou físicos. Além disso, pode-se adicionar informação secundária, de modo a que o autor possa ser declarado e assim atribuir a autoria da obra. A atribuição faz com que seja possível associar o conteúdo ao autor, que, por sua vez, ao quer estar visível, declara esta associação ao consumidor ao mesmo tempo que é identificado para poder ser contatado.

Esta informação, ao ser apresentada ao consumidor, pode incluir dados adicionais tais como a hora da criação, o título do conteúdo, uma descrição, entre outros. A iniciativa Dublin Core (DCMI) vem dar um valioso contributo, pois, através de especificação (DCMI, 2013a), permite efetuar a declaração de direitos de uma forma normalizada integrando-se com o MPEG-21. Contudo, há ainda a considerar possíveis variantes na estrutura do documento DID de acordo com a representação do conteúdo, já que a especificação permite definir a representação de um recurso de duas formas: "*by-value"*, em que a representação é incluída como conteúdo do elemento recurso ou "*by-ref"*, na qual a representação é referenciada por uma URI que é o valor do elemento recurso e que normalmente aponta a um ficheiro num servidor (Bekaert et al., 2006).

Um documento do tipo DID com conteúdo desprotegido e onde alguns metadados estão inseridos, pode ser representado através dos elementos definidos na norma MPEG-21 (MPEG-21:DID, 2005). Pode-se assim esquematizar a estrutura de um objeto correspondente ao documento DID que incorpora o conteúdo desprotegido e metadados relacionados, de acordo com a Figura 47.

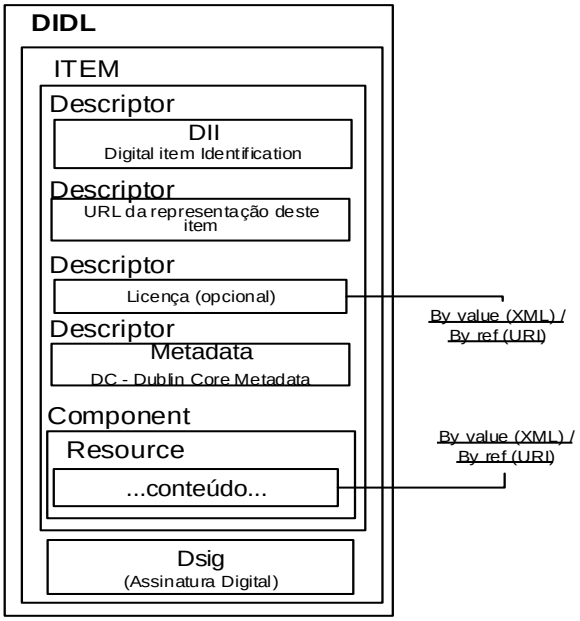


Figura 47 – Estrutura MPEG-21 DID para um conteúdo desprotegido

No exemplo abaixo listado (Figura 48) um primeiro elemento "*Declaration"* permite declarar os direitos sobre os conteúdos contidos no documento DID de uma forma textual. Um primeiro "*Descriptor/Statement"* fornece o *Digital Object Identifier* (DOI) do DI usando o elemento de identificação do DII XML namespace (Bekaert et al., 2006). Um segundo "*Descriptor/Statement"* fornece informação secundária sobre o ID expresso no formato Dublin Core. O conteúdo é fornecido pelo elemento "*resource"* por referência "*By-Ref*" através da inclusão da referência à sua localização. Este conteúdo também é fornecido e incorporado no documento *"By-Value*", sendo codificado em Base64 (Josefsson, 2006). Para comprovar a autenticidade do próprio conteúdo, podem ser embebidas assinaturas W3C XML (MPEG-21:IPMP, 2006) no documento DID, assim como o elemento *Signature* do W3C *Signature XML Namespace* pode ser fornecido como filho do elemento DIDLInfo para comprovar a autenticidade do próprio documento DID (Bekaert et al., 2006).

O suporte fornecido a assinaturas digitais e a sua integração no documento DID para o DI em causa e a todo o ficheiro vem assegurar a integridade e autenticidade que são requisitos prévios que o detentor de direitos pretende ver satisfeitos (Gadd et. al., 2003b). A implementação das assinaturas digitais vai depender da infraestrutura de chave pública (PKI) e certificados digitais implementados no sistema DRM. Contudo, a norma MPEG-21, ao permitir a integração de assinaturas digitais de acordo com o padrão XML *Signature Syntax and Processing* (XMLDSig; Solo, Reagle & Eastlake, 2008) num formato XML, assegura o suporte adequado à autenticidade e integridade do documento DID.

```
<?xml version="1.0" encoding="UTF-8"?>
<didl:DIDL DIDLDocumentId="info:obj/i/00002cb8-c477-11d8-a819-b1db893d21e6"
      xmlns:didl="urn:mpeg:mpeg21:2002:02-DIDL-NS">
      <didl:DIDLInfo>
        <dsig:Signature
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">...</dsig:Signature>
      </didl:DIDLInfo>
      <didl:Declarations>
       <didl:Descriptor id="copyright">
           <didl:Statement mimeType="text/plain">
              Copyright J.Marques. All rights reserved - unprotected Content DIDL.
           </didl:Statement>
        </didl:Descriptor>
        </didl:Declarations>
      <didl:Item id="uuid-00004342-c477-11d8-a819-b1db893d21e6">
          <didl:Descriptor>
             <didl:Statement mimeType="text/xml; charset=UTF-8">
                    <dii:Identifier xmlns:dii="urn:mpeg:mpeg21:2002:01-DII-NS">
              info:doi/11.4015/didlexa11-arms</dii:Identifier>
             </didl:Statement>
          </didl:Descriptor>
          <didl:Descriptor>
             <didl:Statement mimeType="text/xml; charset=UTF-8">
             <oai_dc:dc xmlns:oai_dc="http://www.openarchives.org/OAI/2.0/oai_dc/"
              xmlns:dc="http://purl.org/dc/elements/1.1/"
              xmlns:dcterms="http://purl.org/dc/terms/">
              <dc:title>exemplo DID – digital item </dc:title>
              <dc:creator>J.Marques</dc:creator>
              <dc:created>2014-10-15T18:01:19Z</dc:created>
              <dc:rights> Copyright 2014 by @J.Marques</dc:rights>
              </oai_dc:dc>
             </didl:Statement>
           </didl:Descriptor>
          <didl:Component id="uuid-0000a01c-d579-21d8-a819-a1234b1234c1">
       <didl:DIDLInfo>
             <dsig:Signature
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">...</dsig:Signature>
```

```
        </didl:DIDLInfo>
      <didl:Resource mimeType="application/pdf"
ref="http://openSDRM.pt/tech/pdf/didl_test.pdf"/>
      <didl:Resource mimeType="application/pdf" encoding="base64">
        KMJFweeDDSSJVBERi0xLjMKJeLjz9MNCjEgMCBvYmoKPDwgCi9TdWJq    ...
         </didl:Resource>
         </didl:Component>
    </didl:Item>
</didl:DIDL>
```

Figura 48 - Exemplo MPEG-21 DIDL para um conteúdo desprotegido

A incorporação de metadados não encriptados no objeto permite apresentar ao utilizador informação sobre o conteúdo e respetivo modo de licenciamento sem que este necessite de ferramentas adicionais. Assim, com o recurso à norma MPEG-21, o conteúdo desprotegido pode ser transmitido para terceiros num formato universalmente reconhecido e utilizando tecnologias padrão, não se tornando necessárias alterações no sistema nem no método de transmissão.

2.1.2 Conteúdo protegido

Ao longo desta tese iremos focar-nos na proteção do conteúdo e da chave de proteção desse conteúdo. A proteção dos metadados e direitos expressos será assegurada ao nível da sua integridade através da assinatura digital quando inseridos no DI, permanecendo aí desencriptados. O que se pretende é atingir um nível de proteção suficiente para a preservação do direito de atribuição e da integridade do conteúdo, que são os típicos do contexto académico a serem preservados. Contudo, nada impede que níveis de proteção mais elevados possam ser atingidos.

2.1.2.1 MPEG-21 e a gestão de direitos

Para proteger o conteúdo, qualquer sistema de DRM necessita de fazer uso de mecanismos que assegurem a sua proteção. A tecnologia normalmente usada por estes mecanismos pode ser diferenciada em três áreas: encriptação, assinaturas e autenticação. O seu principal objetivo passa por assegurar a autenticidade, a integridade, e a confidencialidade do conteúdo protegido com vista a garantir o controlo sobre o seu uso. Para que se possa utilizar conteúdos protegidos, o utilizador terá de possuir a respetiva licença que contém a chave que encripta o conteúdo e que lhe permite aceder e usá-lo de acordo com os termos especificados na licença.

A estrutura da licença aqui proposta é composta por elementos que se podem incorporar em quatro categorias: "identificação", "recurso", "proteção" e "termos". A primeira, designada de "identificação", permite identificar as entidades abrangidas pela licença (o licenciador e o licenciado). A segunda categoria, o "recurso", permite identificar o conteúdo a ser protegido. A categoria "proteção" contém os elementos relacionados com a proteção do "recurso" e envolve questões criptográficas e a garantia de autenticidade e integridade da licença. Finalmente, a categoria "termos" permite especificar os direitos descritos na concessão pelo licenciador ao licenciado, ou seja, as permissões e condições de utilização dos conteúdos. Para isso, faz-se recurso a uma linguagem de expressão de direitos que torna possível acionar os atos expressos nessa linguagem.

A organização destes elementos numa licença com estrutura básica pode ser efetuada de acordo com a norma MPEG-21 REL (ISO/IEC 21000-5), que os organiza num ficheiro XML de acordo com a recomendação do W3C e que consiste em uma ou mais concessões (*Grant*) e um emissor (*Issuer*). Basicamente a concessão consta de um "*Principal*", a quem foram atribuídos direitos (*Rights*) pelo emissor (*Issuer*) para poder atuar sobre um determinado conteúdo (*resource*), respeitando certas condições (*Conditions*) (Figura 49).

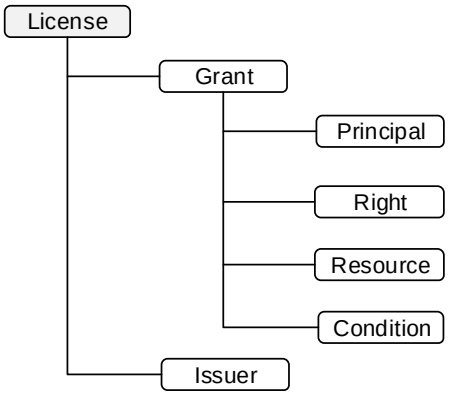


Figura 49 - Estrutura básica da licença MPEG-21

O direito de realizar certas ações sobre o conteúdo é definido de acordo com um vocabulário apropriado descrito através de um dicionário de termos específico MPEG-21 RDD (MPEG-21:RDD, 2006) (como, por exemplo, "*execute", "play", "print"*, entre outros) definido na norma através de uma coleção de três *schemas* XML ("*core","standard extension" e "multimédia extension"*) (Sheppard, 2007). Na Tabela 10 é possível ver a relação entre o "*prefix"* e o "*namespace"*.

Part	Namespace prefix	Namespace
Core	r	urn:mpeg:mpeg21:2003:01-REL-R-NS
Standard	sx	urn:mpeg:mpeg21:2003:01-REL-SX-NS
Multimedia	mx	urn:mpeg:mpeg21:2003:01-REL-MX-NS

Tabela 10 - MPEG-21 *schemas* – *prefix* e *namespace*

Na nossa proposta, ao separar o conteúdo da licença no processo de transmissão, e por questões de simplicidade, é possível distinguir dois tipos de representações de DIs manifestados através de MPEG-21 DIDL: o objeto digital correspondente ao documento DID que representa o conteúdo digital (DID_C), designado por "objeto conteúdo", e o objeto digital correspondente ao documento DID que representa a licença (DID_L), designado por "objeto de direitos". A estrutura básica do documento DID que representa o conteúdo, DID_C, é bastante parecida com a estrutura anteriormente mencionada para um DI, que representa conteúdo desprotegido. A grande diferença reside na possibilidade de associar aos componentes protegidos de um DI uma ferramenta de proteção (*IPMP tool - Intellectual Property Management and Protection*) que implementa um método de proteção específico sobre um recurso (Rodríguez, Gallego & Delgado, 2007c; Sheppard, 2007). A norma MPEG-21 permite que estas ferramentas de proteção possam ser implementadas através da especificação MPEG-21 IPMP (ISO/IEC 21000-4) (MPEG-21:IPMP, 2006), definindo um mecanismo simples de embutir a informação de proteção num documento DID. Contudo, não especifica quaisquer algoritmos criptográficos, infraestrutura de chave pública e certificados, dispositivos e outros componentes de proteção (Sheppard, 2007). O MPEG-21, ao não definir um sistema de DRM, tal como o faz para os variados elementos constituintes dos documentos DID, assume que as funcionalidades de proteção podem ser fornecidas por entidades externas através de ferramentas específicas, e não estão restringidas por nenhuma em particular (Sheppard, et. al., 2006a). A norma MPEG-21 IPMP define a informação relativa à proteção do DI. De uma forma genérica, a norma MPEG-21 IPMP permite a noção de ferramenta podendo indicar o fornecedor de um ou mais serviços de proteção. Ao permitir a declaração da ferramenta IPMP e a sua descrição (o tipo de algoritmo e sua localização) podemos estabelecer a proteção do conteúdo, ou até mesmo a proteção de todo o DI, integrando a ferramenta na estrutura do documento DID. Dizemos assim que o recurso passa a ser governado quando fica protegido por uma (ou mais) ferramenta IPMP (Sheppard, 2007). Cada recurso governado é associado a um identificador e a um descritor que o associa à licença e descreve a(s) ferramenta(s) IPMP requeridas(s) para aceder a esse recurso.

Ao não definir um método específico de como o recurso pode ser protegido, a norma MPEG-21 IPMP permite que não só sejam suportados vários regimes de DRM por vários vendedores, como também a renovação de mecanismos de segurança sempre que estes ficam comprometidos. Isto acaba por ser uma mais-valia, pois não obriga a norma a ficar dependente de um só tipo específico de proteção. Ao fornecer suporte a mecanismos de proteção, como a assinatura digital capaz de garantir a autenticidade e integridade do conteúdo e o suporte aos mecanismos criptográficos capazes de garantir a confidencialidade do conteúdo, o MPEG-21 consegue, assim, satisfazer as necessidades de proteção de conteúdo quando este é partilhado e transmitido de forma segura sob o formato XML. A sua implementação fica assim dependente do desenvolvimento da solução global de DRM que terá de ser integrada com esta norma.

Além do conteúdo protegido, a respetiva chave de proteção deve ser transmitida ao recetor de forma confidencial. Essa confidencialidade é assegurada pela encriptação da chave de proteção do conteúdo com a chave pública do utilizador registado no sistema DRM. Esta cifra encriptada é integrada nos metadados referentes à licença e empacotada num ficheiro XML em conformidade com as especificações MPEG-21, não podendo influenciar a posterior transmissão deste ficheiro. Para que a integridade de conteúdos, chaves e licenças fique assegurada é ainda incorporada a assinatura digital do documento DID e/ou de cada DI, permitindo assim verificar a autoria, assim como provar que o documento não foi adulterado. O documento DID acaba por ser o veículo de transporte dos recursos, chaves e metadados associados. Podemos visualizar de forma esquemática na Figura 50 a estrutura do documento que representa a licença $DID_{L,}$ em conformidade com a especificação REL incorporando alguns dos elementos XML comuns e com assinatura referente a um DI.

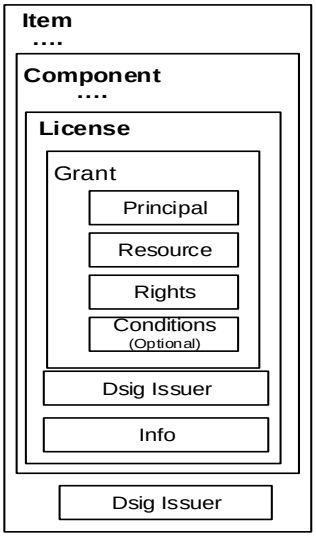


Figura 50 – Estrutura básica de um documento DID contendo a licença

Em (Rodríguez, Gallego & Delgado, 2007c) são apresentados vários métodos de proteção de conteúdo e gestão de chaves baseados em MPEG-21. Vários casos de utilização são aí identificados (*download*, *streaming*, superdistribuição, domínios), assim como vários exemplos. É aí considerada a distribuição mais comum no meio académico – o descarregamento de conteúdo – sendo de referir que a chave que encripta o conteúdo está embebida na licença ficando empacotada num documento DID. Por sua vez, o conteúdo protegido fica embebido separadamente num outro documento DID. Assim, temos um alinhamento perfeito entre a proposta de modelo (onde há a separação do conteúdo dos direitos associados) e o suporte disponibilizado pela norma MPEG-21 IPMP através dos mecanismos de proteção. Estes mecanismos são aqui considerados tendo em vista a futura integração com o sistema ARMS, assim como com os mecanismos de distribuição de licença por delegação suportados pela norma MPEG-21.

2.1.2.2 Conteúdos seguros e transmissão

Para um conteúdo protegido com DRM, quer o ficheiro correspondente ao DID_C quer o correspondente ao DID_L contêm os recursos mais importantes a serem protegidos. O DID_C incorpora o conteúdo encriptado e o DID_L incorpora a chave de proteção do conteúdo encriptado. Assim, convém protegê-los de acordo com o nível adequado ao cenário de utilização. No contexto académico, tal como vimos anteriormente, a proteção a considerar deverá ter em conta a preservação da integridade do conteúdo e o respeito pelos direitos de atribuição. Para assegurar a autenticidade, integridade e confidencialidade do conteúdo e da informação relacionada, temos de assegurar uma proteção conveniente pelo sistema DRM. A assinatura digital e a encriptação são aqui usadas com esse fim, quer para a representação do ID sob a forma de conteúdo DID_C, quer para a representação sob a forma de licença DID_L. Ao aplicar as assinaturas sobre os DID, ou partes deste, estas devem permanecer intactas durante o período em que o conteúdo é armazenado e distribuído, de modo a ser possível atribuir o recurso ao criador. O método de representação de uma assinatura utilizado é o XMLDSig (Barttel, Boyer, Fox, LaMacchia, & Simon 2002; Schreiner, 2011).

Para evitar que quando um recurso é modificado por terceiros essa modificação seja atribuída ao criador desse recurso, este assina-o. A assinatura digital é assim utilizada para verificar a autenticidade e a integridade do recurso disponibilizado evitando o não repúdio por quem a assinou. Num documento típico MPEG-21 DID vários DIs podem ser definidos numa estrutura padrão podendo aplicar-se uma assinatura digital a cada DI ou ao ficheiro no seu todo, ficando

aí encapsulada. A assinatura pode proteger um ficheiro DI completo ou partes do mesmo (Bekaert et al., 2005). A proteção do ficheiro no seu todo é realizada com outra assinatura que precisa de ser embebida num nível superior aos itens, ou seja, logo abaixo do elemento DID ficando todos os itens assinados e também os seus metadados (Schreiner, 2011). A confidencialidade do conteúdo é conseguida com o recurso à especificação MPEG-21 IPMP, a qual permite um método de embeber informação relativa à proteção dentro do MPEG-21 DID (Sheppard, 2007).

A especificação MPEG-21 permite a proteção do conteúdo através da definição de estruturas versáteis onde não só se define a licença que governa o conteúdo, mas também a forma de proteção desse mesmo conteúdo. Ao permitir declarar uma ferramenta IPMP e qual a sua localização, a qual representa um algoritmo criptográfico que fornece um ou mais serviços de proteção, a norma MPEG-21 IPMP permite integrar estas ferramentas na estrutura de uma DID para assegurar a proteção do conteúdo (Sheppard, 2007). Estando o conteúdo protegido, a encriptação dos metadados embebidos no DI é facultativa podendo assim o utilizador final aceder diretamente a estes dados descritivos, de modo a saber mais pormenores sobre o conteúdo que pretende aceder. Neste trabalho, este é o método escolhido na encriptação do conteúdo, isto é, somente o conteúdo é encriptado, permitindo que terceiros acedam aos metadados contidos no DID_C para que possam identificar e categorizar o conteúdo. Assim, o utilizador, tendo obtido o conteúdo diretamente do sistema DRM ou a partir de outros utilizadores, poderá aceder à informação sobre o conteúdo sem ser necessário desencriptar os restantes dados, podendo até saber imediatamente onde pode obter a licença que lhe irá permitir utilizar o conteúdo.

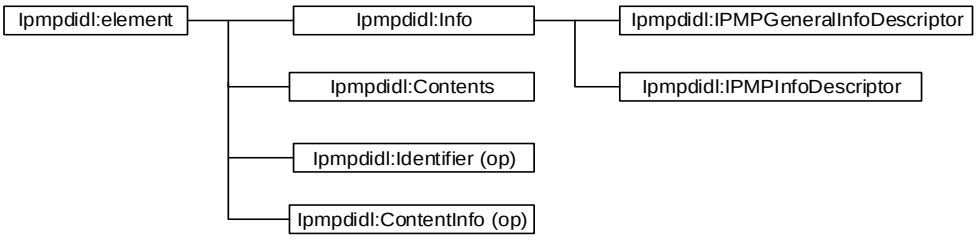


Figura 51 – Estrutura básica dos elementos IPMP

Usando os subelementos IPMP DIDL básicos, "*Identifier"*, "*Info*" e "*Contents"* de cada um dos elementos IPMP de topo ("*ipmpdidl:container","* ipmpdidl:item", *"ipmpdidl:descriptor", "ipmpdidl:resource"*, entre outros) na conceção do ficheiro XML representativo do DID e utilizando os mecanismos do MPEG-21, podemos assim estruturar o documento referente ao conteúdo DID_C. Usando dois sub-elementos de topo do IPMP schema referentes ao elemento

"*info*: o *IPMPGeneralInfoDescriptor"* e o "*IPMPInfoDescriptor",* podemos indicar a governação e proteção do DI (no seu todo ou suas partes constituintes) (Figura 51). Estes elementos e seus sub-elementos (Figura 52 e Figura 53) vão permitir criar um documento DID onde se pode indicar o servidor que disponibiliza o serviço de licenças para o conteúdo em causa, mas também as ferramentas e métodos de proteção.

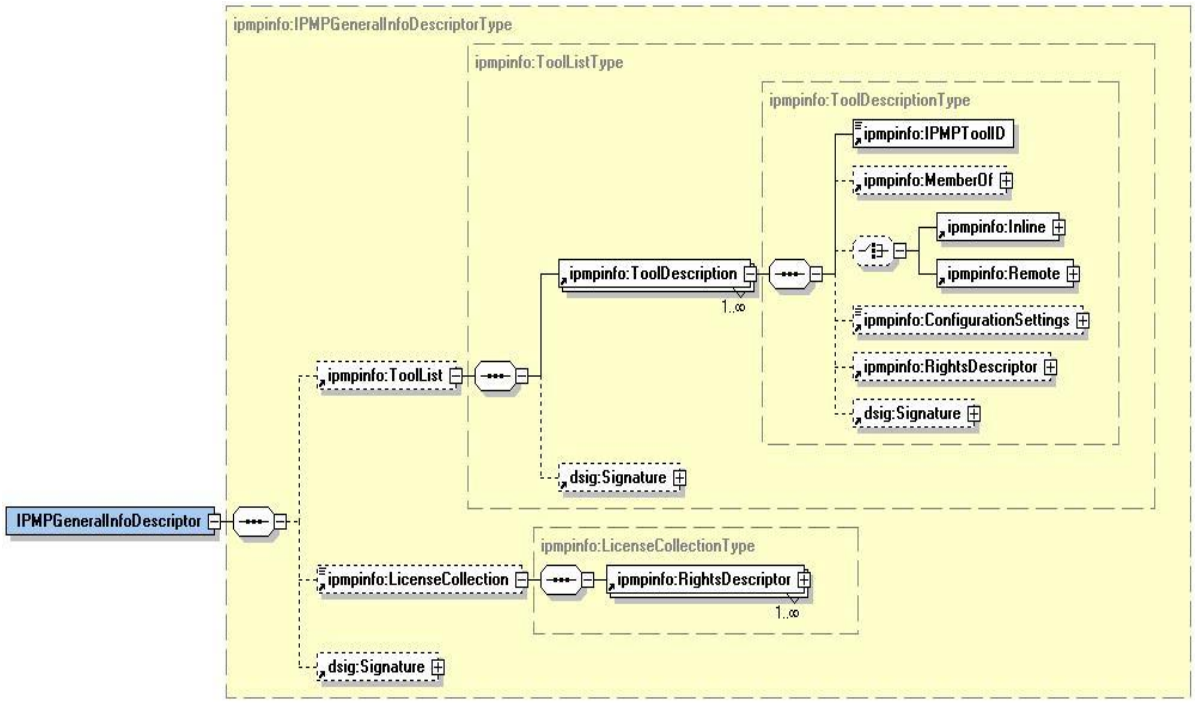


Figura 52 - Estrutura do subelemento IPMPGeneralInfoDescriptor

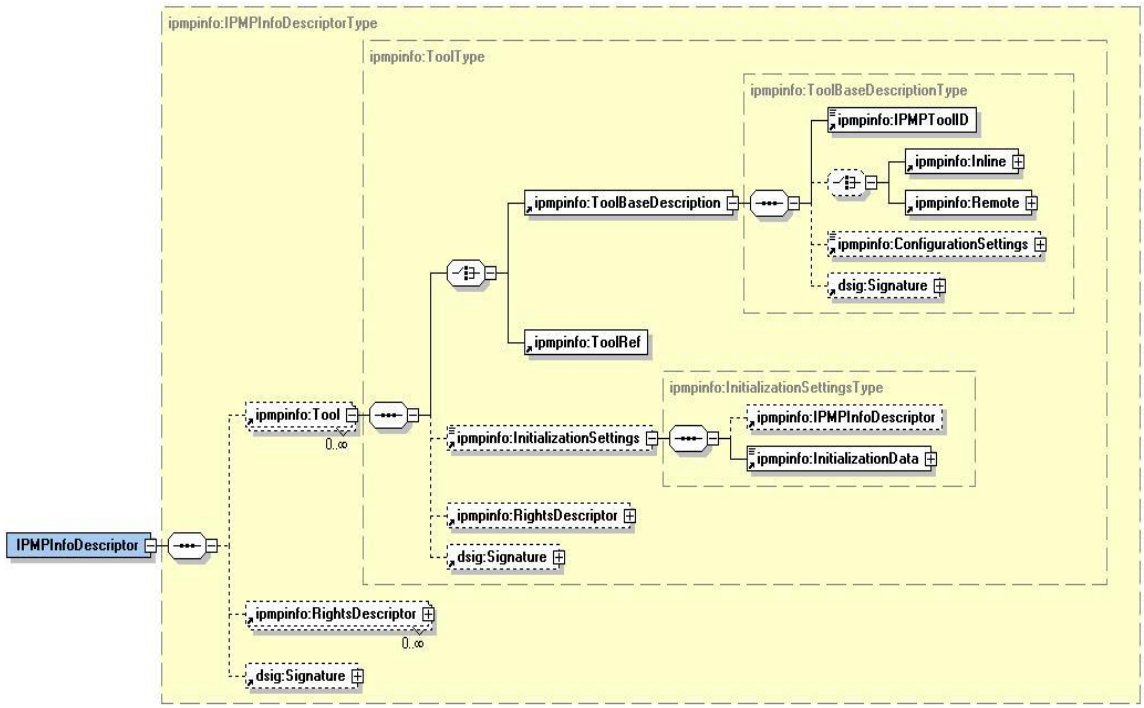


Figura 53 - Estrutura do subelemento IPMPInfoDescriptor

O exemplo que se apresenta a seguir na Figura 54 refere-se a um documento DID contendo um conteúdo no formato PDF, protegido, com indicação da localização do servidor de licenças e da ferramenta de proteção de conteúdo utilizado, recorrendo a elementos IPMP.

```
<DIDL xmlns="urn:mpeg:mpeg21:2002:02-DIDL-NS"
xmlns:dii="urn:mpeg:mpeg21:2002:01-DII-NS"
xmlns:ipmpdidl="urn:mpeg:mpeg21:2004:01-IPMPDIDL-NS"
xmlns:ipmpinfo="urn:mpeg:mpeg21:2004:01-IPMPINFO-NS"
xmlns:r="urn:mpeg:mpeg21:2003:01-REL-R-NS"
xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<DIDL DIDLDocumentId="info:obj/i/00002cb8-c477-11d8-a819-b1db893d21e6"
      xmlns:didl="urn:mpeg:mpeg21:2002:02-DIDL-NS"
      <DIDLInfo>
      <dsig:Signature
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">...</dsig:Signature>
      </DIDLfo>
<Declarations>
  <Descriptor>
    <Statement mimeType="text/xml; charset=UTF-8">
      <ipmpinfo:IPMPGeneralInfoDescriptor>
        <ipmpinfo:ToolList>
           <ipmpinfo:ToolDescription localID="AESEncrypt">
<ipmpinfo:IPMPToolID>urn:mpegRA:mpeg21:IPMP:tool:id:0001</ipmpinfo:IPMPToolID>
              <ipmpinfo:Remote ref="urn:IPMPToolsServer:ToolEnc005-3485"/>
           </ipmpinfo:ToolDescription>
         </ipmpinfo:ToolList>
         <ipmpinfo:LicenseCollection>
          <ipmpinfo:RightsDescriptor>
            <ipmpinfo:LicenseService>
             <r:serviceReference>
                 <sx:uddi>
                  <sx:serviceKey>
                        <sx:uuid>aa1198c0-8abe-11d7-a735-b8a03c50a334</sx:uuid>
                  </sx:serviceKey>
                 </sx:uddi>
                 <r:serviceParameters>
                  <r:datum> ... </r:datum>
                   </r:serviceParameters>
```

```
                </r:serviceReference>
                </ipmpinfo:LicenseService>
              </ipmpinfo:RightsDescriptor>
            </ipmpinfo:LicenseCollection>
          </ipmpinfo:IPMPGeneralInfoDescriptor>
        </Statement>
      </Descriptor>
</Declarations>
<Item id="uuid-00004342-c477-11d8-a819-b1db893d21e6">
              <Descriptor id = "item_1">
                    <Statement mimeType="text/plain">PDF_xyz encriptado</Statement>
              </Descriptor>
              <Descriptor>
                    <Statement mimeType="text/xml; charset=UTF-8">
                    <dii:Identifier xmlns:dii="urn:mpeg:mpeg21:2002:01-DII-NS">
                          info:doi/9.1085/Mark_05</Identifier>
                   </Statement>
              </Descriptor>
              <Descriptor>
                    <Statement mimeType="text/xml; charset=UTF-8">
                          <oai_dc:dc
                    xmlns:oai_dc="http://www.openarchives.org/OAI/2.0/oai_dc/"
                          xmlns:dc="http://purl.org/dc/elements/1.1/"
                          xmlns:dcterms="http://purl.org/dc/terms/">
                          <dc:title>DIDL Concepts </dc:title>
                          <dc:creator>J.Marques</dc:creator>
                          </oai_dc:dc>
                    </Statement>
              </Descriptor>
        <Component id="uuid-00005e90-c687-11d8-a819-b1db893d21e6">
              <Descriptor>
                    <Statement mimeType="text/xml; charset=UTF-8">
                    <dc:format
              xmlns:dc="http://purl.org/dc/elements/1.1/">application/pdf</dc:forma
              t>
                    <dcterms:created     xmlns:dcterms="http://purl.org/dc/terms/">
              2013-10-29T18:07:18Z</dcterms:created>
                    <dc:creator
                    xmlns:dc="http://purl.org/dc/elements/1.1/">MARKKES</dc:creator
                    >
                    </Statement>
```

```
                <dc:rights> Copyright 2014 by @J.Marques</dc:rights>


            </Descriptor>
            <Descriptor>
                <Statement mimeType="text/xml; charset=UTF-8">
                <dsig:Signature
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">...</dsig:Signature>
                </Statement>
            <Descriptor>
            <ipmpdidl:Resource mimeType="application/pdf" >
                <ipmpdidl:Info>
                    <ipmpinfo:IPMPInfoDescriptor>
                            <ipmpinfo:Tool>
                                <ipmpinfo:ToolRef localidref="AESEncrypt"/>
                                <ipmpinfo:InitializationSettings>
                                    <ipmpinfo:InitializationData>
                                        <key_length>128</key_length>
                                        <operating_mode>PBE</operating_mode>
                                        <encrypt_format>Based64</encrypt_format>
                            <initialization_vector>Adrad%daf&fa;</initialization_vector>
                                        <padding_scheme>PCK#5</padding_scheme>
                                    </ipmpinfo:InitializationData>
                                </ipmpinfo:InitializationSettings>
                            <ipmpinfo:Tool>
                            <ipmpinfo:IPMPInfoDescriptor>
                </ipmpdidl:Info>
                    <ipmpdidl:Contents encoding=”base64”>
JVBERi0xLjMKJeLjz9MNCjEgMCBvYmoKPDwgCi9TdWJqZWN0ICgpCi9LZXl3JkcyAoKQovQ3JlYXRvciAo
WFBQKQovVGl0bGUgKCkKL1Byb2R1Y2VyICgpCi9Nb2REYXRlIChEOjIwMDQwNTE0MTIy...
                    </ipmpdidl:Contents>
                    <ipmpdidl:Identifier>
                    <dii:Identifier>urn:mpegRA:mpeg21:dii:IPMPDI0001:01</dii:Identi
                    fier>
                    </ipmpdidl:Identifier>
            </ipmpdidl:Resource>
        </Component>
</item>
</DIDL>
```

Figura 54 – Conteúdo PDF protegido e embebido num documento DID

A representação genérica da estrutura deste documento DID pode ser visualizada na Figura 55.

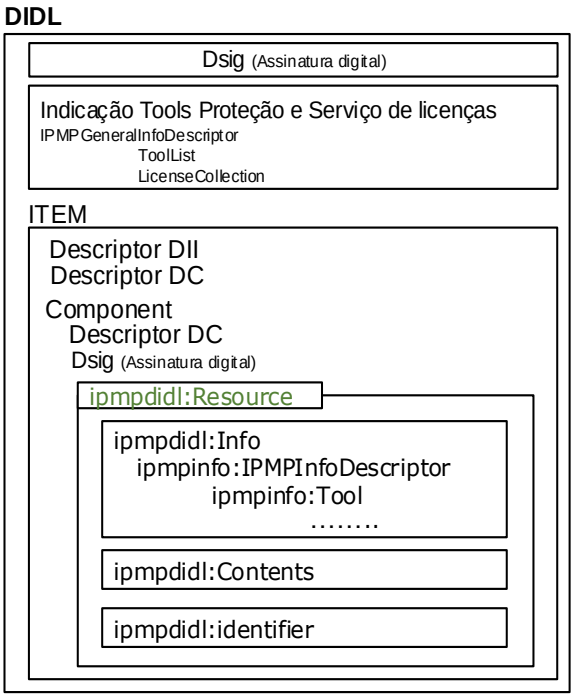


Figura 55 – Representação da estrutura de documento DID$_C$ contendo ficheiro protegido.

O recurso original encontra-se codificado em Base64 (Josefsson, 2006), e embebido no elemento "<ipmpdidl:Contents>". A referência ao método de proteção do recurso PDF é fornecida pelo elemento "ipmpdidl:resource" que incorpora os três elementos básicos "ipmp:Info", "ipmp:Identifier" e "ipmp:Contents" e respetivos sub-elementos. A ferramenta de proteção utilizada e a forma de obter a licença são indicadas como subelementos do elemento DIDL, logo no topo do documento DID. O elemento "<ipmpinfo:ToolRef>" contém o identificador da ferramenta de proteção correspondente ao algoritmo de encriptação utilizado, informando o recetor do método de encriptação na proteção do conteúdo. Por razões de eficiência é aqui utilizado um algoritmo de encriptação simétrica: o AES (AES, 2001).

Através da inclusão dos elementos de topo "<IPMPGeneralInfoDescriptor>" e "<IPMPInfoDescriptor>", que representam as duas categorias de governação e proteção MPEG-21 IPMP, temos assim a possibilidade de não só proteger o conteúdo, mas igualmente indicar a forma de governação e a(s) ferramenta(s) de proteção necessária(s). Uma das formas de exprimir os direitos associados pode ser através de elemento "IPMPGeneralInfoDescriptor". O sub-elemento "LicenseCollection" permite especificar através do elemento "RightsDescriptor" como obter direitos associados ao recurso através da referência a um servidor de licenças. Além disso, existe igualmente a possibilidade de inserir assinaturas digitais no documento e conteúdos, o que vem ao encontro de uma das necessidades básicas dos detentores do conteúdo - a preservação da integridade.

A possibilidade de inserir identificadores e metadados num documento DID torna-o extremamente versátil, pois consegue-se obter uma forma estruturada de representar o conteúdo, ao mesmo tempo que se define a sua proteção e indicação das regras da sua governação (Burnett et al., 2005). Podendo o elemento "*item*" conter atributos de outros *namespaces* XML (como por exemplo, *Dublin Core*) capazes de fornecer informação descritiva sobre esse DI, assim como informação de registo (como, por exemplo, o DOI), é possível identificar inequivocamente o recurso.

As chaves simétricas de encriptação do conteúdo (C_{EK}) podem ser geradas automaticamente a partir de um módulo específico de geração de chaves instalado no servidor de gestão de conteúdos do sistema DRM. A gestão destas chaves pode ser feita de forma dinâmica através de um algoritmo de cálculo de resumo criptográfico, $Hash_{SHA1}$, baseado no conteúdo e na identificação do utilizador, de modo a gerar uma chave forte (por exemplo: $C_{EK} = Hash_{SHA1}\left(Hash_{SHA1}(C) + Hash_{SHA1}(Author_{ID})\right)$. Após a encriptação, a chave é armazenada no servidor de gestão de conteúdos. Quando o utilizador efetua um pedido de licença para um determinado conteúdo, esta chave é encriptada com a chave pública do utilizador para depois ser incorporada no objeto licença. Esta licença irá dar origem a um objeto DID_L ficando aí embebida. Tal como na proteção do conteúdo, podemos aqui proteger esta chave recorrendo à mesma técnica. Usando o elemento IPMP para a proteger com chave assimétrica utilizando o algoritmo RSA, e inserindo-a no elemento *"resource"* do objeto DID_L, conjuntamente com a respetiva licença de utilização (Figura 56).

```
<?xml version="1.0" encoding="UTF-8"?>
<DIDL xmlns="urn:mpeg:mpeg21:2002:02-DIDL-NS"
xmlns:dii="urn:mpeg:mpeg21:2002:01-DII-NS"
xmlns:ipmpdidl="urn:mpeg:mpeg21:2004:01-IPMPDIDL-NS"
xmlns:ipmpinfo="urn:mpeg:mpeg21:2004:01-IPMPINFO-NS"
xmlns:r="urn:mpeg:mpeg21:2003:01-REL-R-NS"
xmlns:mx=" urn:mpeg:mpeg21:2003:01-REL-MX-NS"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<DIDL DIDLDocumentId="info:obj/i/00002cb8-c477-11d8-a819-b1db893d21e6-0001"
      xmlns:didl="urn:mpeg:mpeg21:2002:02-DIDL-NS"
      <DIDLInfo>
            <dsig:Signature
      xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">...</dsig:Signature>
      </DIDLInfo>
```

```
<Declarations>
  <Descriptor>
    <Statement mimeType="text/xml"; charset=UTF-8>
      <ipmpinfo:IPMPGeneralInfoDescriptor>
        <ipmpinfo:ToolList>
             <ipmpinfo:ToolDescription localID="RSA128_Encrypt">
<ipmpinfo:IPMPToolID>urn:mpegRA:mpeg21:IPMP:tool:id:00002</ipmpinfo:IPMPToolID>
                  <ipmpinfo:Remote ref="urn:IPMPToolsServer:ToolEnc001-3000"/>
             </ipmpinfo:ToolDescription>
        </ipmpinfo:ToolList>
      </ipmpinfo:IPMPGeneralInfoDescriptor>
    </Statement>
  </Descriptor>
</Declarations>
<item>
….
   <Component>
        <ipmpdidl:resource mimeType="text/plain">
            <ipmpdidl:Info>
                 <ipmpinfo:IPMPInfoDescriptor>
                <ipmpinfo:Tool>
                             <ipmpinfo:ToolRef localidref="RSA128_Encrypt"/>
                </ipmpinfo:Tool>
                <ipmpinfo:RightsDescriptor>
                    <ipmpinfo:License>
                       <r:license...>
                           <r:grant>
                              <r:keyHolder>
                                  <r:info>
                                   <dsig:KeyValue>
                                      <dsig:RSAKeyValue>
                                         <dsig:Modulus>Cat7QzxAprs=</dsig:Modulus>
                                         <dsig:Exponent>AQABAA==</dsig:Exponent>
                                       </dsig:RSAKeyValue>
                                   </dsig:KeyValue>
                                  </r:info>
                              </r:keyHolder>
                              <mx:play/>
                              <mx:diReference>
```

```
                                    <mx:identifier>urn:mpegRA:mpeg21:dii:IPMPDI0001
                                    :01</mx:identifier>
                                </mx:diReference>
                                <r:validityInterval>
                                    <r:notBefore>2013-01-01T00:00:00</r:notBefore>
                                    <r:notAfter>2014-01-01T00:00:00</r:notAfter>
                                </r:validityInterval>
                            </r:grant>
                            <r:issuer>
                                <dsig:Signature> … </dsig:Signature>
                            </r:issuer>
                        </r:license>
                    </ipmpinfo:License>
                </ipmpinfo:RightsDescriptor>
                </ipmpinfo:IPMPInfoDescriptor>
            </ipmpdidl:Info>
            <ipmpdidl:Contents encoding=”base64”>Ksfgd24kkjasJH0ICdfsdfsdffgp….
            </ipmpdidl:Contents>
              <ipmpdidl:Identifier>

      <dii:Identifier>urn:mpegRA:mpeg21:dii:IPMPDI0001:01</dii:Identifier>
              </ipmpdidl:Identifier>
        </ipmpdidl:Resource>
   </Component>
</item>
</DIDL>
```

Figura 56 – Licença e chave protegida embebidas num documento DID

A representação da estrutura básica deste documento DID_L contendo a licença pode ser visualizada na Figura 57.

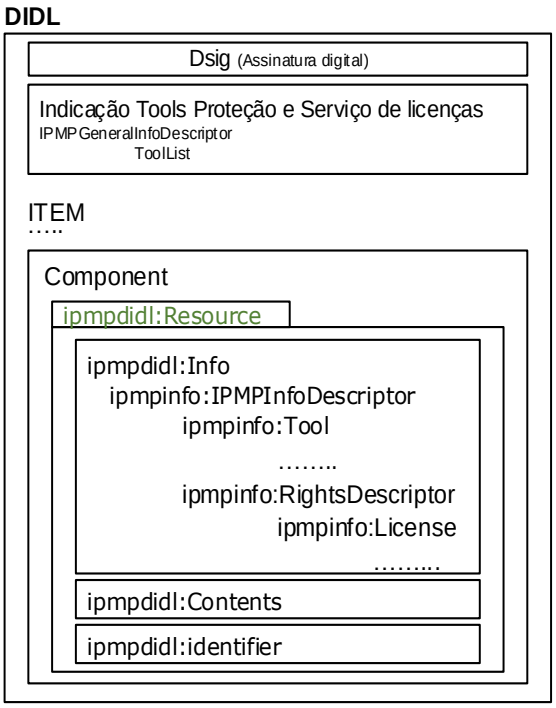


Figura 57 – Estrutura do documento DID_L contendo a chave e a licença

A estrutura dos objetos digitais aqui definidos envolve a encriptação do conteúdo C, embebendo-o no documento $DID_{C,}$ e da chave que protege o conteúdo (C_{EK}) embebendo-a no documento DID_L, permanecendo os metadados dos itens digitais desencriptados. Isto permite que terceiros possam aceder e identificar os metadados. A ferramenta IPMP de proteção refere-se somente ao recurso no documento DID, sendo assim conveniente inserir a sua declaração no elemento "*resource"*.

Fazendo recurso à norma MPEG-21, a estrutura dos documentos IPMP DID reflete os mecanismos pelos quais o conteúdo é encapsulado e governado. Torna-se assim possível expressar e associar informação apropriada de governo de conteúdos em documentos XML DID estruturalmente válidos e transacionáveis, que vão de encontro aos objetivos de controlo do detentor de direitos, capazes de preservar direitos e forma de governação. A proteção e empacotamento de conteúdos e metadados e a desproteção desse conteúdo para reprodução ou outros usos autorizados em concordância com os direitos expressos na licença são suportadas por esta norma através da indicação das ferramentas e mecanismos apropriados.

2.1.2.3 MPEG-21 e rastreio do licenciamento

Como foi anteriormente dito, a estrutura dos objetos digitais aqui definida envolve DIs MPEG-21. Num DI, quer o conteúdo quer a chave que o protege são encriptados e encapsulados num documento DID, podendo assim qualquer DI ser transferido usando qualquer protocolo para

um determinado recetor. Depois dessa transferência, o recetor extrai a chave encriptada no DI contido do documento DID e usa a sua chave privada armazenada na aplicação do dispositivo cliente para desencriptar a chave de proteção do conteúdo, aplicando-a na desencriptação do conteúdo, podendo então acedê-lo e usá-lo, de forma governada. Apesar de o recetor poder distribuir livremente o objeto digital que contém o conteúdo e o que contém a chave de proteção da licença, a distribuição deste último poderá não fazer qualquer sentido. Além da chave que protege o conteúdo ter que ser reencriptada com a chave assimétrica do novo recetor, teremos de garantir a validade das assinaturas digitais inseridas no novo objeto digital, caso contrário o documento DID deixa de observar os requisitos de integridade e autenticidade, o que pode impedir a aplicação no dispositivo cliente de avançar, inviabilizando a utilização do conteúdo. Já foi possível anteriormente verificar duas formas de proceder à reencriptação do conteúdo (Capítulo 5): através de reencriptação da chave de proteção pela aplicação cliente ou através de reencriptação dessa chave por um *proxy*. Contudo, com o MPEG-21 e a estrutura de objetos digitais que englobam assinaturas digitais, o problema coloca-se agora na redistribuição de direitos.

A redistribuição de direitos costuma fazer parte integral de qualquer sistema de gestão de conteúdos que tenha em consideração os direitos de PI. Contudo esta questão torna-se extremamente complexa quando estão envolvidas assinaturas digitais, pois, estando a licença personalizada, a sua redistribuição envolve uma nova personalização para o novo recetor. Em MPEG-21 um DI pode ser assinado para assegurar a integridade e autenticidade desse item. Esse DI pode conter a chave de proteção de conteúdo, estando assinado digitalmente de modo a preservar integridade. Ao transferir o objeto que contém essa chave de um utilizador final para outro, devemos reencriptá-la com a chave pública do recetor para quem pretendemos transferir o objeto e voltar a assinar o ID com a chave do utilizador que a emite. Ao fazê-lo estamos a perder o rasto dos vários emissores identificados pelas assinaturas digitais e com isso perdemos a linha sucessória dos direitos transmitidos. Torna-se, por isso, necessário encontrar um método que permita responder a este problema.

Se considerarmos que a assinatura digital representa metadados descritos dentro de um DI, poderemos incorporar a informação relativa à assinatura digital do utilizador emissor num elemento especial considerado na especificação MPEG-21: o elemento "*annotation*". Este elemento pode conter informação acerca de uma "*entidade identificada do modelo sem alteração ou adição a essa entidade"* (tradução de (MPEG-21:DID, 2005)). Esta informação pode tomar a forma de "*descriptors"*. Quando a assinatura digital de um DI precisa de ser

calculada, o elemento "*annotation"* e a informação nele contida é ignorada. Esta informação é adicional, não fazendo parte do conteúdo, ficando ao critério do cliente DRM mostrá-la ou processá-la. Este elemento pode assim ser utilizado para embeber a assinatura do progenitor num item sem modificar o recurso ou os metadados relacionados com esse mesmo recurso. Assim, o elemento "*annotation"* fica excluído da assinatura, preservando a validade. Isto permite inserir, modificar, ou remover os elementos "*annotation"* do DI ao mesmo tempo que as assinaturas provam a autenticidade e integridade do mesmo. A assinatura fica intacta quando o item é copiado para outro item ou agregado noutros itens. Tal permite facilitar o envio dos objetos DID_L entre utilizadores, pois o método de transmissão não afeta a distribuição do conteúdo. Torna-se assim possível a utilização do elemento "*annotation"* para inserir a identificação dos retransmissores de direitos, acrescentando-os ao elemento "*annotation"* sempre que um utilizador emissor transfere direitos, quer pelo método de reencriptação da licença no cliente DRM, quer através de reencriptação através de um *proxy*, conforme abordado anteriormente (Capítulo 5). Deste modo conseguimos identificar a cadeia sucessória de direitos, desde o progenitor até ao último utilizador a quem a licença foi transmitida, sendo assim possível efetuar o rastreio do licenciamento. O exemplo da Figura 58 ilustra esta situação identificando os intervenientes ao longo da cadeia sucessória.

```
<?xml version="1.0" encoding="UTF-8"?>
<DIDL xmlns="urn:mpeg:mpeg21:2002:02-DIDL-NS"
xmlns:dii="urn:mpeg:mpeg21:2002:01-DII-NS"
xmlns:ipmpdidl="urn:mpeg:mpeg21:2004:01-IPMPDIDL-NS"
xmlns:ipmpinfo="urn:mpeg:mpeg21:2004:01-IPMPINFO-NS"
xmlns:r="urn:mpeg:mpeg21:2003:01-REL-R-NS"
xmlns:mx=" urn:mpeg:mpeg21:2003:01-REL-MX-NS"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<DIDL DIDLDocumentId="info:obj/i/00002cb8-c477-11d8-a819-b1db893d21e6-0001"
       xmlns:didl="urn:mpeg:mpeg21:2002:02-DIDL-NS"
       <DIDLInfo>
             <dsig:Signature
       xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">...</dsig:Signature>
       </DIDLInfo>
<Declarations>
  <Descriptor>
    <Statement mimeType="text/xml"; charset=UTF-8>
      <ipmpinfo:IPMPGeneralInfoDescriptor>
        …..
```

```
      </ipmpinfo:IPMPGeneralInfoDescriptor>
    </Statement>
  </Descriptor>
</Declarations>
<item id=”encrypted_key”>
….
   <Component>
        <ipmpdidl:resource mimeType="text/plain">
            <ipmpdidl:Info>
                ….
            </ipmpdidl:Info>
            <ipmpdidl:Contents encoding=”base64”>
                ….
        </ipmpdidl:Contents>
        </ipmpdidl:Resource>
   </Component>
   <Annotation target="#encrypted_key">
    <Descriptor id=”DSigA”>
        <Statement mimeType="text/xml">
            <r:issuer>
              <dsig:Signature>
                <dsig:SignedInfo>
                  <dsig:CanonicalizationMethod
                  Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                  <dsig:SignatureMethod
                  Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                  <dsig:Reference>
                  <dsig:Transforms>
                  <dsig:Transform       Algorithm="urn:mpeg:mpeg21:2003:01-REL-R-
                   NS:licenseTransform"/>
                  <dsig:Transform Algorithm="urn:uddi-org:schemaCentricC14N:2002-
                   07-10"/>
                  </dsig:Transforms>
                  <dsig:DigestMethod
                   Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <dsig:DigestValue>L05dJk9QdTExKO4ltbj1/Q==</dsig:DigestValue>
                  </dsig:Reference>
                </dsig:SignedInfo>
                <dsig:SignatureValue>L05qOQhAprs=</dsig:SignatureValue>
                <dsig:KeyInfo>
```

```
                    <dsig:KeyValue>
                    <dsig:RSAKeyValue>
                    <dsig:Modulus>Bob7QzxAprs=</dsig:Modulus>
                    <dsig:Exponent>AQABAA==</dsig:Exponent>
                    </dsig:RSAKeyValue>
                    </dsig:KeyValue>
                </dsig:KeyInfo>
              </dsig:Signature>
            </r:issuer>
        </Statement>
    </Descriptor>
    <Descriptor id="DSigB">
        <Statement mimeType="text/xml">
            <r:issuer>
                <dsig:Signature>
                  <dsig:SignedInfo>...</dsig:SignedInfo>
                  <dsig:SignatureValue>L24sdfhAprs=</dsig:SignatureValue>
                  <dsig:KeyInfo>...B...</dsig:KeyInfo>
                 </dsig:Signature>
            </r:issuer>
        </Statement>
    </Descriptor>
    <Descriptor id="DSigC">
        <Statement mimeType="text/xml">
            <r:issuer>
                <dsig:Signature>
                  <dsig:SignedInfo>...</dsig:SignedInfo>
                  <dsig:SignatureValue>L77sdfhAprs=</dsig:SignatureValue>
                  <dsig:KeyInfo>...C...</dsig:KeyInfo>
                 </dsig:Signature>
            </r:issuer>
        </Statement>
    </Descriptor
        ...
   </Annotation>
</item>
</DIDL>
```

Figura 58 - O elemento *annotation* e a cadeia sucessória num documento DID

A estrutura do objeto digital correspondente à licença pode assim ser ilustrada da seguinte forma (Figura 59):

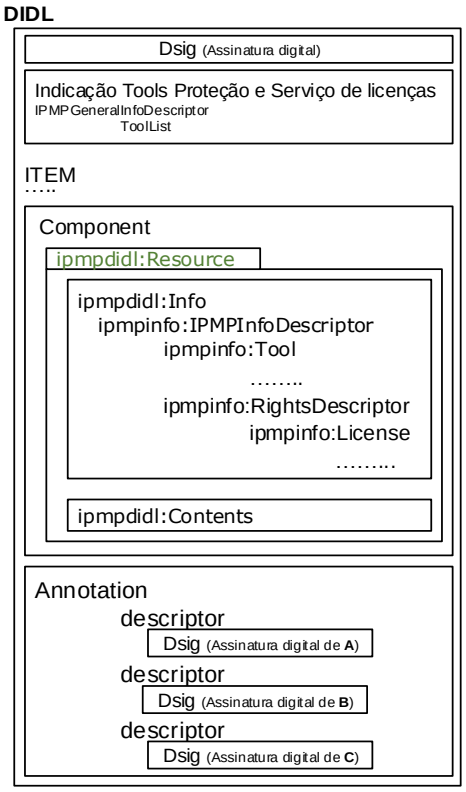


Figura 59 – Representação da estrutura do documento DID_L com o elemento *annotation.*

3 A norma MPEG-21 e o modelo proposto

A separação clara entre objetos conteúdos e objetos de direitos no modelo anteriormente proposto vem permitir que o conteúdo possa ser associado a termos e condições de utilização que podem variar consoante o tipo de utilização do mesmo. A norma MPEG-21, permitindo empacotar conteúdos e metadados em documentos DID com estruturas altamente flexíveis, viabiliza a definição de objetos de conteúdo e de direitos transacionáveis, como os documentos DID_C e DID_L, os quais se encontram perfeitamente alinhados com o modelo proposto. Ao viabilizar a sua definição em objetos separados, ao mesmo tempo que assegura a proteção permitindo uma transmissão segura para terceiros quer do conteúdo protegido quer da chave que encripta esse conteúdo, entra em concordância com o princípio básico do DRM enunciado no Capítulo 2. Ao aplicar o MPEG-21 IPMP na proteção do conteúdo, descrevendo e identificando as ferramentas de proteção, e assegurando ao mesmo tempo uma transmissão eficaz dos objetos digitais, torna-se possível realizar a partilha segura de conteúdos, assegurando a integridade e confidencialidade e garantindo a preservação e governo de direitos. O MPEG-21 IPMP, ao permitir a inserção de informação com a indicação de ferramentas

eficazes na proteção, possibilita o estabelecimento de níveis de segurança que vão ao encontro das principais necessidades e requisitos dos utilizadores no meio académico. A chave de encriptação do conteúdo é uma das peças fulcrais a proteger sendo necessária uma especial atenção ao processo de transferência do objeto digital onde está inserida: o objeto de direitos. De acordo com os requisitos anteriormente enunciados de transferência de licenças (ver Capítulo 4), é possível verificar que:

- A chave que encripta o conteúdo (C_{EK}) inserida no objeto de direitos enviados ao recetor está encriptada com a chave pública do recetor. Estando a C_{EK} personalizada para este recetor, somente este a poderá desencriptar. Mesmo que terceiros possuam o objeto de direitos com a licença emitida para um recetor específico e a C_{EK} protegida, somente este a poderá usar, pois é quem possui a correspondente chave privada que permite desencriptar a mesma. Ou seja, como a licença está personalizada, somente tem utilidade para o utilizador para quem foi emitida, o que permite assim satisfazer o primeiro requisito.
- O segundo requisito depende da interação entre o SL e o SGA no momento em que o SL, face a um pedido de emissão de licenças, solicita ao SGA dados para verificar a pertença do utilizador ao meio académico e se satisfaz as condições expressas na licença de distribuição. O modelo proposto ao assumir a incorporação do Sistema de Gestão Académica na arquitetura, permite ao servidor de licenças (SL) verificar a elegibilidade do pedido do cliente. Só depois de validar o pedido é procede à emissão da licença, satisfazendo assim este requisito.
- O terceiro requisito também é observado, pois assume-se aqui que o dispositivo é de confiança e que o mesmo é capaz de interpretar e manter protegidos objetos digitais que obedecem às regras de segurança estabelecidas e em conformidade com a proteção de conteúdos MPEG-21. Deste modo, assegura-se que não só a proteção do conteúdo é persistente, mas também que chave de proteção do conteúdo é mantida encriptada no dispositivo do utilizador.
- O quarto requisito é igualmente satisfeito, pois qualquer modificação não autorizada ou falsificação será detetada já que os mecanismos de verificação MPEG-21 permitem validar a integridade da licença e do objeto digital de acordo com a assinatura digital do emissor.

O MPEG-21, ao permitir incluir recursos e metadados num único objeto contendo informação sobre o conteúdo e a sua distribuição, permite assim que se possam garantir os dois níveis de

proteção identificados no modelo proposto e que visam garantir uma segurança desde o início até ao fim do ciclo de vida do conteúdo:

- proteção do objeto digital que contém a licença e a chave e do objeto conteúdo no fornecedor de conteúdos;
- proteção do objeto conteúdo no canal de comunicação;
- proteção do objeto que contém a licença no canal de comunicação;
- proteção do objeto conteúdo e do objeto que contém a licença no dispositivo cliente.

4 Modelo baseado na norma MPEG-21 e OpenSDRM adaptado ao contexto académico

Com o intuito de especificar uma solução generalista para a partilha de conteúdos e a gestão segura de licenças e chaves num sistema DRM, foram selecionados alguns dos cenários mais vulgares que as diferentes iniciativas costumam ter em consideração (Rodríguez, Gallego & Delgado, 2007c). Os cenários em causa envolvem casos de utilização e as suas possíveis combinações e cobrem as formas mais correntes de distribuição de conteúdo aos utilizadores finais tendo-se aqui por referência a existência de grupos de utilizadores do meio académico (por exemplo, professores, alunos, turmas, entre outros). Estes casos de utilização baseiam-se na utilização do ARMS tal como este foi descrito no capítulo anterior. Para cada um dos casos de utilização, é definido como o conteúdo é empacotado, protegido e governado, tendo em atenção a interação dos diferentes componentes do ARMS com o SGA. Essa abordagem parte do pressuposto de que o SGA disponibiliza uma interface baseada em serviços *Web* e de que o conteúdo e objetos licença são enviados em separado. Os componentes principais do ARMS envolvidos nos casos de utilização são o CPS, o COS, o LIS, Media Player/Wallet, ITS e o SGA com que o utilizador final interage direta ou indiretamente através de uma arquitetura baseada em serviços.

4.1 Proteção de conteúdo e empacotamento

Para que o conteúdo possa ser partilhado na ARMS, este deve ser preparado numa forma facilmente transmissível onde os direitos de PI possam ser expressos e facilmente acedíveis. A nossa abordagem recorre ao empacotamento de conteúdos, metadados e dos direitos associados sob uma forma facilmente transmissível recorrendo à norma MPEG-21 com vista a tornar exequível a gestão de direitos de PI sobre conteúdos. Para tal, foram considerados duas possíveis situações: o correspondente ao conteúdo protegido e o correspondente ao conteúdo desprotegido. Num caso, o detentor do conteúdo e/ou dos direitos pode ter interesse em proteger o mesmo. O ARMS dá a opção de o conteúdo poder ser, ou não ser, empacotado e protegido

em conformidade com a norma MPEG-21, embebendo conteúdos e informação relacionada num pacote XML que obedece às especificações IPMP DIDL, dando origem a um objeto digital com uma estrutura definida. Tal como vimos, esta estrutura é bastante semelhante entre ambos os tipos de objetos gerados. A principal diferença entre eles diz respeito a referências às ferramentas usadas na proteção do conteúdo e na referência à licença.

Para efetuar a gestão de conteúdos e direitos associados, o detentor deve em primeiro lugar inserir o conteúdo no ARMS interagindo com o CPS. Uma aplicação *Web*, o Ingestion Module (IM), disponibiliza uma interface ao detentor de conteúdo (Figura 60 e Figura 61) permitindo o registo, obtendo um identificador único para o conteúdo, assim como a associação de metadados e a especificação de direitos.

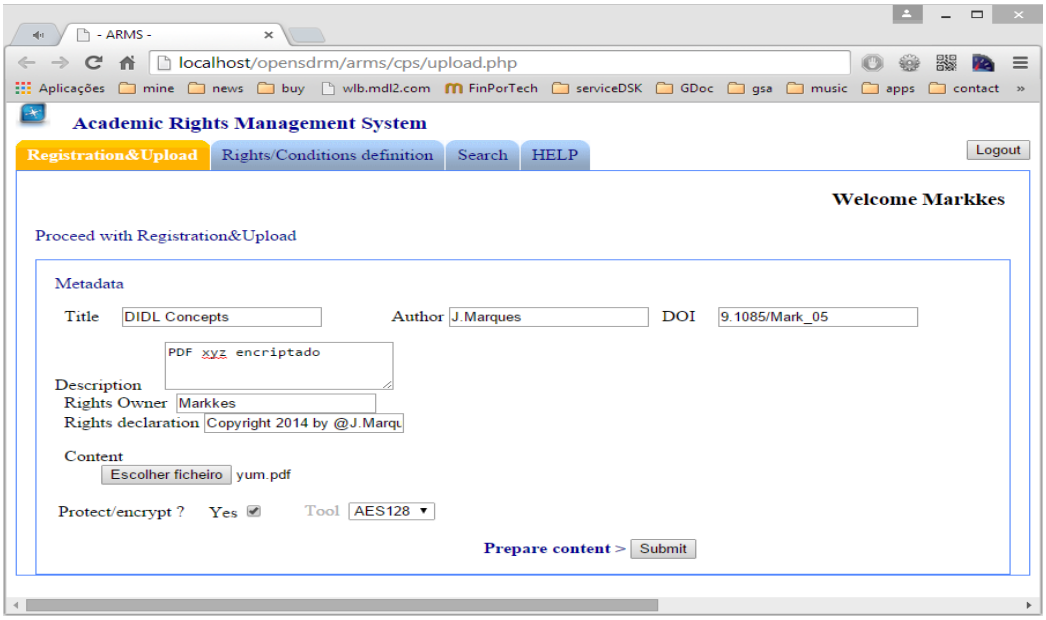


Figura 60 – Preparação de conteúdo

Sempre que necessário o IM aplica o processamento adequado como a codificação e formatação, podendo contactar outros componentes com vista a obter as ferramentas (criptográficas) necessárias para realizar a proteção do conteúdo. Nesta fase, o detentor do conteúdo interage através de um formulário disponibilizado pela aplicação de gestão de direitos do LIS e define os direitos de distribuição que pretende conceder quando o seu conteúdo for partilhado, ficando estes armazenados no LIS.

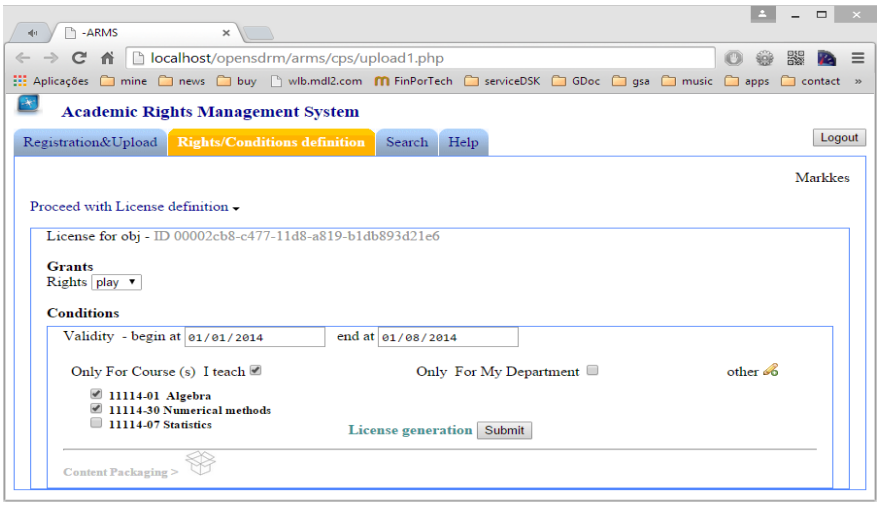


Figura 61 - Definição de direitos

Para verificar se o detentor de conteúdo pertence ao domínio académico, o CPS contacta o SGA a fim de obter a informação necessária. No final, o conteúdo é empacotado como um documento DID em conformidade com a norma MPEG-21 e armazenado no MDS da plataforma ARMS. Nesta altura o IM publica uma referência do novo conteúdo e envia-a para o COS, que a utiliza para criar um endereço (*link)* do pacote que contém o conteúdo para que este possa ser descarregado. O diagrama de sequência (Figura 62) descreve estas interações.

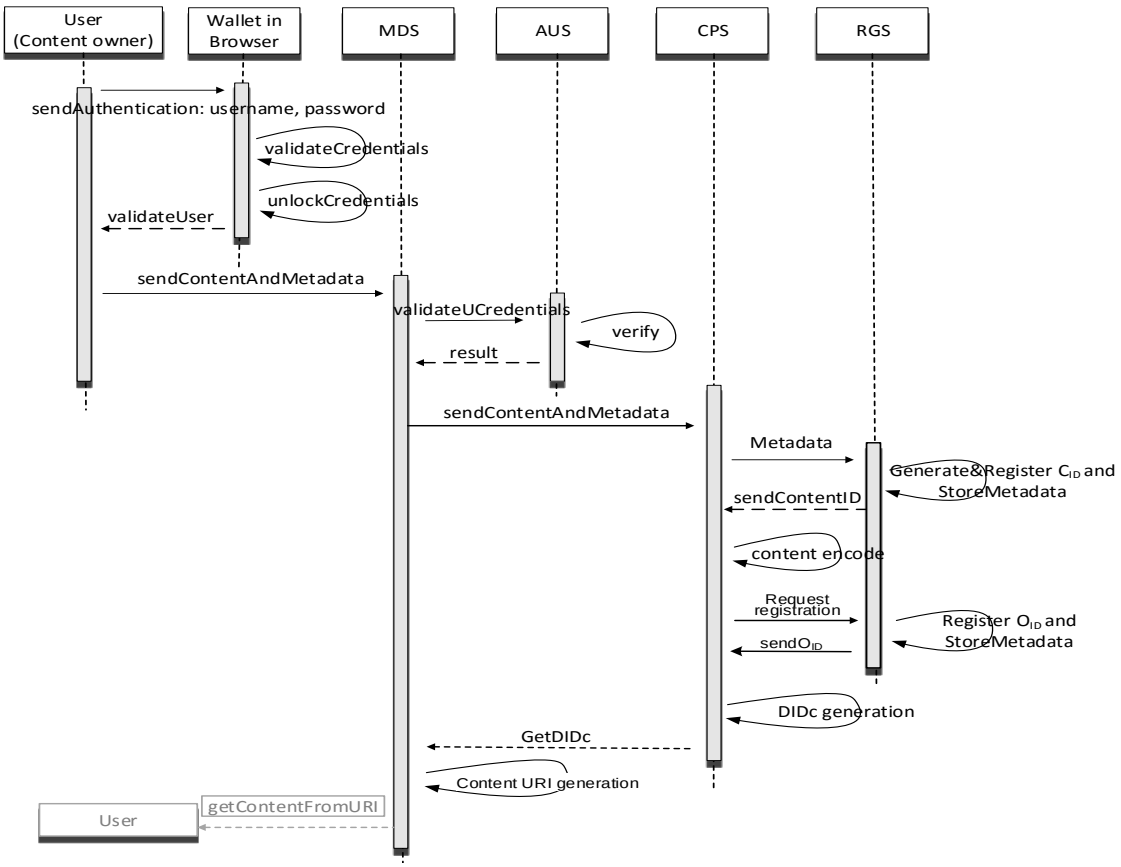


Figura 62 – ARMS: empacotamento e proteção do conteúdo

Caso o autor/detentor do conteúdo não necessite de proteger o conteúdo, a sequência de operações para criar o objeto conteúdo é muito mais simplificada pois só há necessidade de registar e embeber o conteúdo num documento DID. A estrutura do objeto DID_C é muito mais simples, pois deixa de fazer sentido fazer referência à licença e à sua localização, assim como a ferramentas de proteção IPMP. Quando este objeto ficar na posse do utilizador, a "Aplicação/Agente DRM" verifica a sua autenticidade e integridade através da validação da assinatura digital, procede à extração do conteúdo e, com este na sua posse, pode então executar várias ações. A Figura 63 ilustra a sequência de operações.

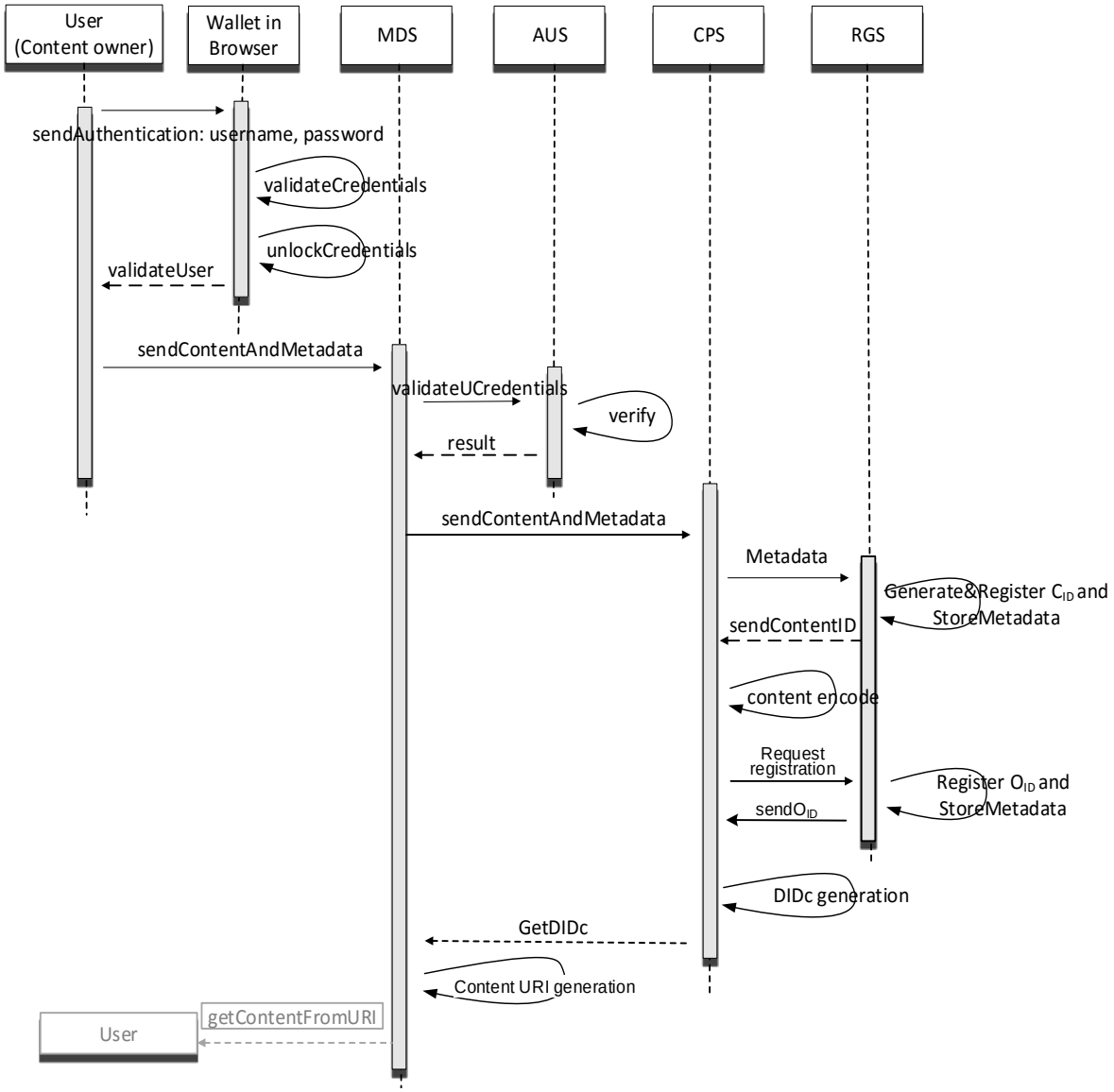


Figura 63 - Empacotamento de conteúdo não protegido no ARMS

A incorporação do conteúdo no objeto digital através das funcionalidades do ARMS assegura que o mesmo é genuíno. Contudo, não é possível garantir que todas as operações sobre esse mesmo conteúdo terão em conta o respeito dos direitos de PI, pois terão de se aplicar outros

mecanismos que garantam o respeito pela vigência de direitos no decorrer da utilização. Para que o conteúdo protegido embebido no documento DID_C possa ser partilhado, um conjunto bastante diversificado de mecanismos implementados no ARMS são ativados.

De um modo geral, estando o objeto conteúdo na posse do utilizador a sua utilização segue os seguintes passos:

- Quando o utilizador acede ao objeto através do cliente no dispositivo este apresenta-lhe informação sobre o conteúdo nomeadamente a sua identificação, autores, criação, entre outras. Além disso, apresenta-lhe também a(s) licença(s) previamente armazenadas no dispositivo correspondentes a esse conteúdo;
- Caso a(s) licença(s) não existam (ou o utilizador pretenda usufruir dos conteúdos noutros termos), então o utilizador, a partir de $DID_{C,}$ seleciona a localização de onde pode obter a licença (através do sub-elemento "*LicenseService*" inserido no elemento "*LicenseCollection*") e dá início ao processo negociação com o fornecedor de licenças para a sua obtenção.
- Caso o perfil do utilizador se enquadre dentro dos critérios de elegibilidade definidos (por exemplo pertencer ao domínio académico da instituição e estar dentro dos condições definidas pelo autor/detentor do conteúdo), então a respetiva licença poderá ser emitida.

Nos capítulos seguintes os mecanismos que permitem emissão da licença e a partilha de conteúdo e direitos associados serão apresentados mostrando todo o potencial que o ARMS disponibiliza. As secções seguintes descrevem alguns cenários correspondentes à partilha de conteúdo mais propriamente descarregamento e a sua redistribuição entre membros de um mesmo grupo.

4.1.1 Descarregamento de conteúdo e respetiva licença

Neste caso de utilização o utilizador interage com o COS para obter o conteúdo empacotado do MDS. Depois de selecionar o conteúdo que lhe interessa para o seu dispositivo o Wallet instalado no dispositivo extrai o URI do documento DIDc e fica a saber, além dos dados descritivos referentes ao conteúdo, como e onde pode obter a respetiva licença. Após selecioná-la o utilizador é redirecionado para o LIS onde poderá escolher as condições de utilização através de um formulário apresentado pelo LIS. Depois disso, pede a emissão da respetiva licença pelo LIS e um módulo especial (o *Issuer License Module* – ILM) que vai verificar se o pedido é válido, é então ativado. Isto é feito através da solicitação de dados ao SGA via serviços

Web, que envia os dados correspondentes ao perfil académico do utilizador. Com estes dados o ILM procede à validação do utilizador verificando se este pertence ao meio académico e verifica se as condições selecionadas pelo utilizador então em conformidade com as definidas na licença de distribuição inicialmente criada pelo detentor de direitos. Se o pedido for válido, este módulo dá início à geração de um objeto de direitos DID_L que identifica claramente o emissor, o dono da licença, o conteúdo a que se refere e as condições. A licença é então empacotada num documento DID_L com a chave de proteção do conteúdo encriptada com a chave pública do utilizador que pediu a licença e metadados, de acordo com a estrutura definida. Um *link* especial é então criado para que o utilizador possa descarregar o objeto para o seu dispositivo. A Figura 64 ilustra a sequência de operações no ARMS.

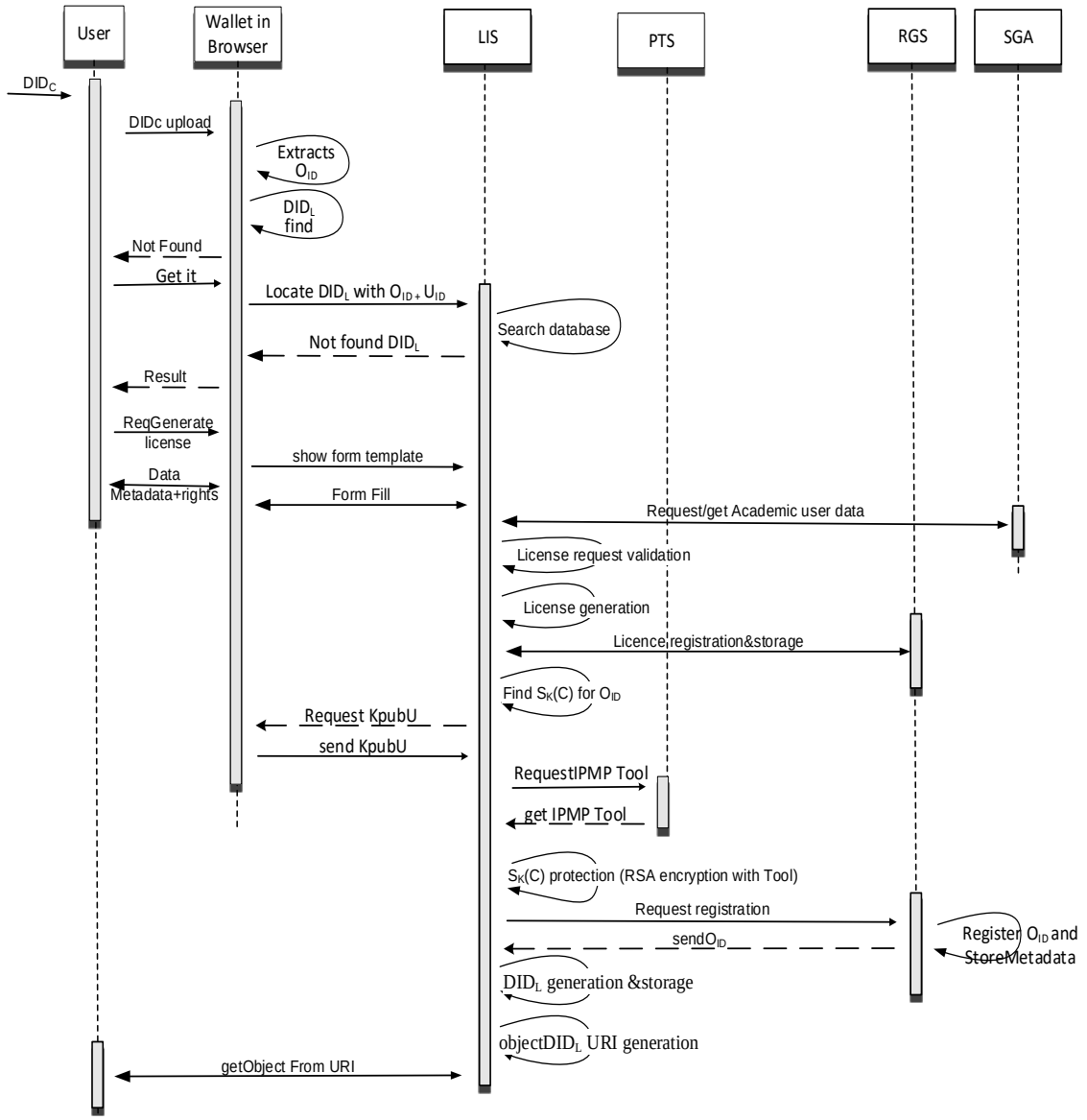


Figura 64 – ARMS e descarregamento de conteúdo e respetiva licença

4.1.2 Superdistribuição do conteúdo

Neste caso de utilização o utilizador que fez previamente o descarregamento do conteúdo protegido a partir do MDS pode distribuí-lo para outros utilizadores. Contudo, para o utilizador que o recebe poder aceder ao conteúdo e usá-lo, terá de adquirir uma licença válida. O procedimento não é diferente do anterior e a Figura 65 ilustra a sequência de passos.

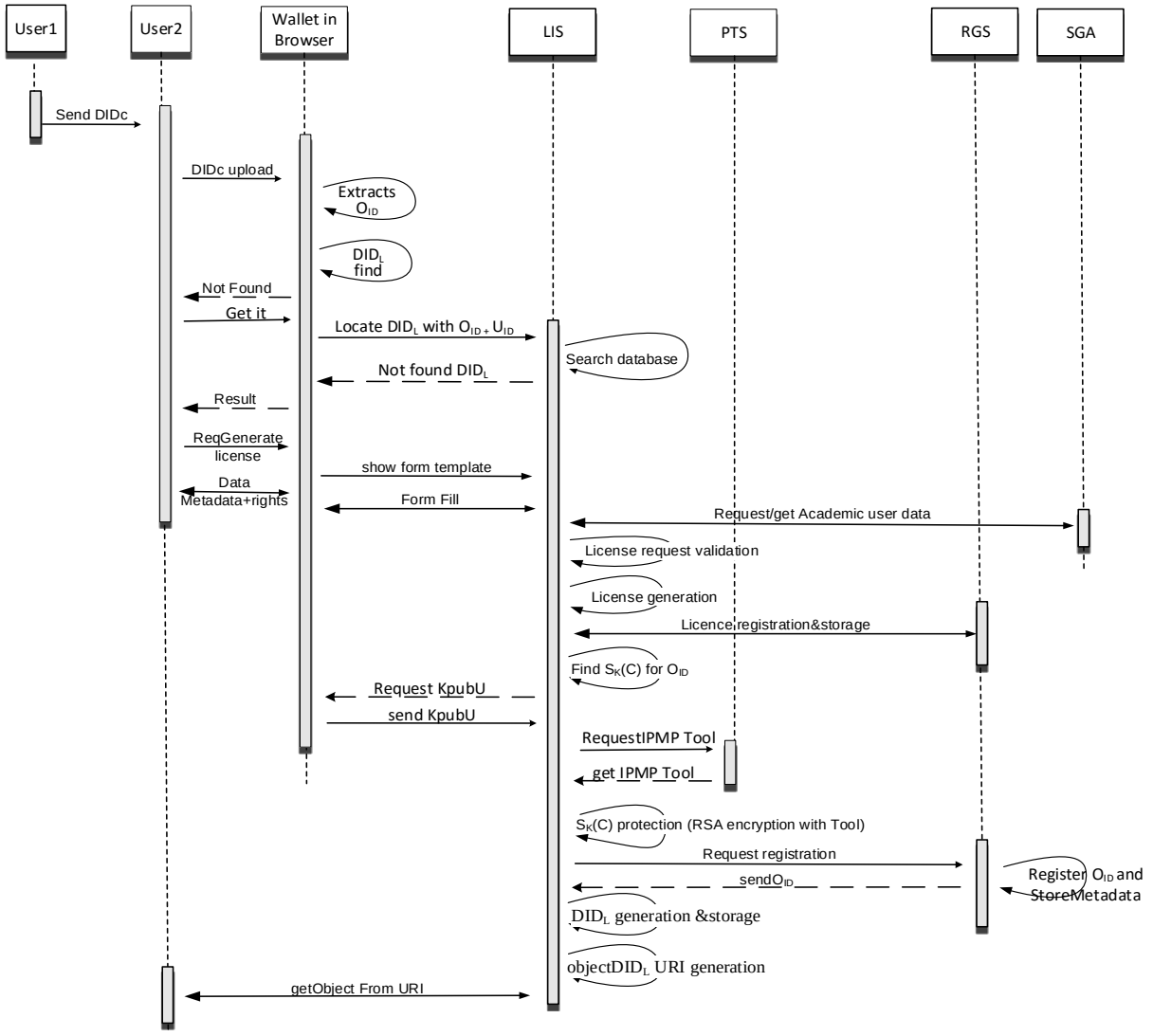


Figura 65 – ARMS e superdistribuição

4.2 O Media Player/Wallet

O ARMS, ao seguir a mesma abordagem do OpenSDRM, permite que várias aplicações de conteúdo possam partilhar o acesso ao conteúdo, atuando o Wallet como mediador. Este facto vem disponibilizar uma camada adicional relativa à interoperabilidade do lado do cliente, assim como do lado servidor, pois o cliente é independente do servidor de onde obtém as licenças (Serrão et al., 2005a). Contudo o cliente deve requerer autorização ao Wallet para executar

operações sobre o conteúdo. O Wallet é responsável por obter as licenças do servidor, interpretá-las e analisar os direitos associados ao conteúdo antes de dar permissões de aceitação ou rejeição da operação a realizar sobre o conteúdo. Isto inclui a desencriptação do conteúdo protegido com a cifra encriptada com a chave pública do utilizador armazenada no seu dispositivo.

5 Conclusão

A norma MPEG-21 ao ser aqui utilizada fornece as ferramentas adequadas capazes de aumentar a partilha de conteúdo, ao mesmo tempo que permite preservar os direitos básicos de PI, garantindo a sua transmissibilidade não só para conteúdo o protegido mas também para o desprotegido.

A norma MPEG-21, ao possibilitar que recursos e metadados possam ser embebidos numa estrutura altamente flexível baseada em XML, vem abrir caminho a que a sua transmissibilidade em meios abertos como a Internet se faça de uma forma neutra em termos de formato. Além de vários tipos de licenciamento poderem também ser integrados através desta norma, o MPEG-21 permite a definição de uma base comum para a estrutura de documentos que representam o conteúdo (protegido ou não) e informação relacionada sobre direitos, não descurando a integração com métodos de proteção. Sendo o ARMS um sistema resultante do OpenSDRM adaptado e alinhado com o modelo inicial aqui proposto, é um exemplo desta integração indo ao encontro das necessidades do contexto académico. Para tal, recorre à interação via *Web services* com o sistema de gestão académica da instituição para verificar a elegibilidade do utilizador perante um pedido de licença. Ao englobar um conjunto de serviços *Web* que permitem estabelecer interfaces entre componentes do sistema e de módulos de retaguarda que dão o suporte à emissão dos objetos, acaba por dar o suporte para garantir o controlo sobre a emissão de licenças dentro do domínio académico.

Os métodos apresentados neste capítulo oferecem o suporte necessário para os restantes capítulos, atuando como base da implementação da plataforma de DRM especificamente vocacionada para a governação de conteúdos de cariz académico no que respeita ao processo de transmissão de direitos com o respeito da linha sucessória.

Com base no trabalho aqui descrito foi produzida a comunicação científica em Marques & Serrão, (2015b).

Capítulo 8

ARMS – Sistema DRM adaptado ao contexto educacional e académico

Resumo

No meio académico, os principais intervenientes no ciclo de vida do conteúdo ao sentirem a necessidade de reproduzir e distribuír conteúdo abrangido por PI, têm de recorrer a mecanismos de proteção capazes de lhes assegurar um ambiente em que a partilha de conteúdo fica sob o seu controlo (Barik & Karforma, 2012). O ARMS é capaz de assegurar esse ambiente, pois utiliza as técnicas de DRM adequadas para a proteção de conteúdos e direitos associados. Para melhor se perceber o seu alinhamento com o modelo proposto e a sua aplicabilidade ao contexto académico, iremos utilizá-lo como referência na proteção de conteúdos e gestão de direitos, tendo sempre por base a norma MPEG-21. Com vista a enquadrar este sistema com o contexto académico serão tidas em consideração as principais interações desta plataforma com o SGA, o qual está subjacente à administração dos atos académicos de qualquer instituição académica moderna, descrevendo-se os métodos e fases de proteção de conteúdos e de transferência de direitos nas situações mais comuns a este meio. A principal contribuição deste capítulo consiste na descrição detalhada das interações entre os diversos componentes do ARMS e nas bases tecnológicas em que assenta o sistema de proteção e as ferramentas de suporte.

1 Introdução

Tal como o OpenSDRM, o ARMS é uma plataforma que integra diferentes elementos DRM numa arquitetura distribuída orientada a serviços, sendo independente do tipo de conteúdos, da proteção aplicada e do modelo de negócios sob o qual o conteúdo é consumido (Serrão, Dias & Delgado, 2005a). Estes elementos permitem a implementação de funcionalidades de proteção de conteúdos, expressão de direitos, gestão de licenças, registo de conteúdos e de metadados e pagamentos (Serrão, Neves, Kudumakis, Barker, & Balestri, 2003), assentando a integração destes elementos a sobre uma arquitetura baseada no paradigma orientado a serviços (SOA) (Serrão et al., 2006a). A comunicação e a segurança entre os diferentes serviços assentam essencialmente em dois patamares. Um primeiro patamar é baseado em ligações seguras HTTP (recorrendo ao SSL/TLS e certificados X.509 instalados nos servidores) que permitem uma

comunicação segura e autenticada entre serviços oferecidos pelo OpenSDRM. Um segundo patamar de segurança é estabelecido a nível aplicacional e permite que através de diversos mecanismos sejam asseguradas a integridade, autenticação e não repúdio necessários dos diversos serviços. Por outro lado, este último patamar permite a permuta segura de mensagens SOAP entre os vários serviços de forma independente da segurança do próprio servidor (oferecida pelo patamar anterior). De igual forma, este patamar também permite a comunicação segura com atores externos, dependendo de um conjunto de interfaces que permitem a comunicação entre os diversos componentes internos e externos (Serrão, et. al., 2005b). No contexto académico, a implementação de interfaces com o SGA no ARMS vem permitir que o estabelecimento de comunicações baseadas em serviços *Web* suporte funcionalidades relacionadas com autorizações para acesso e uso de conteúdo.

Estando um dos nossos focos de investigação orientado para uma forma efetiva de proteger o conteúdo e os direitos de PI, iremos debruçar-nos sobre a forma como as ferramentas criptográficas baseadas em MPEG-21 são capazes de fornecer essas funcionalidades de proteção tendo em conta a interação do núcleo do ARMS com o SGA. Entender como os elementos constituintes dos documentos DID são processados com vista a assegurar que os direitos de PI são respeitados, nomeadamente os mais relevantes no contexto académico e académico, é outro dos objetivos. Por isso, dar-se-á especial realce nas subsecções seguintes à descrição da implementação dos conceitos do MPEG-21 no ARMS.

2 ARMS

Independentemente da importância dos vários componentes do ARMS dentro da própria infraestrutura e considerando o cenário de implementação no contexto académico e académico, neste capítulo iremos essencialmente debruçar-nos sobre as variadas interações com o SGA e os processos de proteção e licenciamento relacionados com a partilha de conteúdo com vista a garantir a preservação de direitos sucessórios entre os participantes ao longo da cadeia de distribuição. As secções seguintes irão descrever o sistema e a interação com este componente de modo a atingir os seus objetivos. Para tal deve considera-se que no ARMS:

- Todos os componentes da plataforma são de confiança, não estando adulterados, e comportam-se tal como o esperado;
- Todos os componentes permutam mensagens por um canal seguro e autenticado, usando cada um dos componentes o seu par de chaves (K_{pub}/K_{priv}) e certificados digitais para estabelecer este canal;

- Todos os componentes estão registados no AUS e possuem credenciais válidas ($Cert^{AUS}$) emitidas pelo AUS;
- No lado do utilizador está implementada uma aplicação específica que permite ao utilizador registar-se na plataforma ARMS, efetuar o carregamento do conteúdo que pretende partilhar e definir as regras de controlo de acesso e uso do conteúdo publicado;
- A proteção do conteúdo será fornecida através da aplicação de diferentes ferramentas de proteção disponibilizados através do PTS. Sempre que um utilizador for autorizado a realizar uma ação sobre o conteúdo, serão utilizados os mecanismos adequados inerentes às ferramentas de proteção disponibilizadas pelo PTS para esse fim.

A proteção de conteúdos e a expressão de direitos será implementada através da aplicação da norma MPEG-21, tendo em conta os conceitos anteriormente abordados ao longo desta tese relativos à proteção e transmissão de conteúdos com vista à sua partilha. Nesta secção descrever-se-á a implementação da MPEG-21 IPMP e REL no ARMS com vista à proteção do conteúdo e processamento dos elementos presentes nos documentos DID onde estão inseridos, de modo a que o acesso e uso sejam realizados de acordo com os termos e condições expressos na licença. A norma MPEG-21 será aplicada na criação de expressões de direitos e para autorizar a realização de ações sobre o conteúdo.

Para que os conteúdos possam ser transportados e partilhados, utilizam-se objetos digitais sob a forma de documentos DID que consistem no objeto protegido e de informação relacionada sob a forma de expressões de informação IPMP. Estas expressões IPMP podem conter informação sobre a proteção (como, por exemplo, ferramentas IPMP que protegem o conteúdo), parâmetros de inicialização, chaves de encriptação, informação de governo do conteúdo (por exemplo, licenças que governam o uso do conteúdo) ou referências a estas licenças ou serviços de licenças. As funcionalidades de governo de direitos sobre conteúdos implementadas no ARMS estão de um modo geral relacionadas com os direitos de utilização do conteúdo. Contudo, nem sempre todas estas funcionalidades estão presentes para todo e qualquer tipo de utilizador, pois tal depende do seu perfil e do contexto em que se insere. No geral, e independentemente do método de criação dos objetos digitais, as principais funcionalidades a considerar são:

- Criação e armazenamento das expressões de direitos (na forma de licenças modelo);
- Autorização da utilização de conteúdos baseadas nas licenças de utilização.

A proteção do conteúdo e a gestão das ferramentas responsáveis fica, por isso, a cargo do componente PTS no ARMS. O LIS permite gerar a informação relacionada com a proteção a

ser incluída nos itens digitais assim como a relacionada com a gestão das chaves de proteção. A existência dos componentes AUS e CFS, ao obrigar que todos os componentes estejam registados e devidamente identificados e localizados, vem permitir o estabelecimento de um elevado nível de confiança no sistema ARMS, pois garante a certificação e autenticação de todos os atores e ferramentas.

O ARMS, para suportar funcionalidades concordantes com a norma MPEG-21, leva a que algumas alterações tenham de ser introduzidas na arquitetura OpenSDRM. As principais diferenças ao nível de interações relativamente à arquitetura original interna do OpenSDRM podem ser ilustradas através da Figura 66, onde é possível observar a integração de um novo componente, o SGA, que estabelece comunicação com o núcleo do OpenSDRM. Além disso, os componentes do OpenSDRM, Content Production Server (CPS) e License Server (LIS) estão adaptados, de modo a suportar itens digitais conforme a norma MPEG-21.

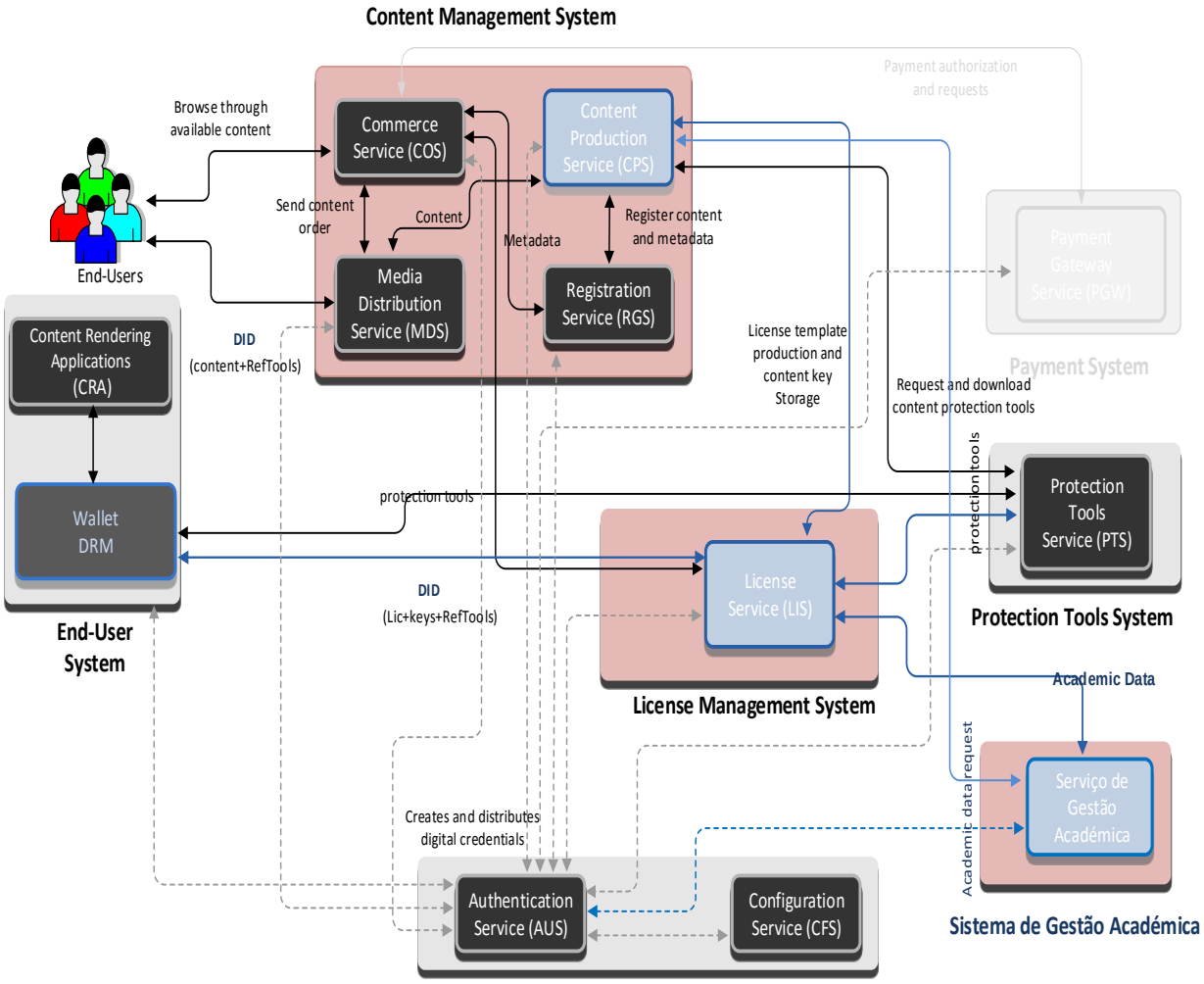


Figura 66 – Compoentes ARMS e principais interações

2.1 ARMS e utilização de objetos digitais

Para proteger o conteúdo é aqui proposto um esquema que incorpora dois patamares distintos, mas interligados pelo fluxo de conteúdo e pelo fluxo de informação relacionada com a proteção em que se faz recurso às normas MPEG-21 para o transporte e proteção dos objetos relacionados. Um dos patamares (patamar A) está relacionado com o fluxo do conteúdo entre os componentes nucleares do ARMS e a sua existência é fundamental na proteção do conteúdo. O outro patamar (patamar B) está relacionado com o fluxo das chaves que protegem o conteúdo e a sua existência é fundamental na proteção dos mecanismos que protegem o conteúdo. A sua separação vem permitir que os objetos resultantes possam ser protegidos e transmitidos independentemente. O esquema de proteção encontra-se ilustrado na Figura 67.

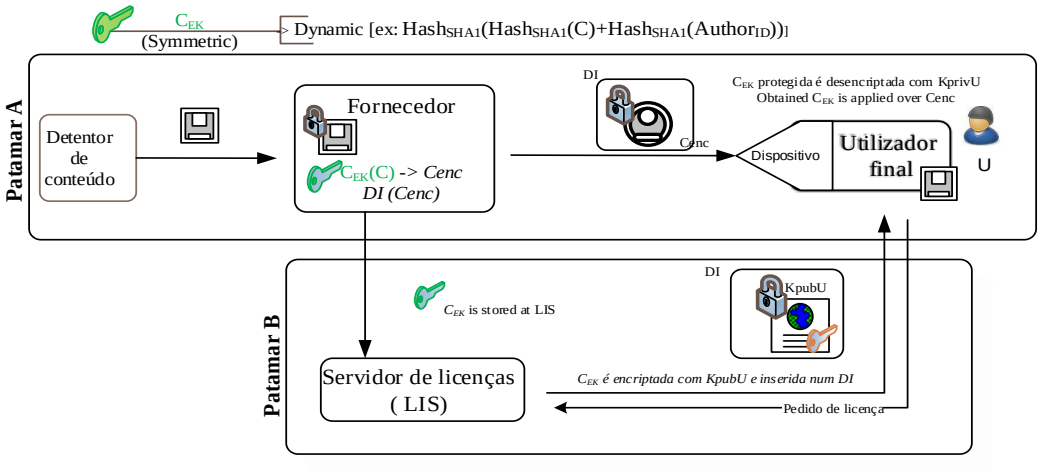


Figura 67 - Patamares de proteção no ARMS

O fluxo de conteúdo é iniciado através do patamar A, sendo aí aplicada encriptação simétrica sobre o conteúdo com uma ferramenta que utiliza o algoritmo AES requerida ao PTS. Visto a encriptação/desencriptação AES ser simétrica, esta torna-se a adequada para conteúdos de grande dimensão. Para evitar que a chave a aplicar na encriptação seja idêntica em todos os conteúdos que se pretenda encriptar, aplica-se uma chave dinâmica obtida a partir de parâmetros variáveis baseados no resumo do próprio conteúdo e na identificação do detentor do conteúdo. Desta forma, obtém-se um conteúdo encriptado onde a cifra que dá acesso ao conteúdo é diferente para conteúdos diferentes mesmo que o autor seja o mesmo. Utiliza-se aqui a função de resumo $Hash_{SHA1}\left(Hash_{SHA1}(C) + Hash_{SHA1}(Author_{ID})\right)$ para obter a cifra.

Na abordagem seguida no ARMS é assumido que um conteúdo protegido só tem utilidade se houver um objeto que contenha e transporte a chave que permita desencriptar a cifra que dá o acesso ao conteúdo protegido. Caso não exista esse objeto (o objeto licença), ou este não contenha a chave que dá acesso ao conteúdo, então deixa de fazer sentido a preservação de

direitos ao longo do ciclo de vida do conteúdo. Independentemente disso há a ter em conta que no ARMS devemos distinguir duas vertentes: o conteúdo a proteger e a ferramenta de proteção a que está associado um método de proteção. O método de proteção tem uma chave associada que permite atuar sobre o conteúdo. Assim, quem detiver esta chave pode ativar esse método de proteção. No caso do conteúdo, a chave do recurso (S_K) é a chave simétrica (cifra) e é gerada variavelmente baseando-se o seu valor na função de resumo cujos parâmetros são o *hash* do conteúdo e o *hash* da identidade do autor/detentor de conteúdo:

$$S_K = Hash_{SHA1}\left(Hash_{SHA1}(C) + Hash_{SHA1}(Author_{ID})\right)$$

C - Conteúdo Digital
AuthorID - Identificação do autor/detentor de conteúdo no AUS
$Hash_{SHA1}$ - Função criptográfica de resumo SHA1 (*hash*)

A utilização desta função na obtenção da cifra permite que a mesma chave do recurso seja gerado em múltiplos *sites* pelo mesmo autor/detentor de conteúdo, mas só para esse mesmo conteúdo. Esta cifra corresponde à chave de encriptação do conteúdo (C_{EK}) anteriormente apresentada na proposta de modelo (Capítulo 4). A função de resumo, ao utilizar estes parâmetros cujos valores são aleatórios, tem a vantagem de tornar a função dinâmica, pois os valores obtidos para a cifra são derivados destes, sendo, por isso, diferentes consoante o conteúdo e o autor. Para fazer com que essa cifra de desencriptação de conteúdo chegue de forma segura e seja somente útil ao utilizador legítimo, dá-se início a um outro fluxo em que se faz recurso a um canal seguro no patamar B, onde a cifra é encriptada através da aplicação de algoritmos de chave pública (K_{pub}^U/ K_{priv}^U). Ou seja, neste patamar, a chave associada ao recurso é a chave pública do utilizador $K_{pub}^U(S_K)$. Separando estes dois fluxos em dois patamares distintos, podemos desta forma garantir um nível de segurança adequado capaz de assegurar a confidencialidade no decorrer da transmissão do conteúdo.

Quer o conteúdo encriptado quer a cifra que lhe dá acesso, apresentam-se sob a forma de um documento DID em conformidade com as normas MPEG-21 e de acordo com a estrutura apresentada anteriormente (Capítulo 7). Enquanto um é representado sob a forma de um objeto digital de conteúdos DID_C, o outro apresenta-se sob a forma de objeto digital licença DID_L. Assume-se que a transmissão das chaves ao utilizador final é realizada pelo LIS, podendo o conteúdo protegido ser inicialmente disponibilizado pelo MDS (depois disso pode estar disponível por qualquer canal de distribuição).

As interações entre o utilizador e os principais componentes do ARMS para obter a chave de proteção que dá acesso ao conteúdo obedecem aos seguintes passos:

- O utilizador final, depois de obter o conteúdo sob a forma de um objeto DID_C interage com este e verifica através do dispositivo do cliente se a assinatura do objeto $DID_{C,}$ onde o conteúdo está embebido, é válida. Se não houver validação da assinatura, o utilizador é avisado e o processo termina;
- Se o resultado for positivo, o cliente verifica se internamente já existe armazenado no dispositivo um objeto DID_L correspondente ao conteúdo, contendo a licença de utilização. Se esta for encontrada, o conteúdo é utilizado nos termos e condições aí especificados;
- Se não a encontrar interage com o LIS através de um formulário onde lhe pode requerer uma licença de utilização para esse conteúdo enviando um pedido com as suas credenciais;
- O LIS procura na base de dados interna se já existe uma licença prévia para esse utilizador e condições especificadas. Caso já exista, disponibiliza-a para poder ser descarregado o objeto DID_L correspondente;
- Se não encontrou, então verifica a elegibilidade do utilizador contatando o SGA. Caso o utilizador não seja elegível (não pertence ao meio educativo ou académico), então o LIS envia uma mensagem ao cliente informando-o de tal;
- Caso o utilizador seja válido, então dá-se início à geração da licença de utilização;
- Se todas as fases forem concluídas com sucesso, o LIS irá proceder à geração do objeto digital DID_L com a estrutura definida anteriormente (Capítulo 7). Para tal, o LIS localiza a chave de proteção do conteúdo (previamente enviada pelo CPS) e encripta-a com a chave pública do utilizador inserindo o resultado no objeto DID_L, em simultâneo com outra informação relevante. O LIS disponibiliza um *link* para que o objeto gerado possa ser descarregado informando o cliente;
- O cliente descarrega o objeto, procede à verificação da assinatura digital do LIS no objeto digital e, caso tenha sucesso, recupera a chave de encriptação do conteúdo usando a sua chave privada e solicitando ao PTS a ferramenta adequada para desproteger o conteúdo (identificada no DID_C);
- Na posse da cifra de proteção e da(s) ferramenta(s) de proteção apropriada(s), o conteúdo pode ser desprotegido ficando disponível para utilização;
- O cliente instalado no dispositivo e o Agente DRM irão assegurar que os termos e condições de licenciamento são respeitados.

3 Proteção de conteúdo no ARMS

Seguindo os passos anteriores, o conteúdo protegido só pode ser acedido por um cliente previamente identificado pelo ARMS e utilizando as credenciais de um utilizador registado no sistema e elegível perante o SGA para poder obter licenças de utilização.

No ARMS qualquer conteúdo (C) tem associada uma chave de proteção do recurso, que neste caso é uma chave simétrica (S_K) e esta, por sua vez, tem associada uma chave $K_{pub}^{U}(S_K)$. Assume-se que todo e qualquer utilizador (U) do sistema ARMS (quer seja um criador/detentor de conteúdo ou um utilizador final) possui o par de chaves (K_{pub}^{U}/ K_{priv}^{U}) onde a chave pública pode ser verificada numa infraestrutura de chave pública (PKI), sendo que a chave privada é acessível somente ao utilizador. Este par de chaves é também usado para identificar os utilizadores e assinar as licenças e itens digitais.

3.1 Registo do utilizador

Em termos de governo e proteção de conteúdo, a utilização da plataforma ARMS requer que os utilizadores estejam previamente registados. No ARMS, o componente "Aplicação/Agente DRM" representa genericamente o componente responsável por lidar com a informação relacionada com o utilizador e por realizar a gestão interna das licenças que estão a intermediar o acesso ao conteúdo partilhado. Ao iniciar este componente pela primeira vez dá-se imediatamente início ao processo do registo do utilizador:

- A "Aplicação/Agente DRM" cria um par de chaves ($K_{pub}^{\mathbf{U}}$ / $K_{priv}^{\mathbf{U}}$) para o utilizador U;
- O utilizador U define uma palavra-passe secreta para o "Agente DRM". A partir dessa palavra-passe é gerado um resumo, que passa a ser a utilizado como a chave de armazenamento a ser usada na criação de um repositório seguro interno ($K_{SecureStorage}$ = SHA1 (palavra-passe)) e onde a chave privada do utilizador ($K_{priv}^{\mathbf{U}}$) é armazenada de uma forma segura. A palavra-passe somente é conhecida do utilizador e o dispositivo deste somente utilizará a chave privada se o utilizador estiver autenticado no sistema usando essa informação;
- O "Agente DRM" solicita informação ao utilizador U, confirma o endereço de e-mail do utilizador e envia ao componente AUS toda a informação encriptada: K_{pub}^{AUS}(U_{ID}, user information + $K_{pub}^{\mathbf{U}}$);
- O AUS confere a sua identificação perante o SGA (U_{ID}) solicitando dados via *Web* services. Com os dados enviados faz a associação entre o utilizador registado no ARMS e o existente no SGA.

- O AUS confirma o registo do utilizador e emite uma credencial ao utilizador: $Cert^{AUS}_{U}$. A credencial é usada para autenticar o utilizador perante outros componentes e serviços do ARMS.

Devido a diferenças de nomenclatura na identificação dos utilizadores do MPEG-21 ("*keyHolder*") e do SGA (como, por exemplo, um número de registo mecanográfico) torna-se necessário converter uma identificação noutra através da correspondência entre as chaves do MPEG-21 e o tipo de identificação atribuído no SGA. Para tal, quando o utilizador no ARMS se está a registar através do "Agente DRM", o AUS efetua um pedido ao SGA via serviços *Web*, obtém a identidade do utilizador e associa-a à chave pública desse utilizador gravando-a de seguida na sua base de dados.

3.2 Partilha de conteúdo

Para que o detentor de conteúdos tenha um controlo total sobre o que pretende partilhar e com quem o pretende realizar, várias funcionalidades de proteção e governo do conteúdo têm de ser ativadas. O ARMS, para garantir um nível de confiança que assegure esse controlo, recorre a dois canais independentes mas relacionados. Um por onde é transportado o objeto conteúdo protegido (MDS → Utilizador final ou então Utilizador final →Utilizador final), e outro por onde é transportado o objeto licença (LIS → Utilizador final) contendo a cifra que protege o conteúdo e a respetiva licença. Assim, podemos distinguir dois tipos de objetos em consonância com o modelo e estrutura anteriormente propostos tendo por referencial a norma MPEG-21: o documento DID_C contendo o conteúdo protegido com a chave S_K, e o documento DID_L contendo a licença e a chave S_K encriptada com a chave pública do utilizador que fez o pedido para emissão de licença. No canal onde o objeto conteúdo é transportado, o conteúdo é protegido com a chave S_K através de uma ferramenta IPMP disponibilizada pelo PTS, sendo embebido num documento DID, e assinado digitalmente pelo MDS, Dsig (K_{priv}^{MDS}, DID_C), que o disponibiliza ao utilizador para poder ser descarregado. As interações entre os componentes ARMS na criação do documento DID_C têm em conta os seguintes passos (Figura 68):

1- Carregamento do conteúdo para o CPS;

2 - Geração da cifra de proteção de conteúdo $S_{K;}$

3 e 4 - Pedido de ferramenta de proteção e proteção do conteúdo;

5 - Envio do conteúdo protegido para o MDS;

6 - Geração do objeto conteúdo e armazenamento;

7- Envio do objeto conteúdo ao Cliente.

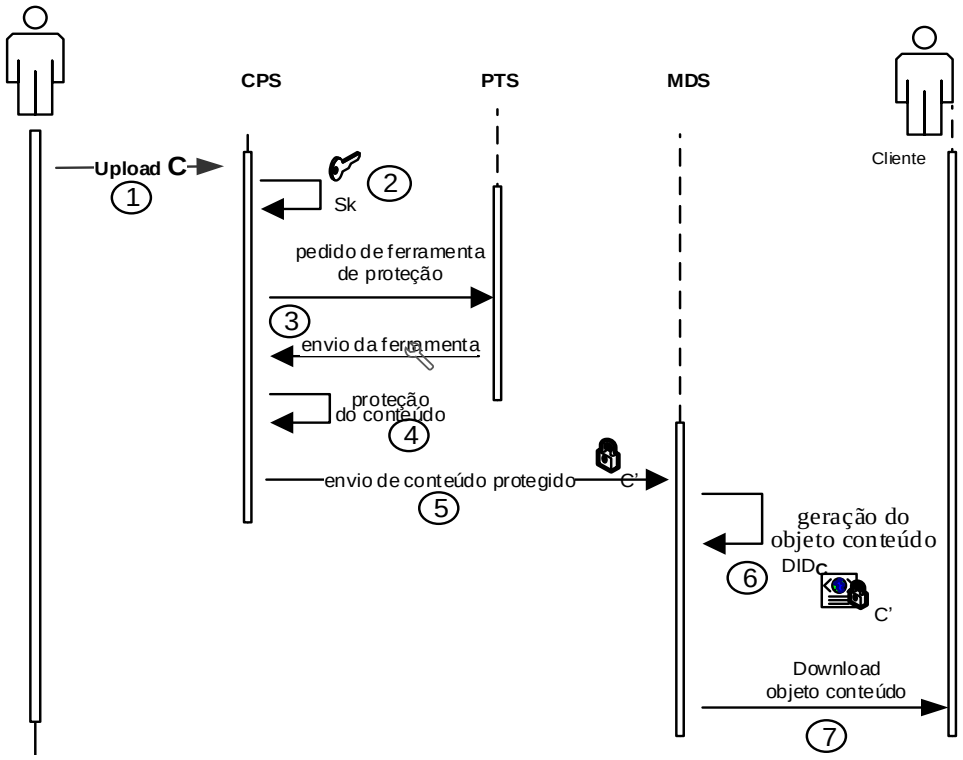


Figura 68 – Proteção do conteúdo e criação do documento DID_C

Sempre que há necessidade de gerar uma nova chave de proteção do conteúdo (S_K), um módulo específico implementado no CPS realiza essa operação e encripta o conteúdo com a ferramenta disponibilizada pelo PTS. Quando o conteúdo sob a forma de um documento DID_C é recebido pela "Aplicação/Agente DRM", a integridade do mesmo é aqui verificada através da assinatura digital embebida pelo MDS. De seguida, a "Aplicação/Agente DRM", obtém do documento DID_C toda a informação relacionada com a ferramenta usada na proteção e estabelece a ligação a PTS para a poder obter.

No canal onde o objeto licença é transportado, a chave de cifra S_K que protege o conteúdo é enviada ao LIS. Sempre que o utilizador pede uma licença de utilização do conteúdo ao LIS este contacta o SGA para verificar se o utilizador pertence ao domínio académico. Se o resultado for positivo e obedecer às condições especificadas pelo detentor de direitos na licença modelo, a chave S_K é encriptada com a chave pública do utilizador que fez o pedido $K_{pub}^{U}(S_K)$, através de uma ferramenta de proteção disponibilizada pelo PTS. Esta chave encriptada fica armazenada no LIS numa base de dados segura ficando disponível para o processo de emissão de licença. A chave encriptada e a licença de utilização gerada pelo LIS são finalmente embebidas no documento DID, sendo este então assinado digitalmente pelo LIS, Dsig (K_{priv}^{LIS}, DID_L), que o vai disponibilizar ao utilizador para o poder descarregar. A Figura 69 ilustra resumidamente as interações entre os componentes ARMS na criação do documento DID_L,

tendo em conta os seguintes passos (é assumido que a chave de proteção de conteúdo está armazenada em LIS):

1. Pedido de emissão de licença pelo cliente ao LIS e envio da chave pública;
2. Pedido/envio de dados entre LIS/SGA e validação da elegibilidade do pedido pelo LIS;
3. Pedido/envio de ferramenta de proteção;
4. Encriptação de cifra de proteção do conteúdo com a chave pública do utilizador;
5. Geração do objeto de direitos;
6. Envio do objeto de direitos ao cliente.

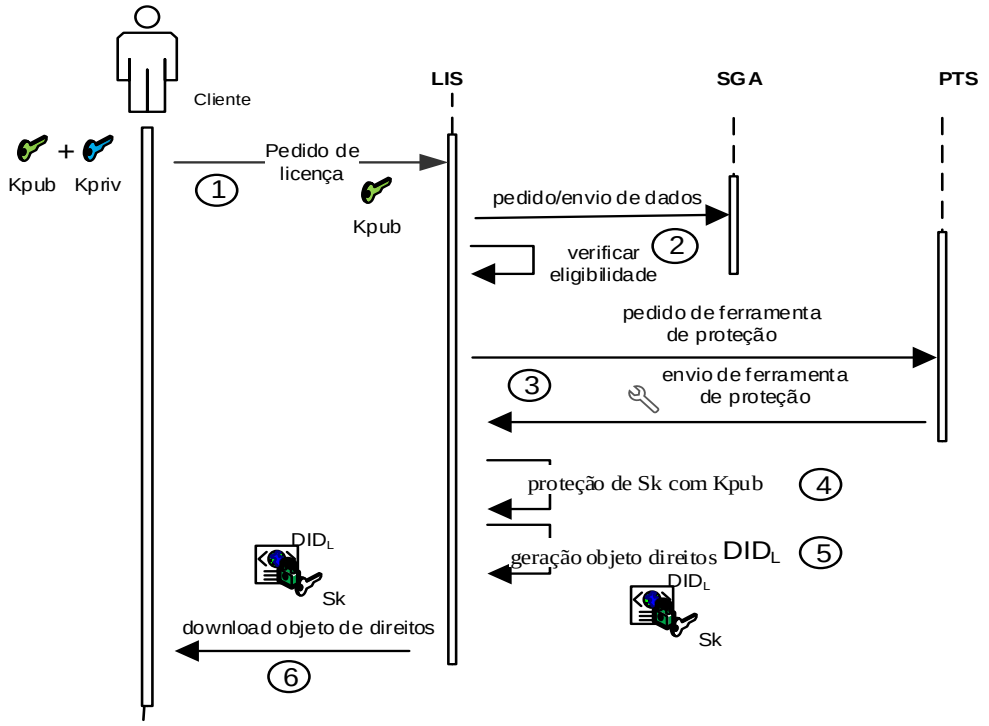


Figura 69 - Proteção da cifra de proteção do conteúdo e criação do documento DID_L

Sempre que existe a necessidade de encriptar a cifra S_K que protege o conteúdo, um módulo específico implementado no LIS realiza essa função e encripta-a com a ferramenta disponibilizada pelo PTS. Se o pedido de emissão de licença for bem-sucedido, quando a chave de proteção de conteúdo encriptada com a chave pública, $K_{pub}^{U}(S_K)$, é recebida pela "Aplicação/Agente DRM" embebida num documento DID_L, a integridade do mesmo é verificada através da assinatura digital embebida pelo LIS. De seguida, a "Aplicação/Agente DRM" obtém do documento DID_L toda a informação relacionada com a ferramenta usada na encriptação e estabelece a ligação ao PTS para a obter, e, na sua posse, procede então à desencriptação da cifra de proteção do conteúdo, S_K, com a chave privada do utilizador $K_{priv}U$.

Estando na posse desta cifra e da ferramenta necessária à desencriptação do conteúdo, então o "Aplicação/Agente DRM" procede à extração do conteúdo do documento DID_C e inicia a sua desencriptação. À medida que o conteúdo vai sendo desencriptado, a "Aplicação/Agente DRM" dá acesso ao utilizador que efetuou o pedido de emissão de licença para esse conteúdo, mas assegurando que os direitos expressos na licença embebida no documento DID_L são sempre respeitados.

3.3 Objetos DID_C e DID_L

Os documentos DID_C (objeto conteúdo) e DID_L (objeto de direitos ou objeto licença) são gerados no ARMS através de um módulo especial nos componentes CPS e LIS, respetivamente. Estes módulos, o IM e o ILM funcionam como uma ponte entre a fonte do conteúdo e o documento DID final, sendo das peças mais importantes, pois, ao embeber o conteúdo numa estrutura com formato universal baseado em XML, contribuem para uma maior interoperabilidade da solução proposta. A estrutura destes objetos apresenta-se de acordo com as especificações da norma MPEG-21 e é construída de acordo com o que foi anteriormente apresentado no Capítulo 7.

4. Protocolo de preparação, partilha e acesso ao conteúdo

Considerando as três principais fases do ciclo de vida do conteúdo (criação, distribuição e consumo) existente nos sistemas DRM, o ARMS não deixa de as considerar, pois ao permitir que a preparação, a partilha e o acesso ao conteúdo sejam realizados de forma controlada abrange todas estas fases típicas dos sistemas DRM. Para melhor perceber como o faz iremos detalhar cada um deles com mais pormenor. As seguintes convenções são de seguida utilizadas:

C	Conteúdo;
C_{ID}	Registo único de identificação do conteúdo;
O_{ID}	Registo único de identificação do objeto;
DID	Documento MPEG-21;
$Hash_{ALG}(n)$	Operação de geração de um resumo de dados (n), recorrendo a um algoritmo de resumo ($_{ALG}$);
S_K	Chave de proteção do conteúdo, gerada pela seguinte operação; $S_K = Hash_{SHA1}\left(Hash_{SHA1}(C) + Hash_{SHA1}(Author_{ID})\right)$;
K_{pub}^{Ent}	Chave pública da entidade (Utilizador, Servidor,…);
K_{priv}^{Ent}	Chave privada da entidade (Utilizador, Servidor,…);
E_X (C, S_k) → Cenc	Operação de encriptação do conteúdo C usando a cifra S_K com o algoritmo X (AES);

$D_X (C_{enc}, S_K)$	Operação de desencriptação do conteúdo C_{enc} usando a cifra S_K com o algoritmo X (AES);
$E_X (K_{pub}^{Ent}(i))$	Operação de encriptação sobre bloco de dados (i) usando a chave pública (K_{pub}) da entidade "Ent" com o algoritmo X (RSA);
$D_X (K_{priv}^{Ent}(K_{pub}^{Ent}(i))$	Operação de desencriptação sobre bloco de dados (i), usando a chave privada (K_{priv}) da entidade "Ent" com o algoritmo X (RSA);
$D_{SIG} (K_{priv}^{Ent}(k))$	Operação de geração da assinatura digital sobre dados (k), recorrendo à chave privada de "Ent" (K_{priv}^{Ent}).

4.1 Preparação do conteúdo no ARMS

Os utilizadores que atuam sobre o sistema ARMS podem assumir diferentes perfis consoante o papel assumido. Tanto podem ser autores, sendo estes os donos do conteúdo e de direitos associados (aqueles que criam e possuem o conteúdo podendo transmitir direitos a terceiros para que estes possam aceder e usar o conteúdo), como simples utilizadores que consomem o conteúdo, tendo acesso e uso de acordo com o especificado nos termos e condições da licença de utilização. Todas as ações sobre o conteúdo são executadas através de uma aplicação residente no dispositivo cliente: o "Aplicação/Agente DRM". No decorrer do consumo todas as ações são controladas de acordo com os termos e condições especificados na licença de utilização. Com vista a disponibilizar o conteúdo ao utilizador, o detentor do conteúdo acede à plataforma ARMS a partir da sua aplicação cliente:

- O utilizador seleciona o componente adequado previamente instalado. Caso ainda não tenha iniciado a sessão no sistema, ou esta já tiver expirado, introduz então as suas credenciais, que podem ser compostas por um nome de utilizador e a correspondente palavra-chave;
- O sistema valida o utilizador através do componente AUS do ARMS e, caso as credenciais sejam as corretas, é autenticado no sistema dando início à sessão;
- O utilizador procede ao carregamento do conteúdo C para o CPS do ARMS e adicionalmente introduz metadados descritivos do conteúdo através de um formulário que irá ser usado pelo RGS no registo do conteúdo. Nesta fase o CPS poderá contactar o SGA com vista a verificar se o utilizador pertence ao domínio académico e se pode fazer o carregamento de conteúdos;
- O CPS é o responsável por preparar o conteúdo para ser partilhado e tal pode incluir o empacotamento, a codificação e a proteção do conteúdo. Para proteger o conteúdo o CPS precisa de obter a(s) ferramenta(s) de proteção do PTS. Para tal, contacta-o e efetua o descarregamento das ferramentas de proteção adequadas;

- O CPS contacta o RGS, registando o conteúdo e associando os metadados. O RGS atribui um identificador único ao conteúdo (C_{ID}), e envia-o ao CPS, assinando o mesmo: $K_{pub}{}^{CPS}(K_{priv}{}^{RGS}(C_{ID}))$;
- O CPS gera a chave de proteção do conteúdo S_K, e com a ferramenta de proteção entretanto obtida de PTS encripta o conteúdo, E_{AES} (C, S_k). O CPS armazena estes dados e de seguida dá início à geração do documento DID_C através do módulo IM nele alojado enviando o pacote assinado digitalmente ao MDS conjuntamente com metadados;
- Para tal o CPS contacta o RGS para registar o objeto e atribui um identificador único ao objeto conteúdo (O_{ID}). Com a informação obtida, metadados e o C_{ID}, o módulo de ingestão IM procede à criação do objeto conteúdo embebendo toda a informação de acordo com a estrutura DID_C (Capítulo 7);
- O CPS gera e envia a chave de proteção do conteúdo S_K ao LIS, que a armazena, para que este, posteriormente, a possa proteger, assim como metadados referentes ao conteúdo, O_{ID}. C_{ID} e chaves do utilizador;
- O LIS, com estes dados, disponibiliza ao detentor de conteúdo um formulário onde este enquadra e define os termos base e direitos de utilização a escolher pelo utilizador final. Com esta informação o LIS cria e armazena uma licença modelo de distribuição correspondente ao objeto com O_{ID} disponibilizando a sua localização URI ao CPS;
- O MDS cria uma URI especial contendo o identificador único do objeto, $O_{ID,}$ e disponibiliza-o para que um utilizador possa descarregar o objeto conteúdo DID_C armazenado na plataforma ARMS.

O conteúdo enviado pelo detentor encontra-se agora armazenado, protegido e sob o governo da plataforma ARMS (Figura 57 – Capítulo 7) podendo ser partilhado. O utilizador final pode usar o URL para obter conteúdo através do ARMS fazendo recurso aos mecanismos fornecidos. Visto os mecanismos que permitem a partilha de conteúdo do ARMS se sobreporem a qualquer outra forma de partilha de conteúdo convencional, o detentor de conteúdo pode partilhar tudo o que quiser publicamente na plataforma. Estando na sua posse, o utilizador poderá disponibilizar o objeto conteúdo a terceiros (por um conjunto de meios alternativos).

4.2 Partilha e regras de utilização do conteúdo

Tal como em diversas áreas, no campo académico torna-se possível estabelecer pré-condições de utilização, de modo a que o utilizador fique enquadrado nessas pré-condições estabelecidas. Para poder associar regras de utilização ao conteúdo, o ARMS disponibiliza ao autor/detentor

de direitos, quando faz o carregamento do conteúdo, uma interface que lhe permite definir como o conteúdo pode ser usado. Esta operação tem como resultado final uma licença modelo que está ligada ao conteúdo colocado sob o governo da plataforma ARMS, cujo objetivo é suportar a expressão de direitos relativamente ao conteúdo em causa. Um exemplo pode ser dado quando um autor/detentor de conteúdo (por exemplo, um professor) pretender dar acesso a um estudante ou grupo de estudantes matriculados num dado curso de um determinado ano. Um outro exemplo pode ser quando a editora universitária pretender dar um desconto ou fazer uma promoção só para os seus alunos que adquiram um determinado publicação digital ou conteúdo. Independentemente de algumas operações relativas à proteção do conteúdo estarem relacionadas com o descrito na secção anterior, há a considerar os seguintes passos:

- O CPS contacta o LIS e pede-lhe a lista de licenças modelo que estão disponíveis;
- O autor/detentor de conteúdos seleciona uma das licenças modelo disponibilizadas através do CPS sob a forma de um formulário. Adicionalmente o ARMS poderá permitir que se possam desenhar e gerar licenças modelo personalizadas adaptadas a situações muito específicas caso o detentor entenda que as existentes são insuficientes. As licenças são criadas em conformidade com a especificação MPEG-21 de acordo com a estrutura definida, tal como descrito no capítulo anterior;
- O autor/detentor de direitos seleciona os campos adequados estabelecendo as condições de utilização. Caso algumas destas condições estejam relacionadas com o meio académico (por exemplo, conteúdo específico a alunos de determinado ciclo de estudos), o LIS contacta o SGA e verifica a elegibilidade do detentor de conteúdo para definir essas condições (por exemplo, somente o professor da unidade curricular X na posse do conteúdo pode definir condições para essa disciplina no atual ano letivo);
- Se a elegibilidade for validada, é então produzida e armazenada no LIS uma licença modelo com essas condições e referente ao conteúdo e ao autor/detentor de conteúdo.

Se o autor/detentor de conteúdo precisar de definir outro tipo de licença modelo, poderá repetir os passos acima indicando os novos termos e condições com que pretende que o utilizador possa aceder e usar o conteúdo.

4.2.1 Licença de distribuição

A licença modelo criada pelo autor/detentor de conteúdo é onde se encontram definidas as condições de utilização genéricas não individualizadas. Desta forma acaba por ser o instrumento do fornecedor de conteúdo que lhe vai permitir definir o modelo de negócio sob o qual pretende realizar a distribuição. As interações entre o fornecedor de conteúdo e o ARMS

requerem clarificações adicionais, pois é preciso aprofundar o relacionamento estabelecido no decorrer da geração das licenças padrão para distribuição de conteúdo. As condições padrão de utilização são aqui estabelecidas e quando o utilizador final precisa de uma licença de utilização acaba por indiretamente interagir com esta licença modelo para obter a sua licença de utilização. Em termos práticos o fornecedor acaba por criar uma licença pai que concede um conjunto de direitos ao utilizador final a quem for emitida uma licença filho. Estando criada essa licença, o utilizador pode interagir com o ARMS. Este tipo de licenças é criado quando o detentor de conteúdo efetua o carregamento do conteúdo e o regista, interagindo com um formulário onde define as condições globais a que a utilização do conteúdo deve obedecer. O fornecedor cria uma licença de distribuição que enquadra o utilizador final com os direitos e condições que poderá receber através da licença a emitir e que será embebida no objeto licença MPEG-21.

4.3 Acesso ao conteúdo

Estando a URI do objeto conteúdo disponível na plataforma ARMS, torna-se possível a qualquer utilizador descarregar e posteriormente distribuir livremente este objeto. Contudo, para que o objeto tenha utilidade, o utilizador necessita de uma "Aplicação/Agente DRM" que consiga interpretar os elementos do documento DID. Recorrendo à instalação da "Aplicação/Agente DRM" disponibilizada pelo ARMS, o utilizador final poderá aceder ao objeto digital e interpretar os seus elementos constituintes, mas adicionalmente necessitará de um objeto licença que o autorize a usar o conteúdo. Os passos seguintes mostram como se processa o acesso ao conteúdo de um utilizador autenticado na plataforma.

O utilizador, registado no ARMS e com o componente apropriado instalado no seu dispositivo, pode navegar pela lista do conteúdo aí armazenado. Sempre que é detetado um objeto apropriado ao ARMS representando conteúdo protegido sob o seu governo ou se o utilizador o selecionar explicitamente, a aplicação extrai e apresenta ao utilizador a informação genérica relacionada com metadados do objeto (título, autor, DOI, entre outros) dando início à execução dos seguintes passos:

- O utilizador autentica-se no sistema (assume-se que o utilizador pertence ao meio académico, tendo essa confirmação sido realizada perante o SGA);
- A aplicação procede à extração da assinatura digital do objeto conteúdo DID_C e executa a validação da assinatura digital contactando o MDS para obter a respetiva chave pública K_{pub}^{MDS}. Caso a assinatura seja inválida, o processo termina informando o utilizador. Caso seja válida, extrai do objeto conteúdo DID_C o elemento que o identifica, $O_{ID,}$ e verifica se o utilizador possui armazenado o objeto licença DID_L correspondente;

1) Se o objeto licença existir no "Agente DRM" do dispositivo cliente:

- A aplicação cliente procede à validação da assinatura digital contactando o LIS para obter a respetiva chave pública K_{pub}^{LIS}. Caso a assinatura seja inválida, termina o processo informando o utilizador e propondo-lhe a obtenção de um novo objeto licença a partir da localização indicada no elemento "<LicenseColletion>" de DID_C. Caso a assinatura seja válida, inicia a extração dos elementos do objeto $DID_{L;}$
- Com os elementos extraídos de DID_L, a aplicação cliente, a partir da indicação da localização da ferramenta IPMP que encripta a cifra que protege o conteúdo C_{ID}, obtém a ferramenta indicada do PTS e aplica-a usando a chave privada do utilizador, $K_{priv}U$, sobre a cifra encriptada que protege o conteúdo, $D_{RSA}(E_{RSA}(S_K, K_{pub}U), K_{priv}U)$. O resultado final é a cifra desprotegida, S_K;
- Com os elementos correspondentes à licença para o conteúdo C_{ID} extraídos de DID_L, a aplicação cliente faz um conjunto de validações:

  - Verifica se a assinatura digital do emissor da licença é válida (usando K_{pub}^{LIS} sobre a Dsig do emissor da licença);

  - Verifica se o C_{ID} e o prazo da licença são válidos;

  - Verifica se o utilizador é o dono da licença emitida (usando $K_{priv}U$ sobre "<keyholder>");
- Caso todas as validações sejam bem sucedidas, é concedida ao utilizador permissão para prosseguir com a obtenção da ferramenta de desencriptação do conteúdo e para utilizar o conteúdo no dispositivo cliente de acordo com o(s) direito(s) expressos na licença fazendo aplicar as condições aí definidas. Para tal, a aplicação cliente procede à extração dos elementos do objeto $DID_{C;}$
- A partir dos elementos extraídos e sabendo a identificação da localização da ferramenta IPMP que protege o conteúdo $C_{ID,}$ (a partir de "<ipmpinfo:ToolRef>") contacta PTS, obtém a ferramenta e aplica-a com o valor de S_K sobre o conteúdo protegido, $D_{AES}(E_{AES}(C, S_K), S_K)$. O resultado final é o conteúdo desprotegido, C, podendo então este ser usado de acordo com os termos e condições especificadas na licença, que a "Aplicação/Agente DRM" fará com que sejam aplicadas;
- O "Agente DRM" armazena o conteúdo C em zona segura, e comunica à aplicação as ações que podem ser realizadas conforme o expresso na licença de utilização.

A utilização de conteúdo com as ferramentas IPMP e um objeto licença já emitido e armazenado no dispositivo cliente pode ser visualizada no diagrama de sequência ilustrado na Figura 70.

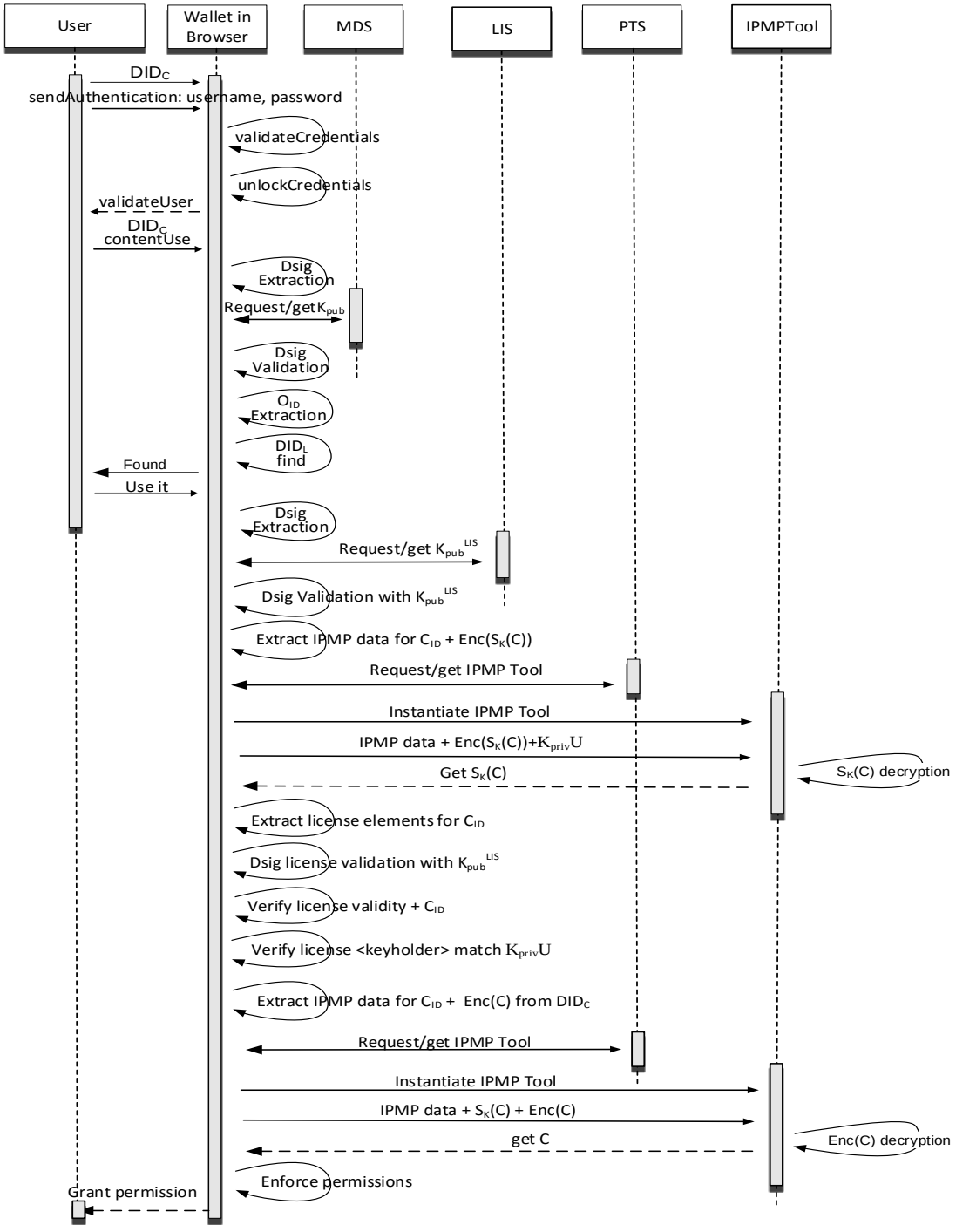


Figura 70 – Utilização de conteúdo com uma licença válida já armazenada no dispositivo

2) Se o objeto licença não estiver armazenado no "Agente DRM" do dispositivo:

- O "Agente DRM" apresenta ao utilizador a obtenção de um novo objeto licença. Caso seja aceite, o utilizador é redirecionado para a localização do componente ARMS (o LIS) indicada no elemento "<*LicenseColletion*> "do objeto $DID_{C;}$
- O "Agente DRM", ao contactar o LIS, pede a emissão de licença e envia o U_{ID}, as credenciais do utilizador ($Cert^{AUS}{}_{U}$) e o O_{ID}: $K_{pub}{}^{LIS}(K_{priv}{}^{U}(U_{ID}, Cert^{AUS}{}_{U}, O_{ID}))$;

- LIS recebe e valida a informação enviada, e usando o U_{ID} e O_{ID} verifica se já existe na sua base de dados o objeto licença DID_L correspondente;

(a) Se existir um objeto licença para esse utilizador e conteúdo, LIS cria um URI temporário do objeto licença para que o utilizador, via "Agente DRM", possa realizar o seu descarregamento (Figura 71). Depois de armazenar o objeto no dispositivo, o utilizador, para usar o conteúdo, pode realizar a mesma sequência de passos como anteriormente para um objeto licença armazenado no dispositivo;

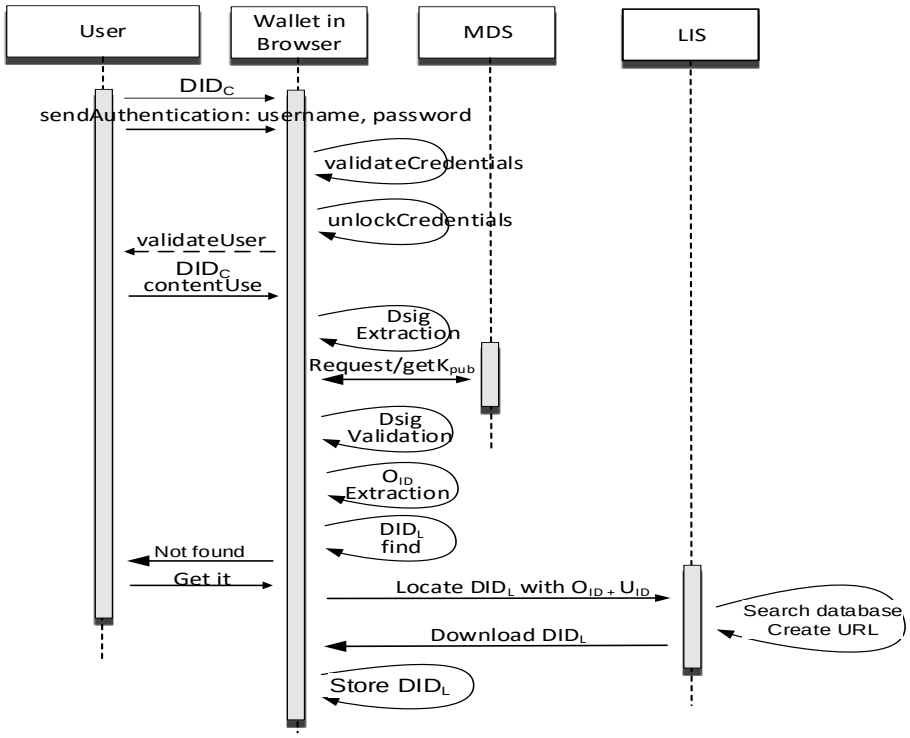


Figura 71 – Obtenção de conteúdo e do objeto licença armazenado em LIS.

(b) Se não existir o objeto licença para esse utilizador e conteúdo, o LIS comunica ao *Wallet* que não o consegue localizar, sendo proposta ao utilizador a criação de um novo objeto. Se o utilizador aceitar, o *Wallet* comunica ao LIS para dar início ao processo de emissão da licença (Figura 72):

- Uma licença padrão de distribuição correspondente ao objeto conteúdo O_{ID} é apresentada ao utilizador final através de um formulário, e o utilizador pode selecionar as condições mais apropriadas ao seu caso. Normalmente, a licença padrão é composta pelos seguintes elementos:
  - Identificação do utilizador (U_{ID}), utilizadores múltiplos (U_{ID1}…U_{IDn}) ou grupos (G_{ID}). A representação de pessoas/utilizadores com quem se pretende partilhar o conteúdo é aqui representada, podendo este ser partilhado com um utilizador

simples e específico, com vários utilizadores ou com um grupo previamente estabelecido pelo autor/detentor do conteúdo;

- Identificador único do conteúdo (C_{ID}). Representa o Identificador único do conteúdo que o vai permitir localizar;
- Tipo de direitos a exercer e condições em que pode ser exercido. Este elemento pode definir as operações (por exemplo, *play*, *print*,…) sobre o conteúdo e quais as condições (por exemplo: número de vezes);
- Validade. Define o período de tempo durante o qual a licença é válida.

- O utilizador seleciona os parâmetros apropriados que são enviados ao LIS conjuntamente com o $O_{ID,}$ $C_{ID\ e}$ U_{ID}. O LIS execut um variado conjunto de mecanismos de validação que passam pela verificação da elegibilidade do utilizador e do pedido realizado perante o SGA (ver Capítulo 9) ativando o módulo ILM.
- Caso todas as validações sejam positivas, o LIS gera a licença para o U_{ID}. Procede então ao registo da licença perante o RGS, assina-a digitalmente e armazena-a;
- De seguida, o módulo ILM procede à criação do documento DID_L correspondente ao conteúdo. Este módulo, além de permitir incorporar os elementos identificados na estrutura do objeto, vai também permitir encriptar a cifra que protege o conteúdo, $S_{K,}$ com as ferramentas de proteção IPMP e incorporá-la no objeto licença. Para tal, procede da seguinte forma:
  a. LIS localiza na sua base de dados a cifra de proteção do conteúdo S_K correspondente ao C_{ID} aí armazenado no decorrer da proteção do conteúdo;
  b. LIS contacta o PTS para obter a ferramenta de proteção adequada (RSA Tool) e encripta a cifra de proteção com a chave pública do utilizador $E_{RSA}(S_{K,}\ K_{pub}U)$;
  c. Com a informação obtida, metadados, C_{ID}, O_{ID}, chaves do utilizador, licença gerada e a cifra de proteção encriptada, o módulo ILM procede à criação do objeto licença. Para tal contacta o RGS enviando o O_{ID} do objeto conteúdo associando-o e procede ao registo obtendo um número de identificação único. Com o registo do objeto licença associado ao objeto conteúdo, incorpora toda a informação no objeto de acordo com a estrutura DID_L definida anteriormente (Capítulo 7), gravando o novo objeto na sua base de dados. No final, o objeto é assinado digitalmente pelo LIS.

- Estando o objeto licença criado, o LIS cria um URI temporário e disponibiliza-o para que o utilizador proceda ao descarregamento do objeto DID_L. Depois de armazenar o objeto no dispositivo, o utilizador, para usar o conteúdo, pode realizar a mesma sequência de passos como anteriormente para um objeto licença armazenado na "Agente DRM" do dispositivo;

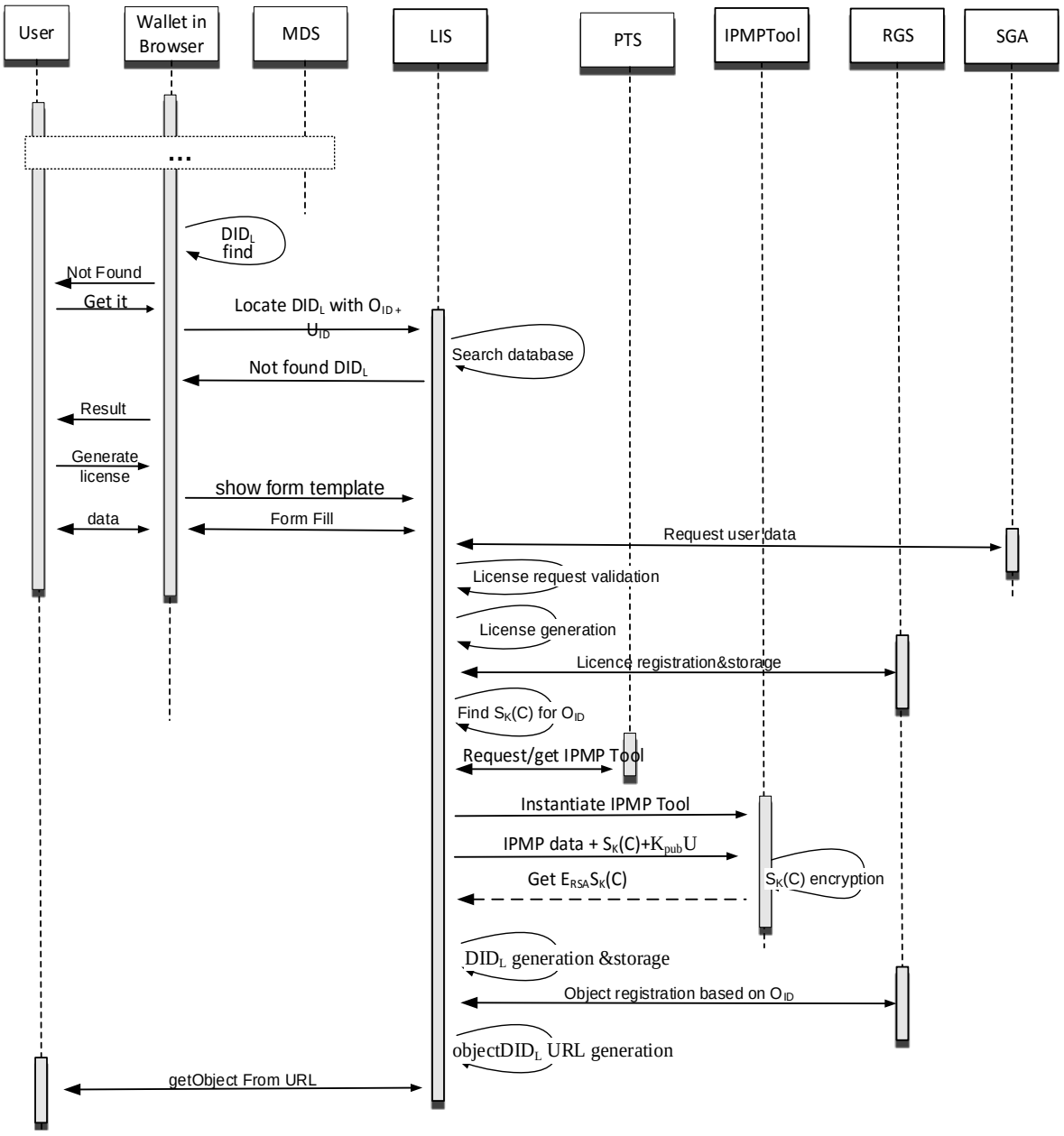


Figura 72 – Criação do objeto licença

5. Ferramentas de suporte MPEG-21 no ARMS

No decurso da preparação do conteúdo para utilização e ao transmitir direitos a terceiros, o utilizador, ao ficar na posse quer do objeto conteúdo quer do objeto licença, leva a que o ARMS recorra a três tipos distintos de ferramentas que dão o suporte ao transporte, proteção e governo

do conteúdo. Estas ferramentas são implementadas sob a forma de módulos quer no CPS quer no LIS e permitem a comunicação com o SGA com vista à realização da proteção de conteúdos e validação das licenças.

Ferramentas de transporte – permitem embeber o recurso num objeto digital (DID_C e/ou DID_L) de acordo com as especificações MPEG-21 IPMP. O ARMS permite que este tipo de ferramentas possa inserir o recurso ou a informação relacionada com direitos de PI embebendo-os num objeto digital transmissível. O ARMS possui dois módulos, a que se deu o nome de Ingestion Module (IM) e o Issuer License Module (ILM). Um foi implementado no CPS e outro no LIS e permitem a geração de documentos DID_C e DID_L, respetivamente, de acordo com a estrutura pré-definida no capítulo 7 e seguindo a especificação MPEG-21 IPMP. Cada um destes objetos é assinado digitalmente e validado de acordo com o MPEG-21 *schema*. Estes módulos são os responsáveis pela geração de objetos digitais de acordo com a estrutura DID_C e DID_L predefinida (Capítulo 7) e ativam sempre que necessário mecanismos de validação que verificam a elegibilidade do utilizador perante os dados do seu perfil existentes no SGA.

Ferramentas de proteção - permitem proteger/desproteger quer o conteúdo quer a cifra que protege o conteúdo. O ARMS permite que estas ferramentas possam ser obtidas a partir de um componente externo. O PTS no ARMS é o componente que estabelece contacto externo e disponibiliza a ferramenta aos outros componentes internos do ARMS que fazem aplicar as funcionalidades de proteção sobre o recurso em causa (sobre o conteúdo – via CPS; sobre a cifra que protege o conteúdo - via LIS). Uma das ferramentas utilizadas permite encriptar/desencriptar o conteúdo com um algoritmo de chave simétrica (AES). A outra ferramenta permite encriptar/desencriptar a cifra que protege o conteúdo com um algoritmo de chave assimétrica (RSA).

Ferramentas de governo – permitem controlar o uso do conteúdo sob condições específicas. A validação da licença quando gerada é um processo complexo existindo uma forte interação com o utilizador em que intervém o LIS (do lado servidor) e o "Agente DRM" (do lado cliente) do ARMS. No decorrer deste processo, o ILM é o módulo principal que faz chamadas a sub-módulos em que tomam parte não só os geradores da licença, os validadores de licença, mas também ferramentas de autorização.

- *Gerador de licença* - esta ferramenta, implementada como uma aplicação *Web*, é constituída por um formulário onde o utilizador procede à introdução de dados, por *scripts* de processamento e por ficheiros auxiliares de validação que formatam e processam a informação. Os dados introduzidos permitem que os principais elementos constituintes

de uma licença MPEG-21 ("*principal"*, "*resource"*, "*right"*, "*conditions"* e "*issuer"*) sejam gerados na licença em conformidadethe com os dados introduzidos. Quando a informação é enviada, esta é validada sendo gerado um ficheiro temporário no formato XML contendo a licença de acordo com o *schema* MPEG-21. Esta licença, depois de validada, fica então pronta para ser incorporada no objeto DID_L de acordo com a estrutura definida.

- *Validador da licença* – esta ferramenta efetua a validação da licença de distribuição (Capítulo 9 e 10) e de seguida usando como entrada a licença temporária gerada e através da aplicação do mecanismo de validação da distribuição adequado (ver os capítulos 9 e 10) procede à comparação dos elementos relacionados da licença progenitora e da temporária, através do módulo de validação das regras MPEG-21 REL. Se a validação falhar, o utilizador será avisado, mas, caso seja bem sucedida, dá início à criação de uma licença a ser incorporada no objeto digital. Para tal, faz recurso de três sub-módulos interrelacionados:
  - *Módulo de validação das regras MPEG-21 REL*: verifica se a licença está em conformidade sintática com as regras da especificação MPEG-21 REL e se passa todos os passos correspondentes às fases de validação da licença (Capítulo 9 e 10);
  - *Módulo de validação de conformidade MPEG-21 REL schema*: verifica se a licença está em conformidade com os *schemas* XML correspondentes ativando um interpretador que realiza pesquisas sobre a licença;
  - *Módulo de autorização MPEG-21 REL*: verifica se o pedido de emissão de licença é legítimo, contactando, sempre que necessário, o SGA para comprovar a elegibilidade do pedido de emissão para o utilizador em causa e para o tipo de licença pretendido. Caso tenha sucesso, procede à extração dos variados elementos para processamento nos módulos que o requeiram.

Para que o utilizador final possa aceder ao conteúdo torna-se necessária a implementação de ferramentas que efetuem a validação e extração de informação dos itens digitais (ID) gerados de acordo com a especificação MPEG-21 IPMP. No ARMS estas ferramentas residem na componente "Aplicação/Agente DRM", a qual está desenhada para efetuar a gestão dos elementos IPMP DID de modo a que o utilizador seja autorizado a aceder e usar um conteúdo de forma controlada. Estando os objetos conteúdo e licença armazenados no dispositivo cliente, torna-se necessário comprovar a autenticidade e integridade dos objetos digitais. Para tal, um módulo específico valida as assinaturas digitais embebidas nos objetos (validador Dsig) e, de

seguida, um interpretador genérico capaz de obter a informação dos objetos é ativado (interpretador IPMP DID) e a partir dos elementos adequados apresenta ao utilizador a informação básica sobre o conteúdo e direitos associados. Perante a escolha do utilizador, o "Aplicação/Agente DRM" procede à obtenção da cifra que lhe permite aceder ao conteúdo. Para tal, necessita de um conjunto de ferramentas adicionais que lhe permitem obter a necessária autorização para poder desencriptar o conteúdo protegido que está embebido no objeto conteúdo. Essas ferramentas residentes na "Aplicação/Agente DRM" são as seguintes:

- *Interpretador de expressões MPEG-21 "IPMP:info"* – esta ferramenta interpreta e valida um conjunto de informação "IPMP:info" inserida nos objetos digitais relativamente à conformidade com os XML *schemas* aí especificados. Pode também verificar se a chave privada do utilizador U corresponde à chave pública que está a encriptar a chave de proteção.
- *O validador REL e autorizador* – esta ferramenta permite não só verificar a conformidade da licença com o *schema* REL MPEG21 mas também a sua validade. Além disso, permite verificar se o utilizador é autêntico, verificando se a licença lhe está atribuída através da correspondência com a chave privada do utilizador (K_{priv}^{U}) armazenada no dispositivo.
- *Extrator de informação MPEG-21 IPMP* – esta ferramenta obtém a informação associada à proteção de um documento DID ou partes dele. Em primeiro lugar, o elemento que está dentro do documento DID é identificado. De seguida, é obtida e apresentada a informação relevante relacionada com as ferramentas IPMP envolvidas para os respetivos objetos digitais, quer na proteção do conteúdo quer na cifra que protege o conteúdo, assim como dos restantes metadados e informação de direitos relacionados com o objeto. Os elementos "ipmpdidl:Info", "ipmpdidl:Contents" e "ipmpdidl:Identifier" de "ipmpdidl:Resource" são extraídos para serem processados posteriormente.
- *Extrator da licença MPEG-21 IPMP* – esta ferramenta obtém do documento DID_L a licença associada com o documento DID_C, ou parte deste, identificando-a com o elemento protegido. A licença que governa o uso do conteúdo é assim obtida.

Para que o utilizador possa usar um conteúdo necessita de ter uma autorização. A autorização dada, depois das várias validações efetuadas, corresponde à permissão para que o utilizador possa usar a ferramenta de proteção. Essa autorização é obtida antes da ferramenta IPMP iniciar o processamento no objeto conteúdo. Para tal, obtém-se a chave encriptada que protege o conteúdo do objeto licença relacionado. Na posse da ferramenta que desencripta a chave de proteção de conteúdo, o utilizador passa a ter a autorização para desencriptar e aceder ao

conteúdo de acordo com os termos e condições especificados através da linguagem de direitos expressa na licença. Ou seja, para desproteger e aceder ao conteúdo é necessária uma autorização que se manifesta pela posse da chave que protege a chave de proteção de conteúdo, chave essa que permite obter a ferramenta que autoriza a desencriptação do conteúdo. Essa chave corresponde à chave privada do utilizador (K_{priv}^{U}) que possui o objeto conteúdo e o respetivo objeto licença. Se houver correspondência entre a chave privada armazenada no "Aplicação/Agente DRM" do dispositivo cliente ARMS e a chave pública que protege a cifra de proteção do conteúdo, o utilizador passa a ter autorização para utilizar a ferramenta depois de ter sido confirmado que a licença também lhe está atribuída. A relação entre estas ferramentas no decorrer da obtenção da ferramenta IPMP do PTS é ilustrada na Figura 73.

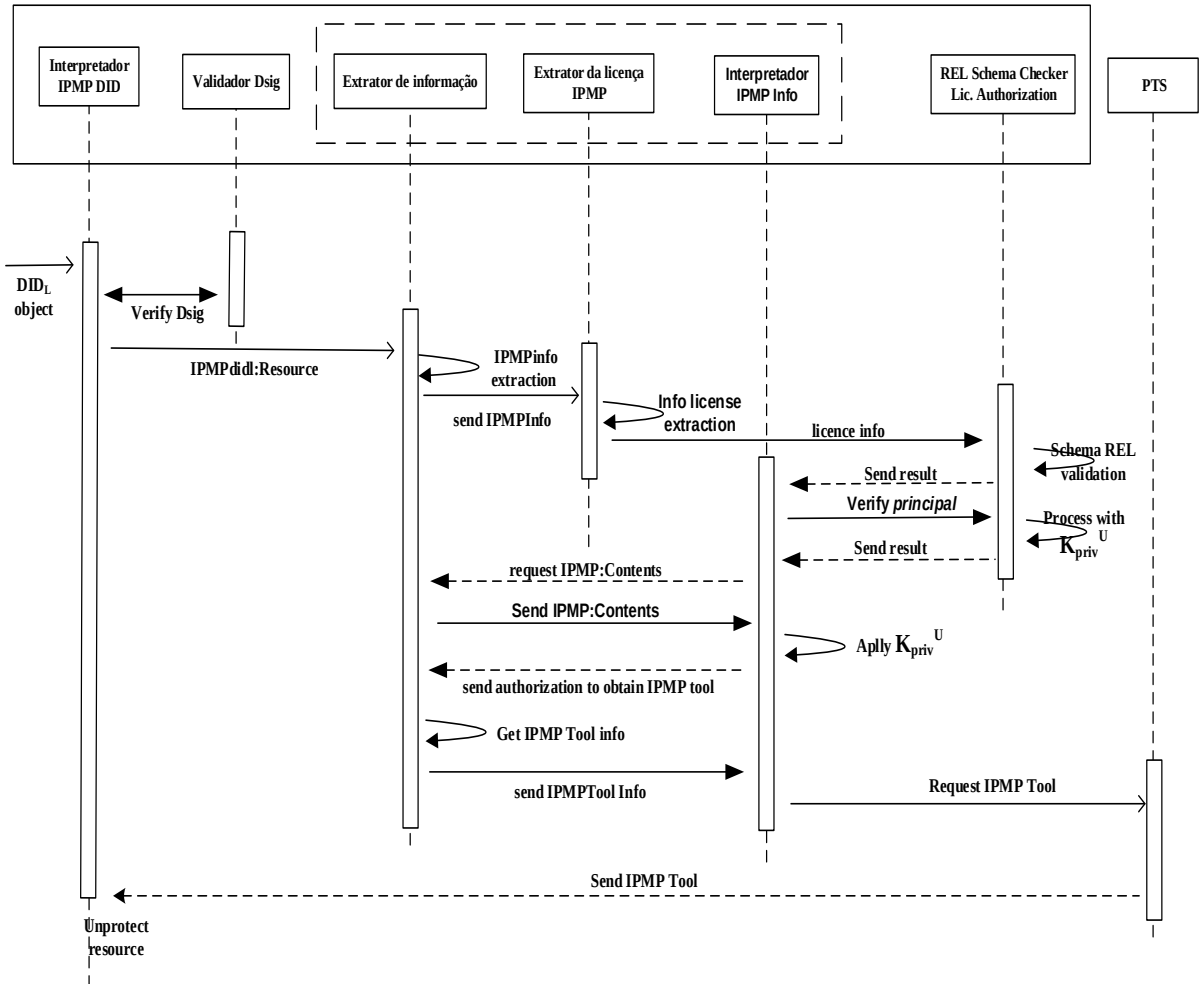


Figura 73 – Interações para autorizar a obtenção da ferramenta IPMP

Estando o utilizador na posse desta ferramenta IPMP, está autorizado a prosseguir com a desencriptação do conteúdo. Depois de o conteúdo estar desprotegido, cabe ao "Aplicação/Agente DRM" fazer vigorar a aplicação dos direitos expressos na respetiva licença.

6. Conclusão

Ao implementar os conceitos inerentes à norma MPEG-21 e indo ao encontro dos principais requisitos dos intervenientes no processo de partilha do conteúdo, o ARMS oferece uma forma de distribuição de conteúdo conveniente, governável e segura aos detentores de direitos. Essa conveniência, aliada à flexibilidade e melhoria da confiança estabelecida entre as partes, vai de encontro à real necessidade dos autores/detentores de conteúdo no respeitante à preservação da integridade do conteúdo e do direito de atribuição, típica do contexto académico. O ARMS, estando orientado para o contexto académico, permite que uma solução de gestão e proteção de conteúdos possa ser implementada tendo em conta a preservação de direitos de PI ao longo do ciclo de vida do conteúdo. Ao recorrer à norma MPEG-21, permite responder aos requisitos específicos de um tipo particular de utilização onde os detentores de conteúdo podem escolher entre dois possíveis cenários: a forma livre e a forma protegida. Deixando a escolha da proteção a aplicar ao cuidado do detentor de conteúdo, o ARMS permite que a partilha desse conteúdo se efetue de uma forma descentralizada e interoperável, pois ao recorrer às normas internacionais como forma de transporte do conteúdo, protegido ou não, vem não só garantir a sua transmissibilidade de forma inócua, como também formas de proteção seguras e sustentadas em padrões aceites pela comunidade.

A simplificação introduzida pela integração com o SGA e com a introdução dos conceitos inerentes ao MPEG-21, faz com que o ARMS, ao não requerer métodos específicos de transmissão ou modificações no sistema operativo, possa ser usado no contexto académico indo ao encontro das necessidades básicas de proteção sentidas pelos participantes neste meio.

Com base no trabalho aqui descrito foi produzida a comunicação científica em Marques & Serrão, (2014).

PARTE IV

Transmissão de direitos e mecanismos de controlo

Capítulo 9

MPEG-21 e transmissão de direitos no contexto educacional e académico

Resumo

Ao longo deste capítulo iremos apresentar uma contribuição em relação à transmissão de direitos, e licenciamento e da importância da utilização de um mecanismo que permite a validação da sua emissão mantendo a linha sucessória. A questão da elegibilidade dos utilizadores e o papel preponderante dos sistemas de gestão académica perante a solicitação de emissão de licenças também são abordados. Além disso, é igualmente analisado o suporte oferecido pela norma internacional MPEG-21 REL no processo de transmissão de direitos, mais propriamente na sua concessão entre os variados tipos de participantes tendo em conta o privilégio para emissão de licenças (PEL) e de como se adaptam ao contexto educacional e académico. Por fim, são propostos mecanismos de validação de emissão de licença e apresentam-se diversos casos de uso, comuns à utilização de conteúdos no contexto académico e respetiva transmissão de direitos. Este acaba por ser o contributo principal deste capítulo tendo em vista a preservação e respeito pelos direitos concedidos e transmitidos ao longo da cadeia sucessória especificamente para o contexto académico.

1 Introdução

A proteção de conteúdos num sistema DRM envolve necessariamente três elementos do ciclo de vida do conteúdo: o criador, o fornecedor/distribuidor e o utilizador final (Sachan et al., 2010). O criador é o autor do conteúdo ou o agregador de vários conteúdos num pacote. Este normalmente é o dono original do conteúdo sendo, por isso, o detentor dos direitos, concedendo direitos de redistribuição aos seus distribuidores. O fornecedor/distribuidor possui a responsabilidade de trocar ou enviar o conteúdo gerindo a respetiva transação. Dependendo das suas atribuições pode haver mais que um distribuidor desde que os mesmos estejam autorizados a (re)transmitir os direitos que lhes foram concedidos. Esta transmissão de direitos pode ser para outros distribuidores, mas também para os utilizadores finais (Sachan et al., 2010). Normalmente, e num sistema automatizado, o distribuidor de linças é o Servidor de Licenças (LIS) a quem foi atribuído o direito de emitir licenças ao utilizador final de acordo com as

regras de utilização especificadas. O utilizador final é aquele que utiliza os conteúdos de acordo com os direitos transmitidos pelo distribuidor. Contudo, este utilizador pode não ser o último da cadeia, já que pode partilhar os conteúdos com outros utilizadores até que as restrições de direitos especifiquem o fim dos direitos ou a licença de utilização caduque.

Do ponto de vista do licenciamento, podemos assim ter vários tipos de distribuição de licença para o utilizador final:

- Distribuição simples, em que a licença é obtida diretamente do servidor de licenças pelo utilizador que procede ao uso do conteúdo de acordo com os termos especificados na licença não podendo transmiti-la a terceiros;
- Distribuição de grupo, em que a licença é obtida por um distribuidor a partir de outro distribuidor autorizado a emitir licenças;
- Distribuição delegada, em que a licença é obtida de um emissor que emite uma licença onde delega direitos de emissão de licenças a terceiros.

Assim, ao partilhar conteúdos, há a considerar ao longo do ciclo de vida do conteúdo a transmissão de direitos entre criador e distribuidor, entre distribuidores, entre o distribuidor e o utilizador, e também entre utilizadores (Figura 74).

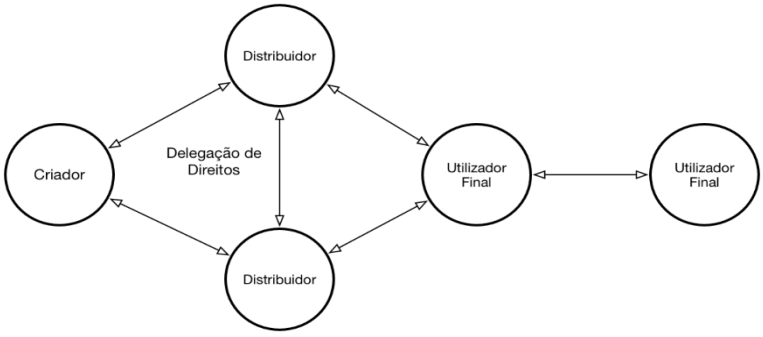


Figura 74 - Transmissão de direitos e ciclo de vida do conteúdo

No decorrer desta transmissão, podemos considerar os seguintes tipos de licenciamento consoante a forma como os direitos podem ser transmitidos entre emissor e recetor:

- Licenciamento de distribuição: o emissor concede ao recetor a capacidade de o mesmo transmitir os seus direitos a terceiros, que os podem usufruir ou delegar a outros;
- Licenciamento de utilização: o recetor tem direito de usufruir dos direitos emitidos pelo distribuidor e, se for caso disso, de os retransmitir a outros utilizadores.

Os diferentes tipos de licenciamento acabam igualmente por definir o tipo de licenças utilizadas ao longo da cadeia de proteção: licenças de (re)distribuição e licenças de utilização (Sachan et al., 2010). De referir que em todos os tipos de licenças existe sempre a possibilidade da delegação de direitos transmitidos a terceiros de forma controlada de modo a não ultrapassar os direitos originais, o que torna possível viabilizar o modelo de superdistribuição. Contudo, para usufruir desses direitos, qualquer interveniente do ciclo de vida do conteúdo terá sempre de possuir direitos expressos numa licença, inclusive o direito de delegação, o que vem de encontro ao princípio básico de DRM previamente enunciado no Capítulo 2.

Essas licenças recorrem a uma linguagem de expressão de direitos (REL), capaz de definir duas vertentes na sua estrutura: uma define os papeis e direitos concessionados através da definição de atores, direitos, recursos e condições (em MPEG-21 temos as designações de "<*principal*>, <*rights*>, <*resources*>, <*conditions*>"). A outra permite verificar se a concessão de direitos a terceiros é realizada de forma correta.

Em grande parte dos casos, pode tornar-se vantajoso para o detentor de conteúdos, em vez de gerir os seus direitos diretamente com os utilizadores finais, delegar essa tarefa a terceiros, como o distribuidor de licenças (que até pode atuar em simultâneo como fornecedor de conteúdos), ficando liberto de lidar com as questões de distribuição, não só do conteúdo em si, mas também das licenças. Esta delegação não pode ser feita sem qualquer controlo de cada um dos intervenientes na cadeia de distribuição, pois o detentor pretende controlar a forma como o conteúdo é utilizado mesmo quando autoriza terceiros a emitirem licenças aos utilizadores finais. Assim, o problema da partilha de conteúdos passa não só por uma correta proteção desses mesmos conteúdos, mas também pela aplicação de um processo de concessão de direitos eficaz, enquadrado pelo modelo de negócio específico ao contexto em que se insere a transmissão do conteúdo e dos direitos associados. No caso específico do meio académico, muitas vezes é do interesse do detentor de direitos original manter o controlo sobre a distribuição dos direitos que atribuiu a outros.

Os sistemas comerciais atuais de DRM especificam a presença de distribuidores entre o criador e os consumidores. Contudo, estes sistemas criam um problema no controlo de direitos, pois, sendo o conteúdo distribuído pelo distribuidor, o criador deixa de ter controlo sobre a distribuição, não podendo ter certeza de que os seus direitos são aplicados (Hwang, S., 2008; Li, Zhao, Wang & Ma, 2010). Podendo o distribuidor distribuir o conteúdo numa forma que viole o acordado com o criador torna-se, por isso, importante gerir os direitos sempre que o distribuidor não seja de confiança (Sachan & Kankanhalli, 2012). Para que a transmissão de

direitos se processe de acordo com os termos definidos inicialmente pelo detentor de direitos, a proteção de conteúdo e direitos associados só faz sentido quando tomada no seu todo, ou seja, não podem existir falhas de sequência na transmissão de direitos ao longo do ciclo de vida do conteúdo. Assim, um distribuidor só poderá transmitir direitos desde que não viole os direitos inicialmente estabelecidos pelo criador. Para tal, é essencial garantir que qualquer um dos intervenientes não possa modificar e/ou emitir uma licença forjada válida para determinado conteúdo.

Apesar de a literatura mencionar vários trabalhos na área da distribuição de conteúdos na presença de distribuidores de não confiança (Sans et. al., 2007; Li et al.,2010), é de referir que nestes trabalhos é permitido ao criador e ao distribuidor associar as suas próprias regras na utilização do conteúdo, mas o consumidor necessita de obter licenças de ambos. O conteúdo é usado de acordo com as regras comuns a todas as licenças não podendo estas serem retransmitidas (cenário de distribuição simples), o que levanta sérios problemas de flexibilidade em termos práticos, pois os distribuidores necessitam de agregar múltiplas licenças de redistribuição para cada conteúdo (Sachan E., 2009) assim como restrições agregadas nas licenças de redistribuição. Por isso mesmo torna-se necessário simplificar todo este processo de gestão de direitos de distribuição realizando uma validação prévia da licença a emitir de acordo com os direitos definidos pelo criador e de acordo com o perfil do utilizador no meio académico. Para o nosso propósito utilizaremos a norma MPEG-21 REL, e os seus elementos associados ao privilégio de redistribuição de licença integrados no sistema ARMS orientado para o contexto académico não comercial.

2 Controlo sobre a utilização do conteúdo

A partilha de conteúdos e direitos associados passa não só por uma correta proteção desses mesmos conteúdos, mas também pela aplicação de processos em que as regras de concessão de direitos sejam corretamente definidas e enquadradas no modelo de negócio específico ao domínio de aplicação em causa (Sans et al., 2007). Normalmente, em qualquer sistema de DRM, a utilização de conteúdos pode ser controlada no ponto de consumo, ou seja, pelo cliente DRM. No caso de um sistema de DRM que utilize uma licença típica (recorrendo, por exemplo, ao MPEG-21 REL), a sua interpretação irá viabilizar e regular (governar) as ações que condicionam a utilização desses mesmos conteúdos. Normalmente, esta licença será interpretada pela aplicação cliente residente no dispositivo do utilizador, que fará o controlo dos utilizadores (e dos dispositivos) a quem a licença foi emitida, assegurando o controlo do

modo de atuação sobre o conteúdo consoante as regras expressas na licença (Petkovic, & Jonker, 2007). Obviamente que nesta situação, o sistema de DRM terá de comprovar se o utilizador (ou dispositivo) diz ser quem realmente é e se possui os atributos exigidos. Por exemplo, no caso de um professor que queira distribuir um trabalho para uma determinada unidade curricular de forma protegida, além de este ter de estar registado no sistema DRM, terá de haver mecanismo(s) que, mediante interação com o sistema de gestão académica (SGA) da instituição, comprove(m) que ele é de facto professor dessa unidade curricular. Esse(s) mecanismo(s) pode(m) assim assegurar se o emissor está credenciado para emitir uma licença com certas condições e garantir que quem pede a emissão da licença é elegível perante as condições do emissor. Ou seja, com esse(s) mecanismo(s) acaba-se por fazer com que o emissor de licenças atue como um controlador de domínio validando a emissão de licenças, neste caso para intervenientes do meio académico e académico, graças à interação com o SGA obtendo previamente dados do utilizador. Assim, o detentor de direitos é capaz de determinar exatamente quais os utilizadores membros desse domínio que podem receber a licença e, assim, ter um total controlo sobre a cadeia sucessória de direitos ao longo do ciclo de vida do conteúdo.

2.1 As licenças e o controlo sobre o uso de conteúdo

Ao lidar com licenças ou com os objetos digitais que as contêm, devemos considerar dois processos de topo: a criação e a utilização da licença. O primeiro processo envolve a enumeração e especificação das condições a serem aplicadas no decorrer da utilização do conteúdo, assim como da informação e mecanismos necessários (por exemplo, uma chave criptográfica) para que o conteúdo possa ser desprotegido e acedido. A complexidade deste processo vai depender do modelo de negócio aplicado e de os direitos poderem ou não ser delegados a terceiros (utilizadores ou distribuidores). O segundo processo envolve a utilização e a garantia de que os direitos estabelecidos na licença estão a ser cumpridos. É por isso importante especificar os mecanismos usados pelos sistemas de DRM com vista a assegurar que o conteúdo sob governo da plataforma DRM é usado e distribuído através da cadeia de valor digital de acordo com os direitos declarados pelo criador (Rodriguez & Delgado, 2007a).

No decorrer da preparação do conteúdo, as regras de distribuição desse conteúdo são definidas através da licença de distribuição que, por sua vez, vai determinar o tipo de condições sob as quais as licenças de utilização podem ser emitidas. Uma licença de distribuição pode requerer que o emissor dessa licença possua um determinado atributo (como, por exemplo, ser um docente da instituição registado no sistema de autenticação dessa mesma instituição como docente de determinadas disciplinas) com vista a possuir um determinado previlégio. Por sua

vez, as licenças de utilização também podem requerer que o recetor possua um determinado atributo (por exemplo, que o aluno esteja registado no corrente ano letivo no ciclo de estudos e na unidade curricular da instituição).

No decorrer da emissão das licenças de utilização, um servidor de licenças irá interpretar as condições expressas na licença de distribuição e verificar a sua aplicabilidade perante os atributos de quem faz o pedido de emissão. Assim, torna-se necessário que exista a validação da elegibilidade não só dos autores de conteúdo que fazem o seu carregamento, verificando se estes são realmente quem afirmam ser, confirmando-o perante o sistema de gestão académica (SGA), mas também dos utilizadores finais. Deste modo, por exemplo, um professor registado no sistema DRM poderá criar a licença modelo (*license template*[13]) contendo os direitos e metadados correspondentes a um determinado conteúdo para a instituição, unidade curricular e ano letivo desde que seja elegível perante o SGA. Por outro lado, um aluno, ao solicitar uma licença de uso de um determinado conteúdo leva a que o sistema de DRM, antes de emitir a licença, verifique a sua elegibilidade também perante o SGA, (verificando se existe e se está enquadrado pelas condições expressas na licença modelo previamente criada pelo professor).

Independentemente da elegibilidade inicial ou não do aluno no domínio da instituição, também é necessário verificar a sua elegibilidade perante as condições expressas na licença de distribuição progenitora, e só depois a licença final de utilização poderá ser emitida. A Figura 75 ilustra este processo sendo aqui de realçar a presença dos tipos de licenciamentos anteriormente assinalados.

[13] De um modo geral, uma *license template* é um modelo ou padrão usado para criar múltiplas cópias de um objeto licença.

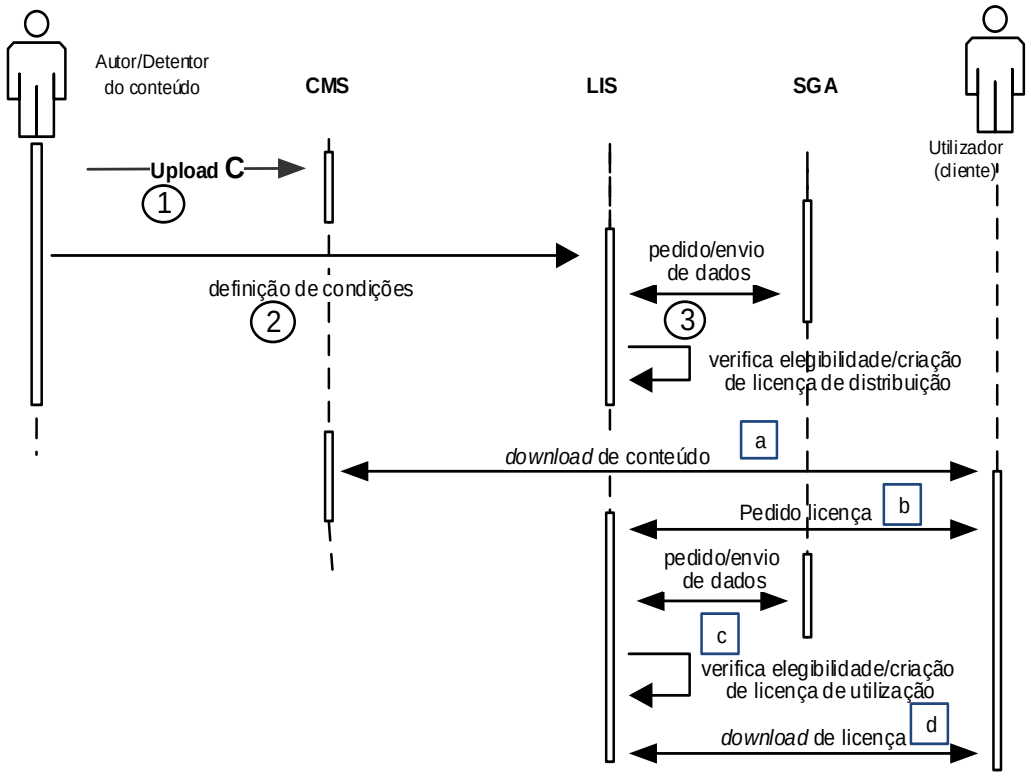


Figura 75 - *Upload* de conteúdos e geração de licenças no contexto académico

1 – O criador faz o carregamento do conteúdo no CMS;

2 – O criador define as condições de distribuição em LIS;

3 - O LS pede dados do criador ao SGA e verifica a sua eligibilidade executando ou não a criação da respetiva licença de distribuição. Para tal são executados os seguintes passos:

a – O utilizador obtém o conteúdo (caso não o possua);

b – O utilizador pede ao LS para emitir a licença para esse conteúdo;

c - O LS pede dados do utilizador ao SGA e verifica a sua eligibilidade autorizando ou não a criar a respetiva licença;

d – O utilizador obtém a respetiva licença de utilização.

2.2 Ciclo de vida do conteúdo e licenciamento

No decorrer do ciclo de vida do conteúdo há a considerar a existência de direitos associados ao conteúdo desde a sua criação até ao seu consumo, passando pela distribuição. No decorrer do consumo de conteúdo, a aplicação cliente do sistema *DRM* requer a presença de uma licença que especifique os direitos que foram atribuídos e as condições sobre as quais os direitos podem ser exercidos. Esta licença, normalmente, é enviada à aplicação cliente de forma separada do

conteúdo protegido num objeto digital (Figura 75), mas também pode estar embebida com o próprio conteúdo num único objeto digital específico que os junta (Figura 76).

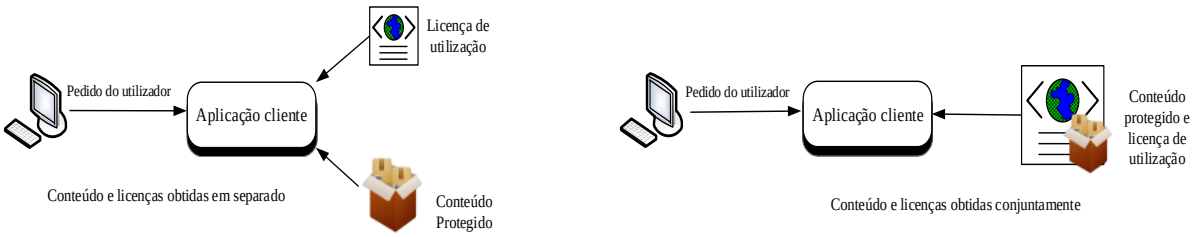


Figura 76 – Consumo de conteúdo e utilização governada por licença

Durante a distribuição do conteúdo as licenças são emitidas para os utilizadores finais a pedido do utilizador através da aplicação cliente. Para que haja um maior controlo das diferentes particularidades dos direitos que podem ser atribuídos a estes utilizadores consoante as condições pretendidas por cada um, é aqui utilizada uma licença especial que viabiliza a criação de licenças: licenças modelo. Estas são utilizadas, para especificar as condições genéricas padrão que o utilizador final poderá selecionar e negociar com o Servidor de Licenças (LIS). Esta licença modelo permite que várias cópias dessa licença sejam instanciadas e emitidas, especificando diferentes direitos consoante o desejo de cada utilizador, mas sempre enquadrados pelos direitos especificados na licença modelo. O esquema DRM deverá, assim, ser suficientemente adaptativo, de forma a enquadrar-se com as necessidades de direitos do utilizador final, de modo a que diferentes licenças de utilização possam ser criadas consoante os diferentes tipos de conteúdos e de utilizadores. No decorrer da interação do utilizador com a plataforma de DRM um destes tipos de licenças é selecionado permitindo, assim, gerar a licença específica para o utilizador final (Figura 77).

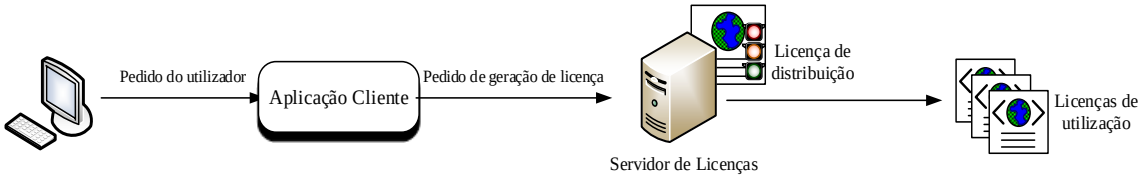


Figura 77 – Licença de distribuição e criação de licenças de utilização

Durante a fase de preparação de conteúdo no sistema de DRM, o autor/detentor do conteúdo pode especificar as condições em que as licenças de utilização podem ser geradas para o utilizador final através da licença de distribuição. Tais condições são expressas na licença de distribuição que se irão apresentar sob a forma de uma licença modelo. É nessa licença modelo que estão especificadas as regras sob as quais as licenças de utilização poderão ser geradas (Figura 78**)**. De um modo geral, uma licença modelo representa uma oferta de distribuição

padrão, definindo o produto e seus termos de utilização para uso tipificado (por exemplo, uma licença de previsualização por 20 segundos válida num espaço de tempo ou então uma licença específica para um tipo específico de utilizador).

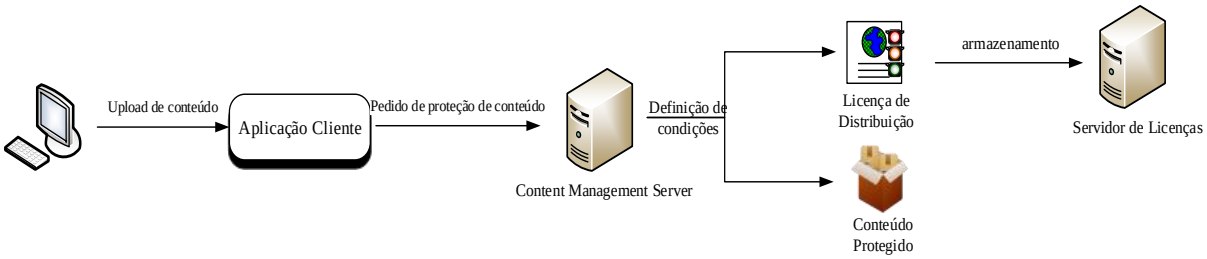


Figura 78 - Proteção de conteúdos e geração da licença de distribuição

Utilizando esta abordagem, um fornecedor de conteúdos pode assim definir o seu modelo de negócio e, utilizando as ferramentas adequadas, pode definir facilmente quais as condições sob as quais o seu conteúdo digital pode ser negociado. Assim, o fornecedor de conteúdos deixa de se preocupar com decisões técnicas no que respeita à seleção dos mecanismos e ferramentas de proteção de conteúdos, podendo focar-se no seu negócio. Uma vez que a licença modelo pode ser representada através de uma forma ou linguagem que permita a expressão de direitos, podem definir-se quantas licenças modelo que se desejem. O número e a complexidade de tais licenças modelo depende, obviamente, da complexidade do modelo de negócio. Se o modelo de negócio adotado for simples, é de esperar que a licença modelo seja igualmente simples.

A definição das licenças modelo e das licenças de utilização resulta das interações entre o fornecedor de conteúdo, o fornecedor da licença e o(s) utilizador(es). O fornecedor de conteúdos, após estabelecer uma ligação contratual com um fornecedor de licenças, usa uma ferramenta deste para estabelecer o seu modelo de negócio associando um tipo específico de conteúdo. Esta ferramenta permite-lhe estabelecer os termos gerais de uso de um certo conteúdo sobre os quais recaem direitos. Este processo de definição ocorre através dos seguintes passos:

- O fornecedor de conteúdo seleciona as variadas condições de negociação e respetivos direitos a partir das licenças modelo existentes;
- Baseado nas escolhas realizadas pelo fornecedor de conteúdo, o fornecedor de licenças cria uma licença modelo usando a REL (ou RELs diferentes) por ele suportada. Este processo cria um meta modelo de licença de direitos, contendo um conjunto de parâmetros variáveis que serão usados para criar instâncias da licença final obedecendo ao formato REL suportado. Estas licenças modelo são armazenadas no fornecedor de licenças e associadas a um determinado fornecedor e tipo de conteúdo;

- Quando o utilizador obtém o conteúdo, a licença modelo associada é apresentada ao utilizador através do fornecedor de licenças, podendo então o utilizador escolher/negociar as condições de utilização. Estas condições podem ser (ou não ser) negociáveis para o utilizador final e, dependendo da situação, o SL apresentará maior ou menor interatividade na escolha a efetuar pelo utilizador. Em alguns casos, os termos e condições são somente apresentados ao utilizador dependendo deste a aceitação;
- Baseado nas seleções realizadas pelo utilizador e nas instruções prévias do fornecedor de conteúdos espelhadas na licença modelo, dá-se início à sua instanciação, sendo produzida uma nova licença, caso o utilizador seja elegível para usar o conteúdo;
- Finalmente, o utilizador final descarrega a licença no formato apropriado suportado pelo dispositivo que contém a aplicação cliente DRM.

Com um grau de detalhe mais pormenorizado o processo de definição das licenças modelo pode ser ilustrado pela Figura 79 (Kamperman et al., 2007) tendo em conta os seguintes passos:

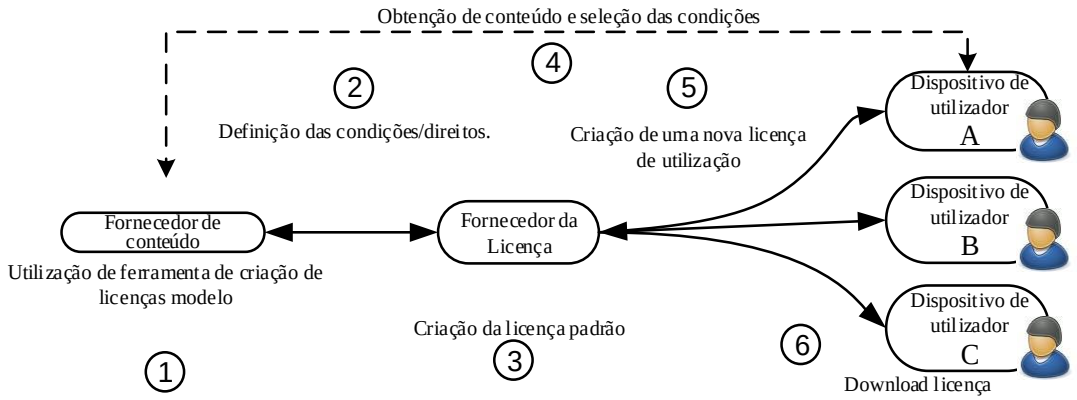


Figura 79 – Processo de definição da licença modelo (adaptado de Kamperman et al., 2007)

1 – Utilização de uma ferramenta do Fornecedor de Licenças para criar uma licença modelo de acordo com o modelo de negócio;

2 - Definição das condições/direitos que melhor se adaptam ao seu modelo de negócio;

3 - Criação da licença padrão com oferta das condições de utilização;

4 - Obtenção do conteúdo pelo utilizador e seleção das condições definidas pelo Fornecedor de Conteúdo na licença modelo;

5 - Criação de uma nova licença de utilização com as condições selecionadas;

6 - *Download* da licença.

2.3 Direitos referenciais

Sempre que um utilizador efetua um pedido de licença nunca poderá obter direitos que não estejam incluídos na licença modelo especificada pelo legítimo detentor do conteúdo. A estes direitos, que o autor/detentor do conteúdo deseja conceder a outros utilizadores dar-se-á o nome *de* "direitos referenciais". O termo refere-se à vontade do autor/detentor do conteúdo em transferir direitos sobre certas condições, mas tendo sempre por referência os direitos originais ao derivar outros direitos. Estes direitos são definidos logo no registo do conteúdo pelo autor/detentor do conteúdo e cobrem qualquer ação que possa ser executada ao derivar qualquer direito sobre o objeto inicial da criação.

Considere-se o exemplo de um docente que permite à sua instituição universitária distribuir um artigo científico aos alunos para que estes consigam visualizar o conteúdo. Para tal, emite uma licença com o privilégio de distribuição para a instituição (por exemplo, a Universidade). Quando a instituição usa este privilégio pode então passar a emitir licenças válidas para os estudantes e estes poderão assim visualizar o conteúdo. Tal vem ao encontro do princípio de posse, pois, apesar de a instituição não possuir o conteúdo, esta tem o direito de emitir licenças desde que as mesmas não excedam os direitos inicialmente concedidos pelo docente. A Figura 80 ilustra as concessões de direitos emitidos e recebidos pelos vários intervenientes num contexto académico típico.

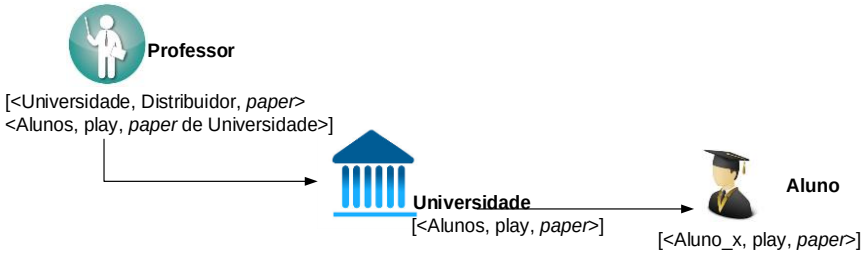


Figura 80 - Cenário de transmissão de direitos referenciais

Sempre que o objeto conteúdo é inserido e registado, o servidor de licenças gera uma licença modelo com os direitos e as condições de referência. Esta licença modelo será usada na oferta de direitos e condições sob as quais o conteúdo poderá ser utilizado, sendo então gerada uma licença de utilização específica para o utilizador que a adquire. Esta licença incorpora direitos herdados do seu progenitor: a licença modelo de distribuição. Por sua vez, esta incorpora direitos provenientes dos direitos referenciais definidos pelo autor/detentor de conteúdo. Caso seja gerado um derivado desta licença, os direitos referenciais são tidos em conta e herdados, sendo um subconjunto dos definidos na licença modelo (ambas igualam-se em situações limite). Por isso, pode-se dizer que há uma hierarquia na transmissão de direitos em linha sucessória.

Os direitos referenciais na vertente temporal, de utilização e de domínio, podendo ser alterados, ficam sempre restringidos a limites, sempre que há transmissão de direitos com derivação de condições. Contudo, e apesar de ser possível efetuar alterações, nem sempre todas as condições podem ser alteradas livremente ao criar um objeto de direitos, derivado de outro. Por exemplo, as seguintes condições não podem ser alteradas livremente:

- *Not Before*: não pode ser alterada para uma data anterior;
- *Not After*: não pode ser alterada para uma data posterior;
- Limite de utilização: se estiver presente não pode ser incrementado;
- Domínio de uso: se estiver presente não pode ser alterada;
- Região: se estiver presente não pode ser alterada;
- Condições económicas:
    - - Preço: se estiver presente não pode sofrer redução;
    - - Moeda: se estiver presente não pode ser alterada;
    - - Tipo pagamento: se estiver presente não pode ser alterado;
- Direitos transferidos: se estiverem presentes não podem ser incrementados.

3 Licenciamento de direitos e etapas da produção

Para melhor perceber como funciona o processo de definição de direitos numa licença torna-se necessário descrever as etapas em que as licenças modelo estão envolvidas. Desde o fornecedor de conteúdos (autor ou detentor do conteúdo), que interage com o sistema geral de licenças modelo da plataforma DRM para definir as regras de utilização de topo através do fornecedor de licenças, o qual, por sua vez, implementa a licença modelo onde os direitos podem ser delegados, existe um conjunto de passos a executar para que o utilizador final obtenha a licença de utilização. Cada um dos fornecedores de conteúdo, ao definir o seu modelo de negócio, está a indicar a forma de gerar a licença de utilização. Se o modelo, independentemente do tipo de conteúdo, for sempre o mesmo, então só existirá uma única licença modelo, mas se definir vários modelos, então existirão tantas licenças modelo quanto o número de possíveis condições de negociação que o fornecedor de conteúdos disponibilizar.

Quando o utilizador final obtém o conteúdo de um fornecedor, assim como a respetiva licença, esta é gerada usando uma licença modelo específica definida previamente pelo fornecedor de conteúdos e contendo os direitos referenciais. Esta licença de utilização contém o identificador único do conteúdo e a identificação do utilizador, podendo ser armazenada para ser descarregada posteriormente e/ou ser enviada diretamente para o dispositivo do utilizador final

responsável por assegurar a correta aplicação dos direitos e condições da licença governando o acesso e uso do respetivo conteúdo (Figura 81).

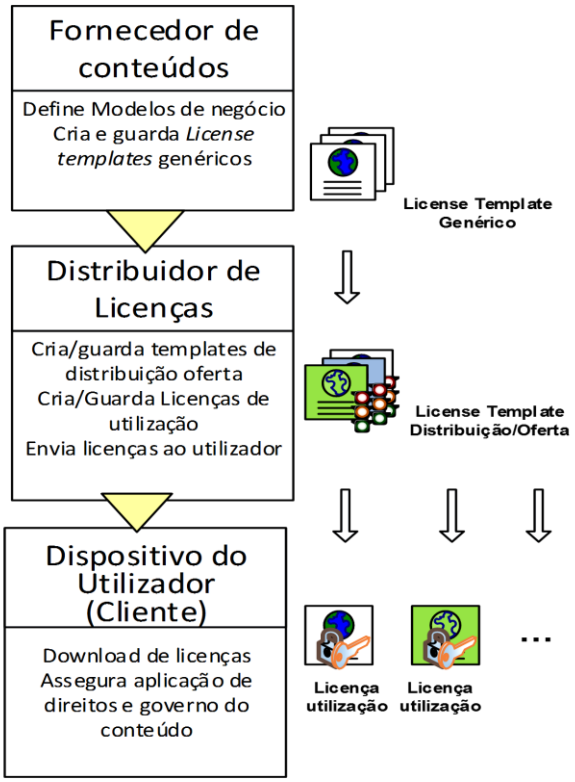


Figura 81 - Geração de licenças de utilização a partir de licenças modelo

Visto o processo de geração das licenças ser fundamental nas interações com os utilizadores quando há transmissão de direitos, as etapas na criação de licenças de um sistema DRM devem ser considerados em consonância com o ciclo de vida do conteúdo. Torna-se assim possível identificar as seguintes etapas:

- No momento da criação - No momento do carregamento do conteúdo, os direitos referenciais disponíveis são embebidos no objeto (objeto de direitos). O sistema DRM deve confirmar se o detentor de conteúdo está registado como criador e deverá ser informado se este utilizador criou efetivamente tal objeto quando o envia para a base de dados (por exemplo, comparando com o resumo de outros conteúdos armazenados no sistema).
- No momento do licenciamento - Ao criar a licença, o sistema DRM necessita de verificar se o pedido de geração tem proveniência legítima, se a licença é válida de acordo com as regras e relações estabelecidas e se a licença foi armazenada em conformidade.

- No momento de consumo - Ao executar determinadas ações correspondentes a direitos atribuídos sobre o conteúdo, terá de haver uma verificação para assegurar a validade da operação, de acordo com os direitos expressos constantes na licença.

A utilização do conceito de licenças modelo, é também importante no contexto académico, pois, de facto, permite estabelecer uma abordagem na proteção de conteúdos que pode abarcar vários níveis de proteção onde múltiplas licenças digitais podem ser geradas para um único conteúdo. O cliente utiliza uma licença modelo para efetuar um pedido de emissão de licença (encomenda) identificando o produto e a si próprio (e/ou ao equipamento que utiliza). Um mediador (servidor de licenças) irá então atuar quando receber este pedido e irá gerar uma licença de utilização para o conteúdo desejado baseado nas condições de utilização previamente definidas pelo fornecedor de conteúdo na licença modelo contendo a oferta de direitos a conceder.

O detentor de conteúdo, ao poder emitir licenças com o privilégio de redistribuição para os seus distribuidores, dá-lhes o direito de gerar novos tipos de licenças de redistribuição para outros subdistribuidores e/ou novas licenças de utilização para os utilizadores finais respeitando as permissões e restrições definidas nas licenças de redistribuição recebidas. As permissões (como, por exemplo, a reprodução, a cópia, a impressão, entre outros) numa licença de redistribuição corresponderão às ações que podem ser executadas e que foram definidas na licença de utilização que foi gerada a partir da licença de redistribuição. As restrições na licença de redistribuição corresponderão às limitações na distribuição do conteúdo. Assim, existe uma relação direta entre a licença progenitora e a licença gerada a partir desta, podendo assim estabelecer-se uma relação entre emissor na licença progenitora e recetor na licença emitida e ainda entre permissões e restrições definidas nas licenças de (re)distribuição e de utilização.

Esta relação vai permitir que um mecanismo de validação possa ser implementado antes da emissão de qualquer licença, devendo para tal existir uma entidade ou módulo que valide a emissão dessa licença. Obviamente que antes de esta ser emitida terão de existir um conjunto de regras que verifiquem a concordância de direitos entre os direitos contidos na licença progenitora e os direitos especificados na licença filho, de modo a que os últimos não ultrapassem os limites definidos nos direitos referenciais. Independentemente da verificação da elegibilidade do pedido realizado pelo utilizador para emissão de licença, um mecanismo simples de verificação poderá envolver os seguintes passos:

- Extração dos elementos da licença progenitora (licença pai);
- Criação de uma licença filho temporária baseada nos elementos extraídos da licença pai;
- Extração dos elementos gerados da licença filho;

- Verificação das regras de concordância entre as duas licenças;
  - Se as regras forem validadas então é emitida a licença filho que fica armazenada;
  - O utilizador que efetuou o pedido pode descarregar a licença filho requerida.

3.2 Redistribuição de licenças

Uma particularidade da redistribuição de licenças entre utilizadores está relacionada com o "*princípio de posse*" (somente o detentor de conteúdo poderá emitir uma licença válida para um determinado conteúdo). À primeira vista não seria possível que o utilizador obtivesse uma licença de utilização válida quando esta fosse emitida por outros que não fossem os detentores de direitos. Mas, sendo possível delegar direitos de forma controlada através da emissão de licenças pré-embebidas numa licença pai progenitora (neste caso a licença modelo), este *princípio* pode ser estendido um distribuidor autorizado.

O MPEG-21 REL e o RDD permitem estender esse mesmo princípio, pois especificam mecanismos que viabilizam a distribuição controlada de conteúdos suportando delegação de direitos. Assim, e tendo em conta esta extensão que permite ao distribuidor de licenças não ficar obrigado a possuir o conteúdo para que possa emitir uma licença, há, contudo, uma outra condição que o distribuidor de licenças tem de obedecer: possuir acesso à licença pai progenitora que lhe concede o direito de transmitir direitos sob a forma de licença a terceiros. Aqui há a ter em conta que para que o controlo sobre os direitos seja racional, sempre que haja concessão de direitos a terceiros, estes não podem ultrapassar os direitos referenciais.

No caso do contexto académico aqui analisado, há a considerar, não só do ponto de vista do utilizador final, mas também do fornecedor de conteúdos, uma interação com o SGA, que irá permitir a liberação das licenças consoante o perfil do utilizador. Com os dados obtidos do SGA o servidor de licenças dá início à verificação da elegibilidade do utilizador e ao posterior processo de emissão. No final, o utilizador, através do seu dispositivo, poderá obter a licença de utilização que lhe permitirá usar o conteúdo. De um modo indireto o SGA acaba por ser quem dá a autorização (ou não) da emissão de uma licença a utilizadores do contexto académico disponibilizando os interfaces de comunicação adequados perante o sistema DRM para que se possam obter os dados do utilizador e verificar a sua elegibilidade.

4 MPEG-21 e transmissão de direitos

A norma MPEG-21 REL permite que o detentor de conteúdos possa controlar os direitos concessionados e o distribuidor os possa propagar aos utilizadores finais de forma

condicionada, mas de acordo com as premissas iniciais definidas pelo detentor de conteúdos. O MPEG-21 REL, ao dar suporte ao licenciamento por emissão na distribuição e por delegação, permite que um distribuidor possa conceder direitos definindo quais os direitos a transmitir embebidos numa nova licença (Wang, 2004). Um dos direitos descritos no "*Core Schema"* do MPEG-21 REL é o direito de emissão ("*issue*"), o qual pode ser usado para especificar que o concessionado tem o direito de transmitir um determinado direito, podendo, contudo, não possuir necessariamente esse mesmo direito para seu uso (o concessionado tem o privilégio de transmitir um determinado direito, mas não o pode usar). A Figura 83 ilustra a estrutura típica de uma licença de distribuição MPEG-21 contendo este tipo de privilégio (Wang, 2004; Wang et al., 2005).

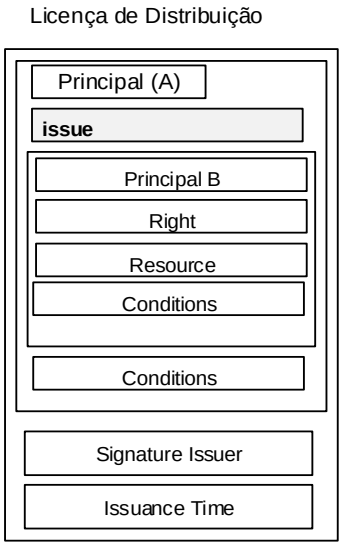


Figura 82 – Estrutura básica de uma licença de distribuição

Uma licença com o direito ou privilégio de emissão, é uma licença de distribuição em que o emissor ("*issuer*") autoriza ou concede ("grant") o concessionado ("*principal*") a emitir ("*issue*") outra licença com os direitos embebidos no direito de emissão. Neste tipo de licença o elemento "*resource*" é uma concessão emitida pelo concessionado ("*principal*").

A especificação MPEG-21 REL permite que o PEL possa ser definido e, por isso, este atributo está considerado na estrutura da licença. O suporte a este privilégio permite que o detentor de direitos original possa conceder a terceiros o direito de estes emitirem uma nova licença (filho) baseando-se nos direitos previamente definidos na licença progenitora (pai). Com base nos direitos definidos na licença secundária, e se aí estiverem definidos PELs, torna-se possível a emissão de uma licença de utilização que irá permitir o acesso e uso do conteúdo referenciado (Figura 83). Pode assim dizer-se que existem dois tipos de privilégios: o administrativo, em que

o detentor possui privilégios de emissão de licença, e o de acesso, em que o utilizador na posse da licença pode usar o conteúdo de acordo com o definido na licença emitida.

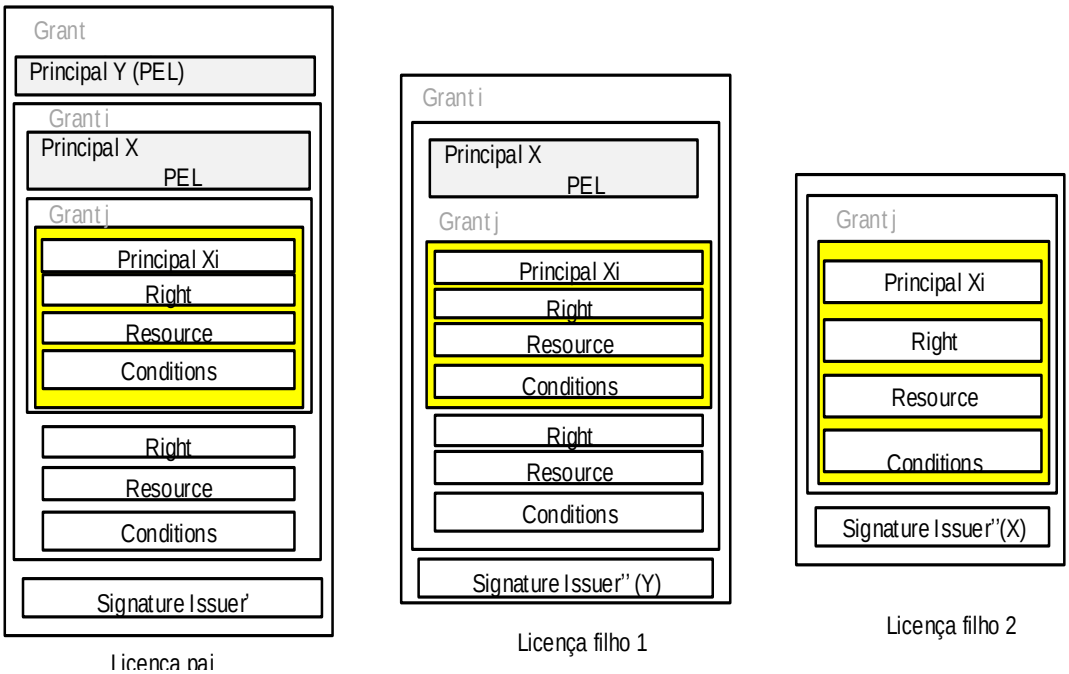


Figura 83 – Distribuição de licenças e estrutura básica de licenças MPEG-21

Para melhor se perceber o funcionamento deste tipo de licenciamento no caso específico do meio académico considere-se o seguinte caso de utilização em que um docente Professor A emite uma licença que autoriza a Instituição Universitária ABC a emitir licenças para que os seus estudantes possam ver/ler o conteúdo PDFxyz (Figura 84).

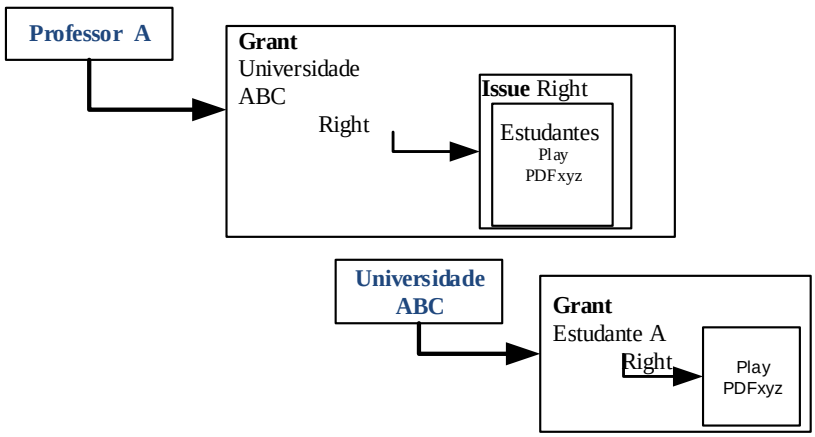


Figura 84 - Exemplo de transferência de direitos no meio académico

Neste caso a Instituição Universitária ABC tem autorização do professor para emitir licenças sobre o documento PDFxyz para os seus alunos, dando-lhes o direito de visualização. Contudo, note-se que a Instituição Universitária, apesar de poder emitir licenças a terceiros, não está

autorizada a aceder ao documento PDFxyz. Ou seja, tem direitos de nível administrativo (por exemplo, emissão de licença) mas não tem direitos de nível de acesso (Figura 85).

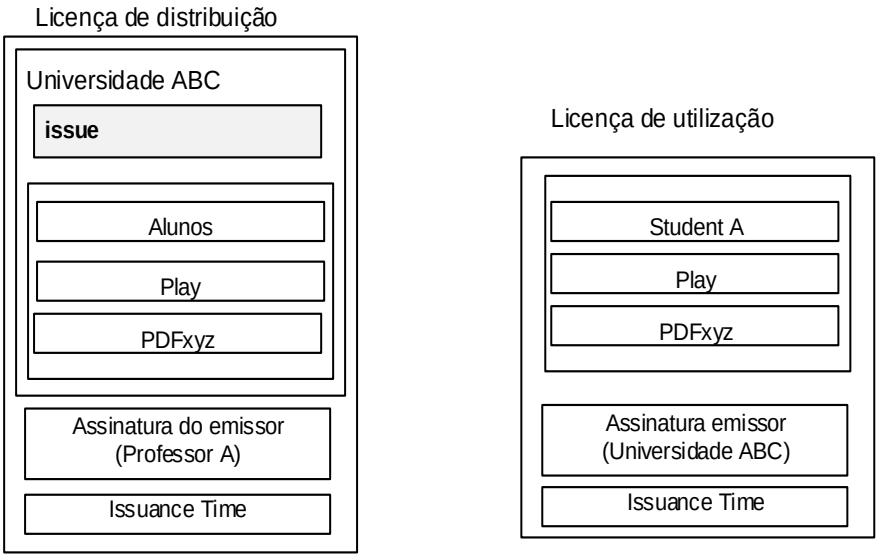


Figura 85 – Emissão de licenças e sua estrutura

Uma particularidade importante a considerar sobre o direito de emissão é que este especifica que o direito pode ser transmitido como uma concessão completa substituindo o elemento "*resource*". Assim, a concessão pode ser restringida aos sujeitos que recebem a permissão de nível de acesso. Este tipo de licenciamento permite assim a uma instituição educacional distribuir licenças de utilização por delegação dos detentores de conteúdo sem alterar os direitos originais da linha sucessória.

4.1 MPEG-21 - Dependência de direitos e validação

Considerando os principais papéis assumidos no decorrer da transmissão de direitos ao longo do ciclo de vida do conteúdo onde vários tipos de participantes interagem com o LIS, torna-se possível identificar dois elementos chave no controlo da delegação de direitos: a licença de distribuição e a licença de utilização.

- A licença de distribuição (licença pai) permite expressar direitos concedidos desde a origem, ou seja, desde o criador e/ou detentor de direitos sobre o conteúdo, para que o concessionário os possa negociar. Torna-se assim possível expressar e distribuir direitos para outros intervenientes na cadeia de valor desde que o concessionário tenha privilégios de delegação para tal (repare-se que o fluxo de direitos vai de montante para jusante (*downstream*), ou seja, do produtor de conteúdos para o utilizador final).

- A licença de utilização (licença filho) permite expressar direitos concessionados e negociados com o fornecedor de licenças através de uma licença de distribuição. Este tipo de licença é usado pelo utilizador final e exprime os direitos atribuídos por um concessionário.

A grande diferença entre estes dois tipos de licenças reside nos papéis que os intervenientes assumem, assim como nos direitos e condições em cada tipo de licença. Num caso a entidade que delega direitos atua como emissor, no outro, atua como recetor, existindo sempre uma relação de parentesco. Os direitos e condições recebidos nunca podem ultrapassar em quantidade e género os da licença pai devendo, por isso, ser validados. Na abordagem aqui apresentada, para validar se um participante pode exercer um direito sobre um recurso (neste caso os direitos transmitidos) definido na licença, as seguintes tarefas devem ser executadas (Wang, 2005):

- Verificar se o emissor é de confiança:
  - a assinatura associada ao emissor deve ser validada para assegurar que a informação na licença é autêntica.

- Verificar para cada uma das concessões ("grant") na licença:
  - se existe um *concessionado* na concessão, compatível com quem fez o pedido de licença;
  - se o direito na concessão é aquele que foi solicitado;
  - se o recurso na concessão é compatível com o recurso solicitado;
  - se a condição a observar na concessão é satisfeita.

Quando a verificação do emissor se realizar com sucesso e as verificações de todas as concessões também se realizarem com sucesso, então o pedido é autorizado. O SL fica assim responsável por verificar a concretização de todas estas tarefas antes de emitir qualquer licença. Para tal, o sub-módulo existente no módulo ILM do LIS executa todas essas validações e caso todas forem válidas dará início à criação da licença.

Um exemplo de utilização da norma MPEG-21 relativamente à concessão de direitos recorrendo ao elemento "<r:*issue*>" quando aplicado à plataforma ARMS pode ser dado através da situação comum em que o Professor A concede à Instituição Universitária B o direito de emitir licenças para um determinado conteúdo aos seus alunos C matriculados no seu curso X, licenças essas válidas para o corrente ano. A Figura 86 é exemplificativa de parte do objeto XML correspondente à licença de distribuição.

```
…
<r:license licenseID=”001”>
   <r:Grant licPartId=”issueGrant”>
      <r:forAll varName="alunoX"/>
      <r:forAll varName=”cursoX”>
        <r:anXmlExpression>curso123<r:anXmlExpression>
      </r:forAll>
      <r:forAll varName="anoX">
            <r:anXmlExpression>2013<r:anXmlExpression>
      </r:forAll>
      <r:keyHolder>...Universidade...</r:keyHolder>
      <r:issue/>
            <r:grant licPartId=”UsageGrant”>
                  <r:keyHolder varRef="alunoX"/>
                  <mx:play/>
                  <mx:diReference>urn:example:PDFxyz</mx:diReference>
                  <r:validityInterval varRef="anoX"/>
            </r:grant>
    </r:grant>
    <r:issuer>
      <dsig:Signature>
            <dsig:SignedInfo>...</dsig:SignedInfo>
            <dsig:SignatureValue> … </dsig:SignatureValue>
            <dsig:KeyInfo>...Professor A...</dsig:KeyInfo>
      </dsig:Signature>
    </r:issuer>
</r:license>
…
```

Figura 86 – Licença de distribuição da Universidade emitida pelo Professor

Face a um pedido de emissão de licença do aluno_111 dá-se início ao processo de validação do pedido. Resolvendo a variável “alunoX” para o “r:keyholder” que identifica o aluno e resolvendo a variável “anoX” para “r:valityInterval” que identifica o ano (por exemplo, 2013) e fazendo a validação interna no LIS através do sub módulo de validação do ILM com os dados retornados pelo SGA, confirma-se se o aluno está matriculado no corrente ano e no curso123. Se o resultado for positivo, torna-se possível emitir uma licença de utilização para o “aluno_111" ou outros na mesma situação (Figura 87). A resolução destas variáveis fica ao cuidado do sub-módulo ILM do LIS, que, para além de verificar se o utilizador está autenticado

no sistema, irá verificar se o pedido de emissão de licença é legítimo validando internamente as variáveis da licença obtendo os dados através do interface de comunicação com o SGA.

```
…
<r:license licenseID=”0001_1”>
   <r:Grant LicPartId=”usageGrant”>
      <r:keyHolder licPartId=”Aluno_111”>
            <r:info>
                  <dsig:KeyValue>
                        <dsig:RSAKeyValue>
                              <dsig:Modulus>…</dsig:Modulus>
                              <dsig:Exponent>…</dsig:Exponent>
                        </dsig:RSAKeyValue>
                  </dsig:KeyValue>
            </r:info>
      </r:keyHolder>
      <mx:play/>
      <mx:diReference>
            <mx:identifier>urn:example:PDFxyz</mx:identifier>
      </mx:diReference>
      <r:validityInterval>
            <r:notBefore>2013-09-01T00:00:00</r:notBefore>
            <r:notAfter>2014-09-01T00:00:00</r:notAfter>
      </r:validityInterval>
   </r:grant>
   <r:issuer>
      <dsig:Signature>
            <dsig:SignedInfo>...</dsig:SignedInfo>
            <dsig:SignatureValue> … </dsig:SignatureValue>
            <dsig:KeyInfo>...Universidade...</dsig:KeyInfo>
      </dsig:Signature>
</r:issuer>
</r:license>
…
```

Figura 87 – Licença do utilizador emitida pela Universidade

O privilégio de emissão de licença fica assim definido pela designação inicial do grupo ou indivíduo a quem foi concedido esse direito recorrendo ao elemento “<*issue*>” da norma MPEG-21 REL.

4.2 Validação da licença distribuição por emissão

A norma MPEG-21, indo ao encontro da necessidade de preservar os direitos básicos ao longo da cadeia de transmissão (direito de atribuição e integridade do conteúdo), permite especificar vários elementos na sua linguagem REL capazes de suportar a delegação de direitos entre intervenientes na partilha de conteúdo. No licenciamento que permite a concessão de direitos entre progenitor e descendentes deve ser considerada a dependência de direitos, de modo a não ultrapassar os direitos inicialmente definidos e transmitidos na cadeia sucessória (Figura 88). Antes de emitir a licença de utilização para o utilizador final, o sistema DRM tem de verificar se um conjunto de regras são cumpridas, nomeadamente se os termos e condições de utilização são corretamente definidos conforme estipulado pelo detentor de direitos. Para tal, deve ser executado um mecanismo de verificação da distribuição por emissão de licença, de modo a validar o seguinte conjunto de regras (adaptado de Rodriguez & Delgado, 2007a):

a) O elemento emissor na licença filho (*I'*) é igual (pertence) ao elemento *principal* (PA) na licença pai;

$$I' = PA \rightarrow True$$

b) A licença filho foi emitida posteriormente à licença pai e está dentro do intervalo de tempo de emissão especificado nas condições da licença pai;

$$valor(IT') > valor(IT) \rightarrow True$$

c) A concessão na licença pai (GP) é o direito "*issue"(S);*

$$GP(S) = "issue" \rightarrow True$$

d) Os elementos da licença pai incluídos no elemento recurso da concessão relacionam-se com os elementos da concessão na licença filho da seguinte forma:

1) O elemento "*principal"* na licença pai a quem podem ser concedidos direitos engloba sempre os elementos individualizados em "*principal"* da licença filho. Isto é, cada elemento principal da licença filho está sempre incluído no domínio "*principal"* definido pela licença pai;

$$G'(P') \in G(P) \rightarrow True$$

2) O elemento "*right"* dentro da concessão na licença pai é igual ao elemento "*right"* concessionado na licença filho;

$$G(R) = G'(R') \rightarrow True$$

3) O elemento "*resource"* na licença filho (Re) é igual ao elemento "*resource"* incluído na concessão na licença pai (Re');

$$G(Re) = G'(Re') \rightarrow True$$

4) O elemento "*conditions"* dentro da concessão da licença pai (Cg) é igual ao elemento *conditions* da licença filho (Cg').

$$G(Cg) = G'(Cg') \rightarrow True$$

e) As condições definidas na licença pai são observadas;

$$verificar(C) \rightarrow True$$

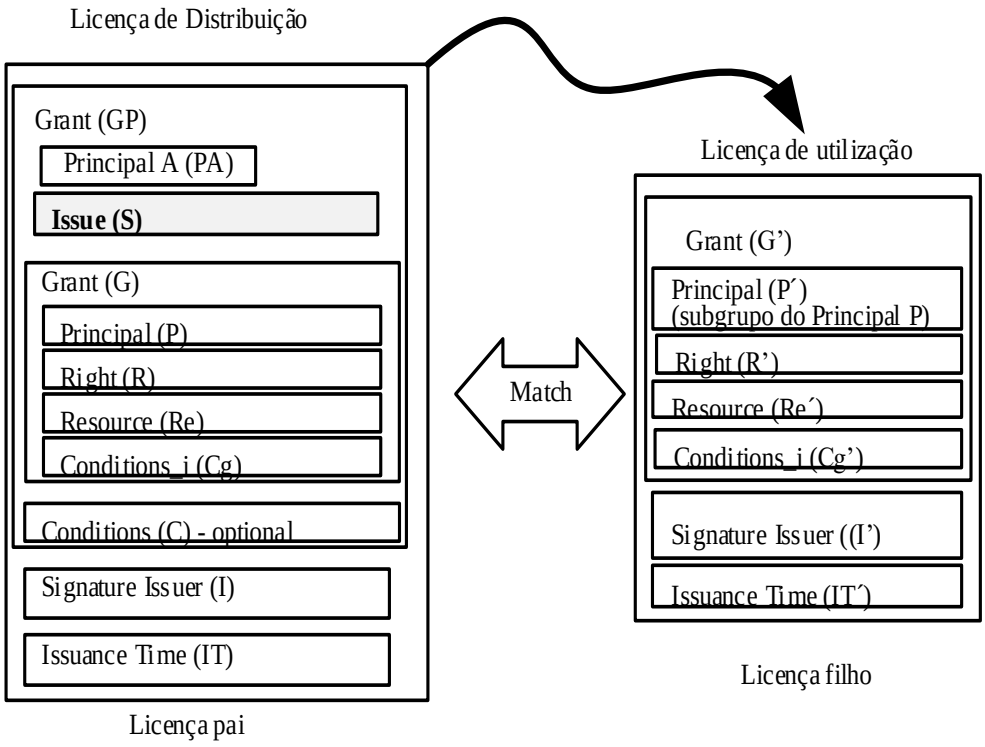


Figura 88 – Licenças de distribuição pai/filho por emissão de direitos

Podemos assim dizer que o mecanismo que permite a validação ao aplicar o conjunto de regras acaba por estabelecer e delimitar a linha sucessória de direitos a serem transmitidos entre quem concessiona e quem é concessionado.

5 Casos de utilização

Para melhor se perceber a aplicação do mecanismo de controlo de verificação da emissão na concessão de direitos, são de seguida analisados alguns casos de utilização considerando o meio académico.

Um caso de utilização vulgar ocorre quando um fornecedor de conteúdo (Professor) emite uma licença concedendo ao Bibliotecário da Instituição educacional (fornecedor/distribuidor) a autorização de conceder aos utilizadores o direito de visualizar um ficheiro PDF, mas obedecendo às condições definidas por ele. O Professor age como um fornecedor de conteúdo concedendo ao distribuidor (Bibliotecário) o direito de emitir um documento PDF durante um ano e de distribuir os direitos concedidos aos estudantes matriculados no ano letivo de 2013/2014. O Bibliotecário possui uma licença de distribuição com privilégios de emissão que consiste numa concessão que o habilitam ("principal") a emitir direitos ("*issue"*) de uso a estudantes sobre o documento PDF ("*resource"*) durante um ano ("*condition"*). Na licença de distribuição o emissor da licença deverá estar identificado pela sua assinatura digital, assim como a data e hora de emissão devem estar presentes (Figura 89). Contudo, o Bibliotecário deve emitir esta concessão para os alunos matriculados na instituição do Professor tendo as propinas pagas para o ano letivo de 2013/2014.

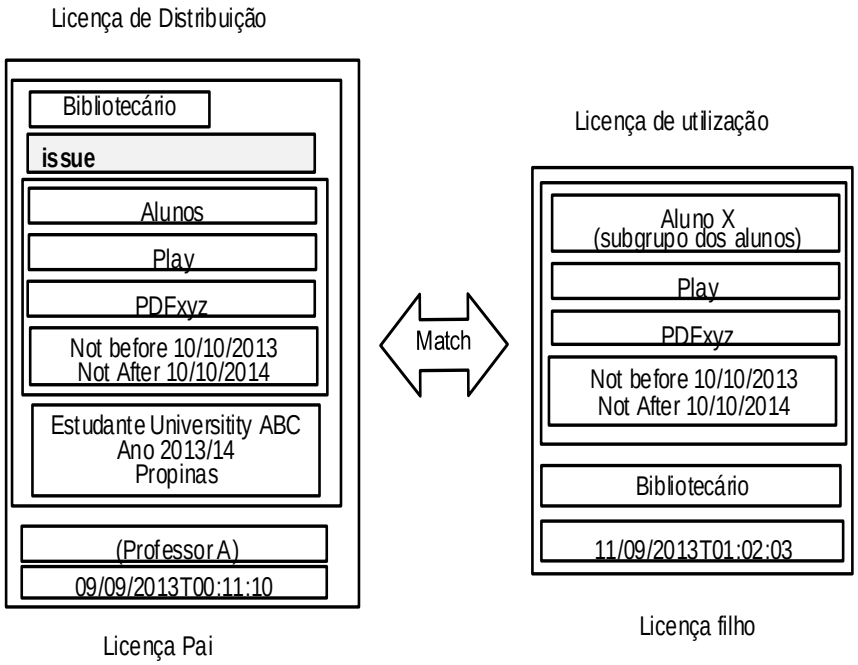


Figura 89 – Caso de utilização: licença de distribuição por emissão *versus* licença de utilização

No cenário aqui apresentado o mecanismo de verificação será aplicado sempre que o utilizador final fizer um pedido de emissão de licença, na qual lhe é concedido o direito para visualizar um documento PDF durante um ano. Ao pedir uma licença de utilização ao distribuidor de licenças, o utilizador final está a pedir ao LIS para gerar uma licença e emiti-la. Este serviço deve verificar se o distribuidor pode fornecer a licença de acordo com os termos e condições especificadas devendo para isso executar o seguinte mecanismo de forma a validar o processo de emissão de licença:

a) Verificar se:

$I' = PA -> True$

$I'(Bibliotecário) = PA(Bibliotecário)$

b) Verificar se:

$valor(IT') > valor(IT) -> True$

$11/09/2013T01:02:03 > 09/09/2013T00:11:10$

c) Verificar se:

$GP(S) = "issue" -> True$

$GP("issue") = True$

d)

1 – verificar se:

$G'(P') \in G(P) -> True$

$G'(aluno\ X) \in G(alunos)$

2 – verificar se:

$G(R) = G'(R') -> True$

$G(Play) = G'(Play)$

3 - verificar se:

$G(Re) = G'(Re') -> True$

$G(PDFxyz) = G'(PDFxyz)$

4- verificar se:

$G(Cg) = G'(Cg') -> True$

$G(_{10/10/2013} < valid < _{10/10/2014}) = G'(_{10/10/2013} < valid < _{10/10/2014})$

e)

$verificar(C) -> True$

G'(aluno X) = é aluno do professor A na Instituição Universitária ABC e tem as propinas pagas no ano letivo de 2014/2015

No cenário apresentado a validação do principal ("aluno X") na licença filho e de todos as condições de distribuição (estudantes da Instituição Universitária ABC, matriculados no ano 2013 com propinas pagas) tornam-se fulcrais, pois definem a quem e em que condições os direitos são concedidos. Usando estes elementos declarativos, os detentores de conteúdos (por exemplo, os docentes) e os distribuidores (por exemplo, o bibliotecário a quem a Instituição Universitária atribui a tarefa de conceder direitos) podem declarar o concessionado ("principal") a quem a licença de utilização será designada e o perfil que este concessionado deve possuir. Contudo, uma validação adicional deve ser executada de modo a confirmar o

perfil do concessionado e se as condições adicionais são por ele obedecidas. Possuindo o LIS do sistema ARMS uma interface de comunicação com o SGA, torna-se possível implementar o mecanismo de validação, de modo a confirmar se o Professor em causa é membro da Instituição Universitária. Sendo este válido, então o gerador de licenças cria uma licença padrão para distribuição aos estudantes da Instituição Universitária. Quando o aluno, atuando sobre a licença de distribuição, tenta obter uma licença de utilização realizando um pedido de emissão de licença, o gerador de licenças do LIS contacta a plataforma SGA para confirmar se o aluno pertence à instituição e se está matriculado naquele ano com as propinas pagas. Se a confirmação for positiva, então o utilizador é elegível podendo dar-se início à criação da licença de utilização (Figura 90).

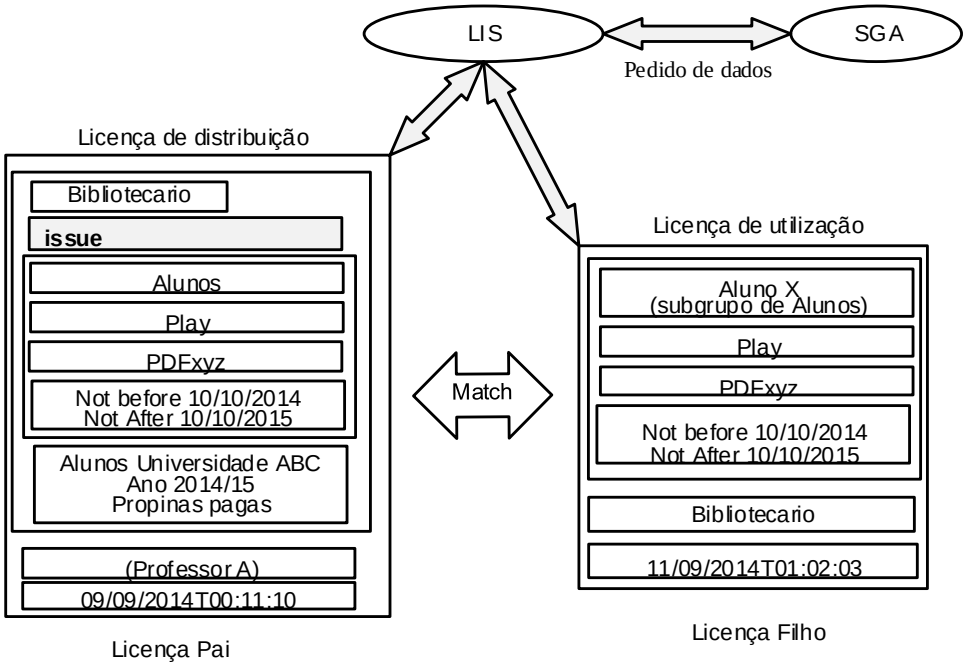


Figura 90 – Cenário académico: emissão da licença de distribuição

Um outro caso de uso típico de demonstração da aplicação do mecanismo de verificação da distribuição de licenças pode ser considerado quando um docente pretende partilhar um documento com os seus colegas com quem leciona uma disciplina e também com os alunos matriculados nesse ano nessa unidade curricular. Esta é uma situação típica nos sistemas de e-*learning* no meio académico onde "Professor Z" dono do conteúdo original pretende emitir uma licença que autoriza os seus colegas a visualizar esse documento, mas autorizando também os seus alunos a visualizá-lo desde que estejam matriculados nessa unidade curricular nesse ano letivo. Na licença de distribuição estes dois tipos de concessionados (alunos e colegas docentes) deverão estar presentes, assim como as condições a que devem obedecer. O mecanismo de verificação de licenças, inserido no gerador de licenças do LIS encarregar-se-á de confirmar

perante os dados provenientes pelo SGA se é possível a emissão de licenças (Figura 91) para o perfil de utilizador e perante as condições especificadas.

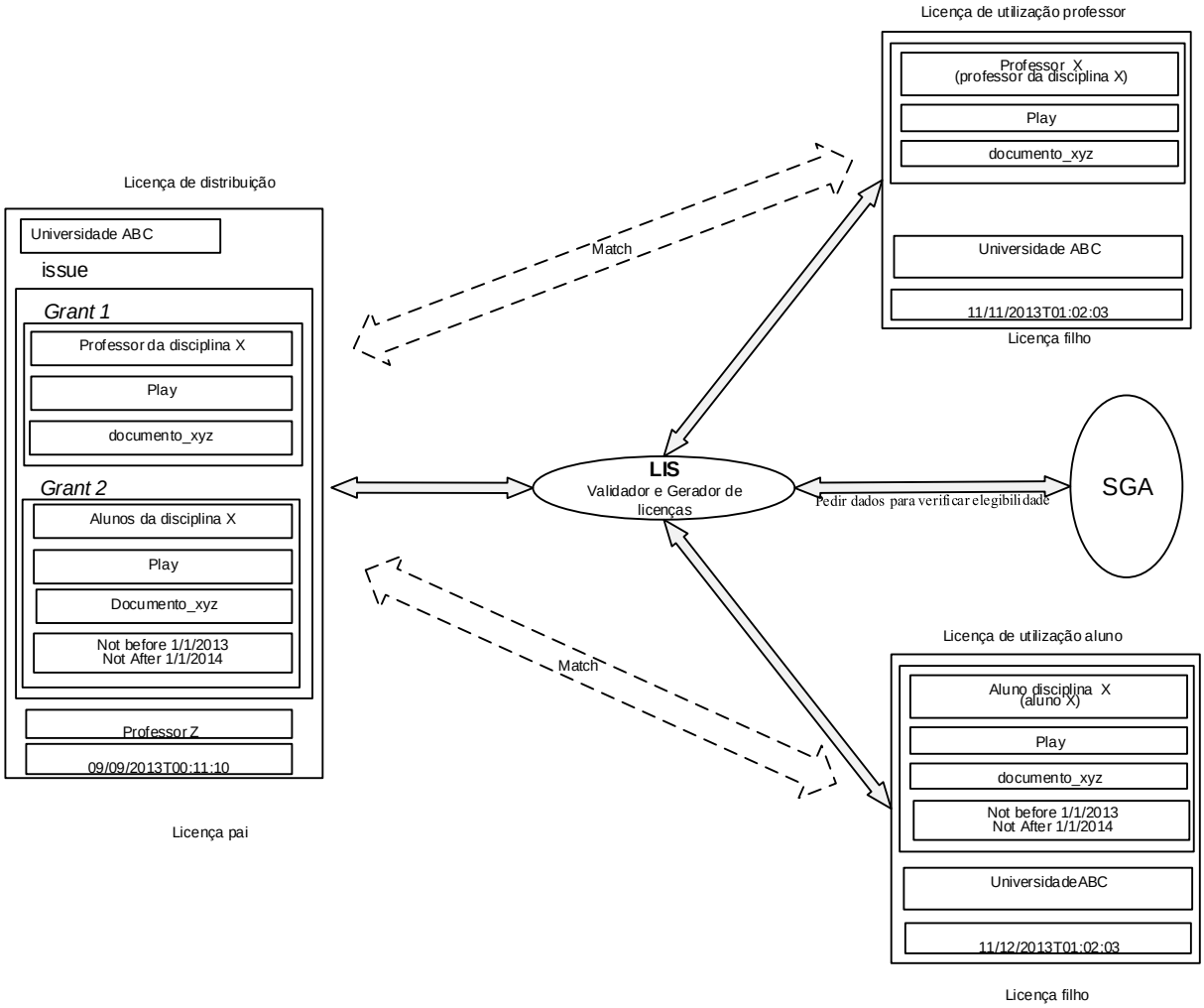


Figura 91 – Cenário académico: distribuição direta de licenças e interação com o SGA

O mecanismo de verificação encarregar-se-á de validar a licença a emitir consoante o perfil do utilizador que realizou o pedido de emissão da licença, procedendo à emissão de um de dois tipos de licenças de utilização, de acordo com o perfil do utilizador. Obviamente que a validação das condições de utilização descritas na licença de distribuição e do perfil do utilizador perante o SGA terão de ser satisfeitas de acordo com o mecanismo de verificação para que a criação da licença se realize.

Um outro caso de uso de demonstração da aplicação do mecanismo de verificação da distribuição de licenças pode ser considerado quando um docente pretende partilhar um documento só com os seus colegas de departamento, concedendo-lhes o direito de o visualizar e autorizando-os a distribuir licenças aos seus alunos matriculados no atual ano letivo. Considerando que o Professor Z possui o conteúdo original podendo atuar como emissor de

direitos para outros professores, devemos notar que é possível atribuir dois tipos de direitos correspondentes a dois tempos diferentes. Num primeiro tipo, permite aos seus colegas a visualização do conteúdo e, num segundo tipo, autoriza-os a emitir licenças para os alunos pertencentes à instituição académica onde ensina, de acordo com as condições especificadas por ele (alunos matriculados no corrente ano letivo).

O Professor Z, ao agir como um fornecedor de conteúdo, concede aos seus colegas de departamento autorização para acederem ao conteúdo. Ao mesmo tempo, autoriza-os a emitir licenças aos alunos matriculados na Instituição Universitária desde que estes estejam matriculados no corrente ano letivo. A verificação perante os dados do SGA é crucial para que o gerador de licenças faça a emissão quer da licença para os docentes da unidade curricular X quer posteriormente para a emissão da licença dos alunos dessa unidade curricular (Figura 92).

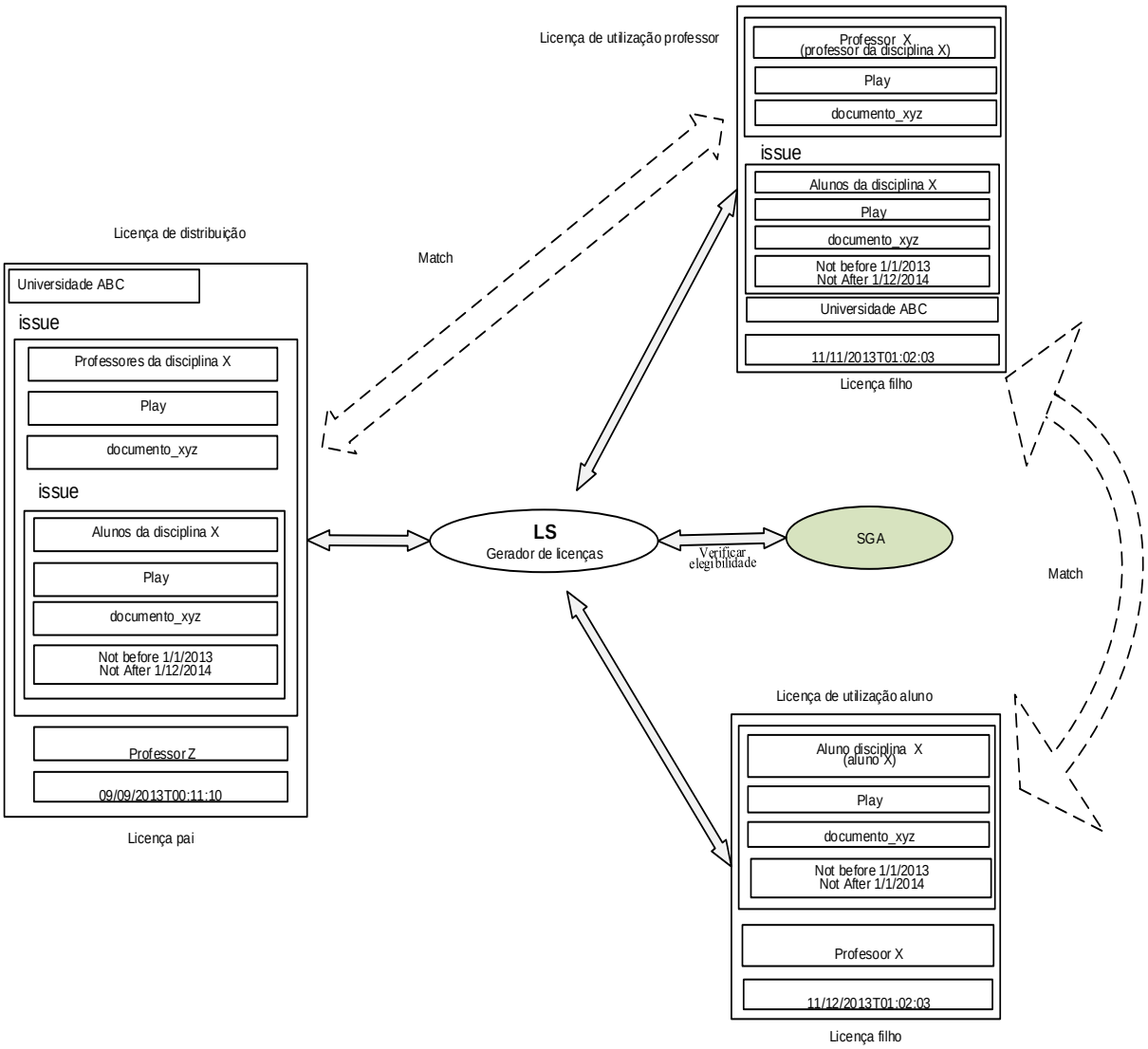


Figura 92 – Cenário académico: geração de licenças e distribuição por emissão

No final da cadeia de emissão temos dois tipos de licenças: uma para o docente (de utilização e de redistribuição) e outra para o aluno (de utilização). A grande diferença entre elas reside na dependência que a licença dos alunos tem sobre a dos docentes. A aplicação do mecanismo de verificação de distribuição de licenças considera que temos duas concessões: uma dentro da outra. A primeira é para o docente poder usar e emitir licenças sobre o conteúdo ("grant1"), a outra é para o aluno poder usar o conteúdo ("grant 2").

A aplicação do mecanismo de verificação da distribuição de licença faz validações muito similares quer para a primeira concessão ("grant1") quer para a segunta ("grant2").

"grant1":

a) O elemento emissor na licença filho é igual/pertence ao elemento "*principal"* na licença pai;

$$I' = PA -> True$$

$$\text{UnivABC}_{\text{filho}} = \text{UnivABC}_{\text{pai}}$$

b) A licença filho foi emitida posteriormente à licença pai e está dentro do intervalo de emissão permitido especificado nas condições da licença pai;

$$valor(IT') > valor(IT) -> True$$

$$11/11/2013T01:02:03_{\text{filho}} > 09/09/2013T00:11:10_{\text{pai}}$$

c) A concessão na licença pai é o direito "*issue";*

$$GP(S) = "issue" -> True$$

$$\text{"issue"}_{\text{pai}} \text{ -> True}$$

d) Os elementos da licença pai incluídos no elemento recurso da concessão relacionam-se com os elementos da concessão na licença filho da seguinte forma:

1) O elemento "*principal"* na licença pai a quem podem ser concedidos direitos engloba sempre os elementos individualizados em "*principal"* da licença filho; isto é, cada elemento principal da licença filho está sempre incluído no domínio "*principal"* definido pela licença pai;

$$G'(P') \in G(P) -> True$$

$$\text{Professor da disciplina } x_{\text{filho}} \in \text{Professores da disciplina } x_{\text{pai}}$$

2) O elemento "*right"* dentro da concessão na licença pai é igual ao elemento "*right"* concessionado na licença filho;

$$G(R) = G'(R') \rightarrow True$$

$Play_{pai} = Play_{filho}$

3) O elemento "*resource"* na licença filho é igual ao elemento "*resource"* dentro da concessão na licença pai;

$$G(Re) = G\acute{} \ (Re\acute{}\ ) \rightarrow True$$

$documento_xyz_{filho} = documento_xyz_{pai}$

4) O elemento "*conditions"* dentro da concessão da licença pai é igual ao elemento "*conditions"* da licença filho;

Não aplicável

e) As condições definidas na licença pai são observadas;

condições não definidas(não aplicável)

"grant2":

a) O elemento emissor na licença filho é igual (pertence) ao elemento "*principal"* na licença pai,

$$I' = PA \rightarrow True$$

Professor da disciplina $X_{filho} =$ Professor da disciplina X_{pai}

b) A licença filho foi emitida posteriormente à licença pai e está dentro do intervalo de tempo para emissão permitido especificado nas condições da licença pai,

$$valor(IT') > valor(IT) \rightarrow True$$

$11/12/2013T01{:}02{:}03_{filho} > 11/11/2013T00{:}11{:}10_{pai}$

c) O elemento "*right"* concessionado na licença pai é o direito "*issue"*,

$$GP(S) = "issue" \rightarrow True$$

"issue" $_{pai}$ -> True

d) Os elementos da licença pai incluídos no elemento recurso da concessão relacionam-se com os elementos da concessão na licença filho da seguinte forma:

1) O elemento "*principal*" na licença pai a quem podem ser concedidos direitos engloba sempre os elementos individualizados em "*principal"* da licença filho; isto é, cada elemento principal da licença filho está sempre incluído no domínio "*principal"* definido pela licença pai;

$$G'(P') \in G(P) \rightarrow True$$

Aluno $x_{filho} \in$ Alunos x_{pai}

2) O elemento "*right"* dentro da concessão na licença pai é igual ao elemento "*right"* concessionado na licença filho;

$$G(R) = G'(R') \rightarrow True$$

$\text{Play}_{\text{pai}} = \text{Play}_{\text{filho}}$

3) O elemento "*resource"* na licença filho é igual ao elemento "*resource"* dentro da concessão na licença pai;

$$G(Re) = G'(Re') \rightarrow True$$

$\text{documento_xyz}_{\text{filho}} = \text{documento_xyz}_{\text{pai}}$

4) O elemento "*conditions"* dentro da concessão da licença pai é igual (ou está englobado) ao elemento "*conditions"* da licença filho;

$$G(Cg) = G'(Cg') \rightarrow True$$

1/1/2013<validade<1/1/2014 = 1/1/2013<validade<1/1/2014

e) As condições definidas na licença pai são observadas;

(assume-se que é verificado por uma aplicação externa que valida a condição: condições não definidas (não aplicável).

A validação do concessionado ("*principal"*) nas licenças filho e de todas as condições são importantes no contexto de validação. Só assim é possível verificar se o perfil a quem se atribui a licença está inserido no meio académico e quais as restrições que podem ser transmitidas. A obtenção de dados do utilizador graças à interação do gerador de licenças no LIS com o SGA é aqui o elemento essencial nesta validação, pois assim consegue obter-se a informação necessária para aplicar o mecanismo de verificação de distribuição de licença antes de se emitir a licença ao concessionado, garantindo-se a linha sucessária. Os cenários de utilização são inúmeros e dada a diversidades de situações existentes no meio académico podem tornar-se extremamente complexos consoante as interações entre participantes e direitos a transmitir.

6 Conclusão

A transmissão de direitos e a importância da questão da sua manutenção possui um papel preponderante em qualquer sistema DRM. A validação do pedido de emissão de licença, tendo em conta a elegibilidade de quem o solicitou, mas também a validação do pedido perante as condições definidas pelo criador, vem assegurar que os direitos são preservados ao longo da linha sucessória. A norma MPEG-21 REL fornece o suporte necessário no processo de transmissão de direitos tendo em conta o PEL, estando por isso adaptado ao contexto académico e às necessidades mais elementares dos detentores de conteúdos/direitos. O mecanismo de

avaliação do pedido de emissão aqui proposto, com vista a verificar se os direitos referenciais inicialmente definidos são respeitados ao longo da linha sucessória, vem permitir o controlo de direitos pelo criador do conteúdo. A intervenção do SGA como entidade capaz de disponibilizar a informação necessária para realizar essa validação pelo LIS na plataforma ARMS é de crucial importância e vem viabilizar a implementação desse mecanismo. Assim, a licença pode ser corretamente emitida em observância com os direitos da linha sucessória e obedecendo aos termos e condições inicialmente definidos pelo detentor de direitos/autor. Ao atuar como um controlador de domínio permite verificar se o pedido do utilizador é legítimo sendo proveniente de membros da instituição e também se obedece aos critérios da linha sucessória estabelecidos pelos direitos referenciais. A integração do ARMS com o sistema SGA simplifica a gestão da emissão de licenças evitando a complexidade da gestão do licenciamento de sistemas baseados na gestão de certificados digitais X.509 (Morin, 2009), de licenças certificado MPEG-21 REL (Yang et al., 2008; Wang et al., 2005; Sheppard & Safavi-Naini, 2006a), ou licenças agregadas (Sachan et al., 2010; Sachan & Kankanhalli, S., 2012). Não sendo necessário aos utilizadores possuírem comprovativos adicionais às licenças de utilização que os validem como membros de um determinado grupo (por exemplo, o de pertencerem ao meio académico) e que obedecem às condições especificadas inicialmente para concessão de direitos o licenciamento passa a ser mais simplificado. Os utilizadores deixam assim de possuir objetos adicionais que comprovem a pertença a um grupo e condições (no caso de possuírem licença certificado), como também se torna desnecessário a confirmação perante todos distribuidores de quais os direitos que podem ser transmitidos (licenças agregadas), pois basta a confirmação do servidor de licenças, através do mecanismo de validação, para se proceder à emissão de licenças.

Este capítulo é baseado nas publicações de Marques et al. (2015a); Marques & Serrão (2015c) e Marques, Serrão & Metrolho (2015).

Capítulo 10

Controlo da concessão de direitos entre utilizadores

Resumo

Neste capítulo apresenta-se uma contribuição para uma solução de transmissão de direitos baseados num esquema de gestão de licenças em que se considera a delegação de direitos entre utilizadores do domínio académico. A intervenção do sistema de gestão académica (SGA) num sistema DRM como o ARMS permite estabelecer um ambiente em que a validação da emissão das licenças possa ser realizada de forma controlada para o domínio académico. É aqui tida em conta a possibilidade de transmissão infinita de direitos entre membros de um mesmo grupo através da distribuição de licença por delegação a terceiros suportada pela norma MPEG-21 (Bekaert, De Kooning & Van de Walle, 2006; Wang, 2004) e também é considerada a possilidade do controlo da profundidade dessa delegação ao longo da cadeia de transmissão. O contributo principal deste capítulo relaciona-se com a descrição de mecanismos de validação do licenciamento por delegação entre os utilizadores do meio académico. Alguns casos de utilização são aqui apresentados, assim como o método de processamento das licenças de distribuição que permitem a validação e criação de licenças de utilização e a sua transmissão entre membros do mesmo meio.

1 Introdução

A capacidade de especificar e comunicar informação relacionada com direitos entre os intervenientes do ciclo de vida do conteúdo e fluxos associados é um requisito importante a ter em conta no desenvolvimento de sistemas DRM eficazes e eficientes (Wang et al., 2005). Por isso, no desenvolvimento de sistemas de DRM eficazes é de especial importância a linguagem de expressão de direitos (REL) que permita aos participantes definir e transmitir direitos. Contudo, esta transmissão, ao evoluir com as relações entre intervenientes, torna-se tanto mais complexa quantos mais papeis puderem os participantes assumir no ciclo de vida do conteúdo. O ambiente educativo e académico é um destes ambientes complexos bastante difícil de analisar, pois qualquer utilizador que atue sobre um conteúdo ou recurso educativo tanto pode agir como detentor de direitos/autor, como distribuidor e/ou como consumidor, tornando difícil

classificar clara e objetivamente as suas propriedades referentes a direitos para os vários papéis assumidos. Apesar da capacidade de distribuição direta de direitos poder dar o suporte necessário aos detentores de conteúdo em variados modelos de negócio relacionados com o acesso e a partilha do conteúdo, tem de se tomar especial atenção a uma forma de distribuição de conteúdos inerente ao meio académico, ou seja, a distribuição entre utilizadores. Nesta forma de distribuição, mais complexa que a distribuição direta, somente os membros de um determinado grupo podem usar o conteúdo partilhado podendo definir a profundidade da transmissão de direitos entre eles. Deste modo consegue-se assim viabilizar a superdistribuição de conteúdos. A redistribuição de direitos entre utilizadores é de facto uma técnica chave dos sistemas de DRM podendo aumentar a motivação dos utilizadores comuns para obterem e usarem mais conteúdos, contribuindo assim para que o sistema de DRM seja mais facilmente aceite pelos utilizadores (Cheung & Curreem, 2002). A intervenção do SGA como entidade capaz de disponibilizar a informação adequada à implementação de mecanismos de validação da emissão da licença permite que esta possa ser corretamente emitida em observância com os direitos da linha sucessória para membros do mesmo domínio. Ao atuar como um controlador de domínio permite verificar se o pedido do utilizador é legítimo para utilizadores do domínio educacional.

Para melhor perceber as interações entre os variados intervenientes na concessão de direitos neste meio, tomou-se como referência o modelo proposto apresentado no capítulo quarto, onde são considerados três papéis fundamentais: o criador e detentor de conteúdo, o fornecedor ou distribuidor de conteúdo e o utilizador final. Um esquema onde estes papéis fazem parte permite delinear uma abordagem do controlo da concessão de direitos, suficientemente abrangente, capaz de suportar os mais variados modelos de negócio, incluindo os mais representativos do meio académico. Nesta abordagem começa-se sempre pela proteção do conteúdo e o criador do conteúdo atribui uma concessão do conteúdo original e admite que diferentes distribuidores o possam distribuir aos consumidores através da utilização de uma plataforma de DRM, o ARMS, onde se pode efetuar o controlo das licenças. Para que haja um maior controlo sobre a emissão da licença, torna-se necessário considerar um esquema/mecanismo que permita a gestão de licenças onde o detentor de conteúdos consiga gerir a transmissão dos seus direitos concedidos a terceiros definindo a profundidade da cadeia sucessória. Assim, neste capítulo apresenta-se a descrição de mecanismos de validação de licença por delegação e do método de processamento de licenças para distribuição que permite a criação deste tipo de licenças.

2 Dependências de direitos e licenciamento

Para que os termos e condições definidos pelo criador sejam sempre observados ao longo da cadeia de valor, devem existir mecanismos que validem a emissão de licenças quando estas são geradas em conformidade com os termos e condições predefinidos pelo criador ou detentor de direitos (Rodriguez & Delgado, 2007a). O mais simples dos cenários de concessão de direitos corresponde àquele em que o detentor de direitos sobre o conteúdo (como, por exemplo, o criador/autor) concede num elemento que tem acesso ao servidor de licenças o direito de poder emitir licenças de utilização a terceiros. Este cenário corresponde tipicamente a uma concessão direta, pois existe um intermediário a quem o criador concede direitos, para estes poderem ser posteriormente transmitidos a terceiros. O detentor de conteúdo (por exemplo, um professor) com direitos sobre o conteúdo delega num elemento que tem acesso ao servidor de licenças (por exemplo, alguém que representa a entidade académico, outro professor ou professores do seu departamento) o direito de poder emitir licenças de utilização a terceiros (por exemplo, alunos.) (Figura 93).

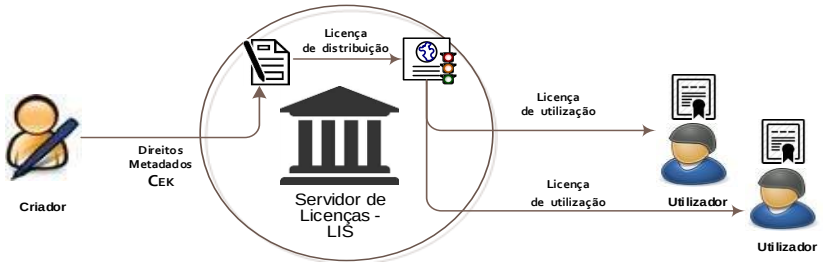


Figura 93 – Distribuição simples de licenças

Neste tipo de concessão, os direitos são transmitidos pelo criador ou detentor de conteúdo através de um formulário disponibilizado pela aplicação de gestão de direitos do LIS. Este formulário está alinhado com a licença modelo (*license template*) que define o tipo de transmissão de direitos adotado pelo detentor de conteúdo. Os direitos transmitidos são guardados conjuntamente com outros metadados no LIS sob a forma de uma licença de distribuição. Esta licença fica assim disponível no LIS para que terceiros, devidamente autorizados (por exemplo, a Universidade), possam aceder e transmiti-los. Essencialmente estas concessões podem desdobrar-se em dois tipos distintos que passam a ser descritos de seguida:

Subconcessão (Figura 94). Um utilizador, depois de interagir com o LIS através da aplicação de gestão de direitos e de verificar quais as licenças de distribuição que lhe concedem direitos de delegação (licença de delegação), pode transmitir novamente direitos a terceiros de acordo com os termos definidos na licença (2). É então criada uma licença de distribuição no LIS que

fica disponível para a interação com os utilizadores finais (2a). Estes, depois de selecionarem a licença e os termos pretendidos, podem então obter a respetiva licença de utilização (2b) caso preencham os requisitos necessários especificados na licença de distribuição. Este tipo de licenciamento tem certas particularidades, pois a licença não sai fora do perímetro de atuação do LIS ficando aí alojada e servindo para a emissão de licenças de utilização. Contudo, este tipo de concessão aumenta a complexidade de gestão de licenças, pois introduz novos participantes que interagem com o LIS com capacidade de distribuição de licenças.

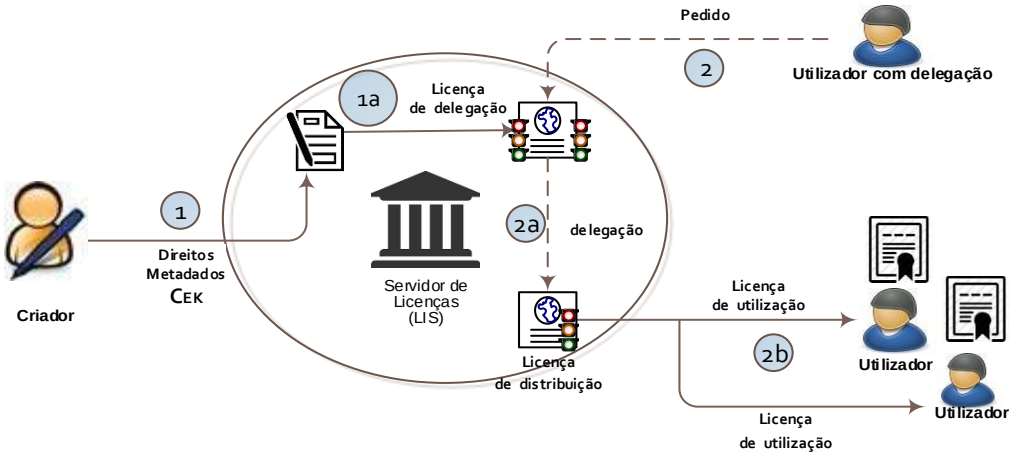


Figura 94 – Licenciamento por subconcessão

Como exemplo deste cenário podemos considerar o caso de um professor que delega direitos sobre um conteúdo por si criado a outros professores da sua instituição, em que estes têm o previlégio que os autoriza a criar licenças de distribuição e assim poderem emitir licenças de utilização aos alunos. Na forma mais minimalista a concessão direta acaba por ser o tipo mais simples de subconcessão.

Superdistribuição. Por fim, podemos considerar a concessão de direitos entre utilizadores ou entre membros de um grupo de utilizadores através de uma licença que lhes foi atribuída. Os direitos a transmitir são guardados na própria licença podendo os utilizadores, quando autorizados, retransmitir direitos a terceiros, independentemente de poderem usar o conteúdo ou não. Um exemplo concreto é o de envio de uma licença de utilização entre alunos a atuar como utilizadores finais e/ou entre alunos e professores que lhes concedem direitos de utilização.

A possibilidade de conceder e redistribuir direitos é aqui o conceito fulcral na descentralização da gestão de privilégios num sistema DRM. O direito de conceder um privilégio pode somente ser atribuído por aqueles que possuem esse privilégio. Tal vem viabilizar cenários onde um detentor tem autoridade para criar uma permissão, ou seja, o licenciador delega no licenciado a

autorização para agir como licenciador de um conjunto de novas licenças. A concessão passa assim a ser a peça chave para controlar os direitos concedidos ao longo do ciclo de vida do conteúdo, permitindo ao licenciador ser capaz de controlar qualquer parte da licença concedida. Contudo, quando os licenciados são declarados como elementos emissores numa licença de distribuição, passam também a possuir privilégios, não podendo contudo ultrapassar os direitos delegados pelo emissor original da licença. Por isso, e independentemente da elegibilidade do utilizador perante o sistema DRM, torna-se premente que se faça respeitar um conjunto de regras antes da emissão da licença. Ou seja, o processamento da licença para distribuição deve assegurar que a licença gerada está em conformidade com a licença progenitora validando os concessionados e os direitos transmitidos em observância com os termos e condições originais. Assim sendo, pode-se garantir que atavés de mecanismo de validação a licença emitida irá permanecer dentro do domínio em causa.

3 Controlo sobre direitos transmitidos recorrendo ao MPEG-21

A especificação MPEG-21 REL permite realizar a distribuição de direitos através de alguns mecanismos que governam o licenciamento (Wang et al., 2005; Rodriguez & Delgado, 2007a). Nesta especificação o controlo de direitos transmitidos é realizado com o recurso a diferentes tipos de licenciamento em que o detentor de conteúdo pode restringir o fluxo de direitos definidos na licença emitida (Wang et al., 2005). O detentor de conteúdo define uma licença modelo e a licença emitida pelo distribuidor deverá enquadrar-se nas regras definidas nesta licença modelo. Por isso, é possível dizer que há uma dependência de direitos na licença em que esses direitos são transmitidos não podendo estes exceder os direitos de referência da licença progenitora. Tal como vimos anteriormente (Capítulo 5), a utilização do privilégio de emissão é um dos mecanismos básicos pelo qual o conteúdo sob governação pode ser distribuído de uma forma controlada. Para que a licença possa ser emitida, o PEL deve estar atribuído ao emissor da licença relativamente à concessão de direitos, devendo este estar explicitamente autorizado. Assim, a licença transporta a autorização para que um elemento possa emitir uma concessão, ou seja, transporta a autorização, sob a autoridade do emissor da licença, para que um participante emita outras licenças para as quais está autorizado. Este tipo de transmissão de direitos é suportado pela norma MPEG-21 REL através do elemento "<*issue*>" inserido no elemento "<*grant*>" que permite efetuar subconcessões. A identificação do emissor é garantida na emissão da licença através da assinatura digital assim como os detalhes específicos de emissão da licença (como, por exemplo, a data e hora). Contudo, ao usar a concessão por emissão ("*issue"),* o nível de delegação de direitos tem patamares (ou degraus)

muito restritos que têm de ser pré-definidos logo na origem da criação da licença de distribuição, o que limita a profundidade da cadeia de delegação. A norma MPEG-21 REL, ao disponibilizar funcionalidades de controlo por delegação na concessão de direitos, não limitativas da profundidade da cadeia de delegação, permite uma granularidade mais precisa na redistribuição e governo de direitos, podendo esta ser usada em cenários em que a distribuição possa até ser infinita. No MPEG-21 REL a delegação é manifestada por um elemento opcional da concessão: "*delegationControl"* (Rodriguez & Delgado, 2007a). Se o controlo por delegação ficar incluído na concessão ("*grant*"), o "*principal"* autorizado pela concessão pode emitir outra licença com a concessão a outro "*principal"*. Para poder delegar esta concessão a outro, o emissor tem de a possuir. No momento em que a licença é emitida, o privilégio de emissão deve estar na posse do emissor da licença concedendo-lhe esse direito, o que vem ao encontro do "*princípio de posse*".

Na abordagem aqui assumida, o objetivo consiste em delimitar os direitos emitidos pelo distribuidor, de modo a que a licença final esteja enquadrada pelos direitos do detentor de conteúdo e pelos vários distribuidores envolvidos na cadeia de distribuição. Esse enquadramento faz recurso de um mecanismo que iremos chamar de distribuição por delegação. Nesta abordagem, tal como no Capítulo 9, somente a licença gerada para emissão será avaliada com vista a decidir se os direitos podem ser transmitidos em concordância com as regras definidas na licença de distribuição progenitora. Caso esta licença seja compatível, então inicia-se o processo de emissão desta nova licença que irá ser embebida no objeto DID_L que contém a chave criptográfica que protege o conteúdo. Contendo este objeto a licença e a chave que desprotege o conteúdo, e sendo esta licença emitida pelo detentor do conteúdo ou por distribuidor autorizado, então o "*princípio de posse*" fica assegurado.

Mais uma vez a aplicação o mecanismo de validação de emissão de licença é assegurar que os direitos são transmitidos entre utilizadores finais preservnado a linha sucessória de direitos, simplificando ao mesmo tempo complexidade dos processos de emissão e gestão de licenças em soluções suportadas por certificados digitais X.509 (Morin, 2009), licenças certificado MPEG-21 REL (Yang et al., 2008; Sheppard & Safavi-Naini, 2006a), e de licenças agregadas (Sachan et al., 2010; Sans et al., 2007).

3.1 Distribuição de licenças com controlo da delegação de direitos

O fornecedor de conteúdos, ao interagir com o formulário de especificação de direitos do sistema DRM, seleciona o tipo de controlo de delegação que pretende e cria então a licença de

distribuição com os direitos de referência incorporados. Esta é a licença pai e a partir desta podem ser criadas outras licenças filho em que os direitos devem estar em concordância com a progenitora. Podendo ser retransmitida de forma encadeada, o número de níveis das licenças filho vai depender do tipo de delegação definida pelo detentor de conteúdo. Assim, ao criar uma licença com controlo por delegação, devem ter-se em conta os vários subtipos de licenciamento consoante o tipo de limitações ("*constraints")* ($D_{1...4}$) declaradas (Figura 95).

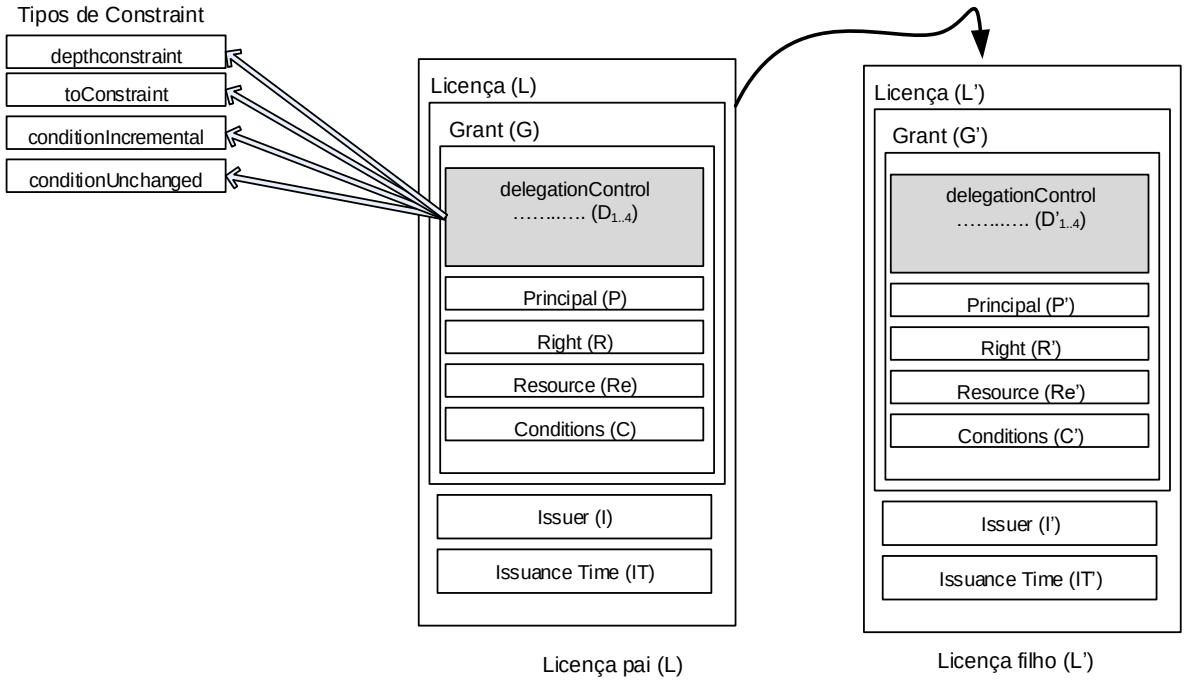


Figura 95 – Estrutura básica de licenças com controlo por delegação.

Na norma MPEG-21 REL uma licença que permita uma redistribuição infinita deve possuir uma concessão ("*grant"*) contendo o elemento "*delegationControl"* (Rodriguez & Delgado, 2007a). Este elemento vem permitir ao concessionado delegar direitos a terceiros noutra licença a emitir. Contudo, devem observar-se algumas regras na emissão de licenças, pois a licença filho, além de ter de possuir o elemento "*delegationControl"* compatível com o elemento idêntico (Figura 96) da licença pai, terá de, no mínimo, ser tão restritiva quanto a licença progenitora. Além disso, o emissor da licença pode impor restrições na delegação, de forma a controlar não só a profundidade da cadeia de delegação, mas também a quem a concessão pode ser delegada.

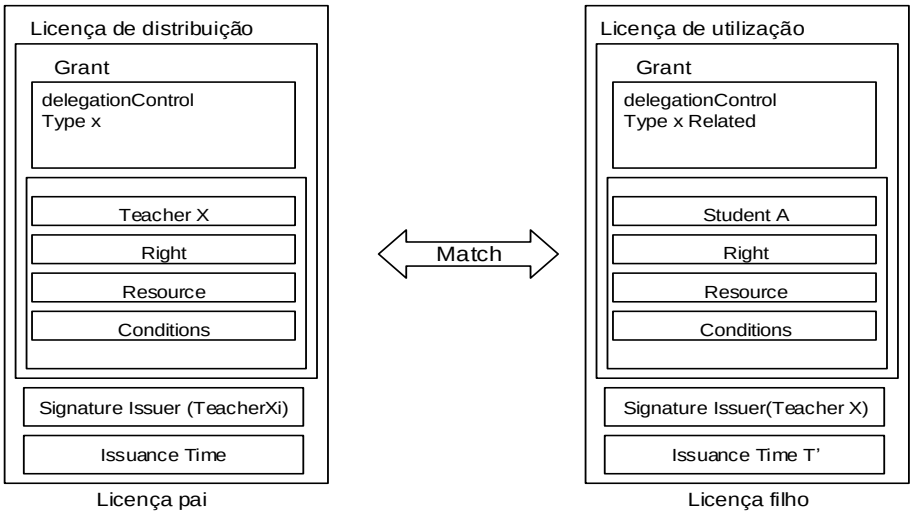


Figura 96 – Licenças pai/filho *delegationControl*

A nossa proposta apresenta uma solução para a validação de direitos concedidos entre utilizadores através da funcionalidade de controlo por delegação baseada na norma MPEG-21 REL. Através do elemento "*delegationControl"* da norma MPEG-21 REL, é possível aplicar várias formas de delegação através da declaração de limitações ("*constraints"*) inerentes à norma (Thomas et al., 2009). As principais formas de limitação a considerar na especificação MPEG21- REL são: "*Condition Incremental", "ConditionUnchanged", "DepthConstraint" e "ToConstraint"* ($D_{1...4}$).

Sendo o número de exemplos práticos de aplicação bastante vasto e dependendo das situações e do tipo de limitação ("*constraint"*) aplicada no decorrer da transmissão de direitos, iremos focalizar-nos em algumas situações correntes em que a delegação de direitos é usual entre utilizadores. O seguinte exemplo demonstra a utilização do elemento "*delegationControl"* aplicando a limitação ("*constraint") "conditionUnchanged"* na situação em que um Professor pretende que os seus alunos utilizem determinado conteúdo e o possam distribuir entre si. Esta limitação requer que as condições a quem foi delegada a licença permaneçam idênticas às do emissor. Um extrato exemplificativo da licença emitida pelo Professor pode ser o seguinte (Figura 97):

```
<r:license...>
…
<r:keyHolder>...Aluno A...</r:keyHolder>
 <r:grant>
    <r:delegationControl>
       <r:conditionUnchanged/>
    </r:delegationControl>
```

```
    <r:keyHolder>...Aluno B...</r:keyHolder>
    <mx:play/>
    <mx:diReference>urn:example:pdf123</mx:diReference>
    <r:validityInterval>..2014/15 ...</r:validityInterval>
   </r:grant>
   <r:issuer>
      <dsig:Signature>
            <dsig:SignedInfo>...</dsig:SignedInfo>
            <dsig:SignatureValue>…</dsig:SignatureValue>
            <dsig:KeyInfo>...Professor A...</dsig:KeyInfo>
             <details>
                   <timeOfIssue>2014-10-01T01:25:00</timeOfIssue>
             </details>
      </dsig:Signature>
   </r:issuer>
…
</r:license>
```

Figura 97 – Exemplo de licença pai para *conditionUnchanged*

Neste exemplo, o Professor A permite ao Aluno B visualizar um ficheiro PDF durante o ano letivo de 2014/2015. Estando o elemento "*delegationControl"* presente, tal significa que o Aluno B pode emitir uma licença estruturalmente idêntica à que recebeu para outros utilizadores e estes, por sua vez, também o poderão fazer de forma encadeada. Apresenta-se de seguida um extrato de uma licença emitida para um Aluno C (Figura 98), podendo este emitir mais licenças limitadas obviamente aos termos da licença progenitora.

```
<r:license...>
…
<r:keyHolder>...Aluno B...</r:keyHolder>
 <r:grant>
      <r:delegationControl>
            <r:conditionUnchanged/>
      </r:delegationControl>
      <r:keyHolder>...Aluno C...</r:keyHolder>
      <mx:play/>
      <mx:diReference>
      <mx:identifier>urn:example:pdf123</mx:identifier>
      </mx:diReference>
      <r:validityInterval>
```

```
            <r:notBefore>2014-01-01T00:00:00</r:notBefore>
            <r:notAfter>2015-01-01T00:00:00</r:notAfter>
      </r:validityInterval>
</r:grant>
<r:issuer>
    <dsig:Signature>
      <dsig:SignedInfo>...</dsig:SignedInfo>
      <dsig:SignatureValue>…</dsig:SignatureValue>
      <dsig:KeyInfo>...Aluno A...</dsig:KeyInfo>
            <details>
                  <timeOfIssue>2014-10-02T01:25:00</timeOfIssue>
            </details>
     </dsig:Signature>
</r:issuer>
…
</r:license>
```

Figura 98 - Exemplo de licença filho para *conditionUnchanged*

A limitação imposta por "*conditionUnchanged*", podendo levar a uma distribuição infinita entre os utilizadores que obedeçam às condições, torna imperativa a validação da licença a emitir, de modo a que o pedido do requerente satisfaça os critérios de elegibilidade dentro do domínio académico.

3.2 Validação da distribuição de licença por controlo de delegação de direitos

O mecanismo proposto, ao permitir que a emissão de licença com controlo por delegação de direitos seja validada, faz com que não só a elegibilidade do requerente seja confirmada, mas também se este obedece às condições do detentor. Neste mecanismo a licença só será validada pelo mecanismo de controlo de delegação quando um dos quatro elementos de limitação da "*delegationControl" ($D1_{…4}$)* estiverem presentes no elemento "*grant*" G($D1_{…4}$), da licença pai (Figura 99). Aplicando os algoritmos de (Rodriguez & Delgado, 2007a), adaptados ao mecanismo de validação este deve ter em conta a verificação da seguinte regra principal:

a) $G(D_{1…4})$ = (*toConstrain* ou *ConditionIncremental* ou *conditionUnchanged*, ou *depthconstraint*)

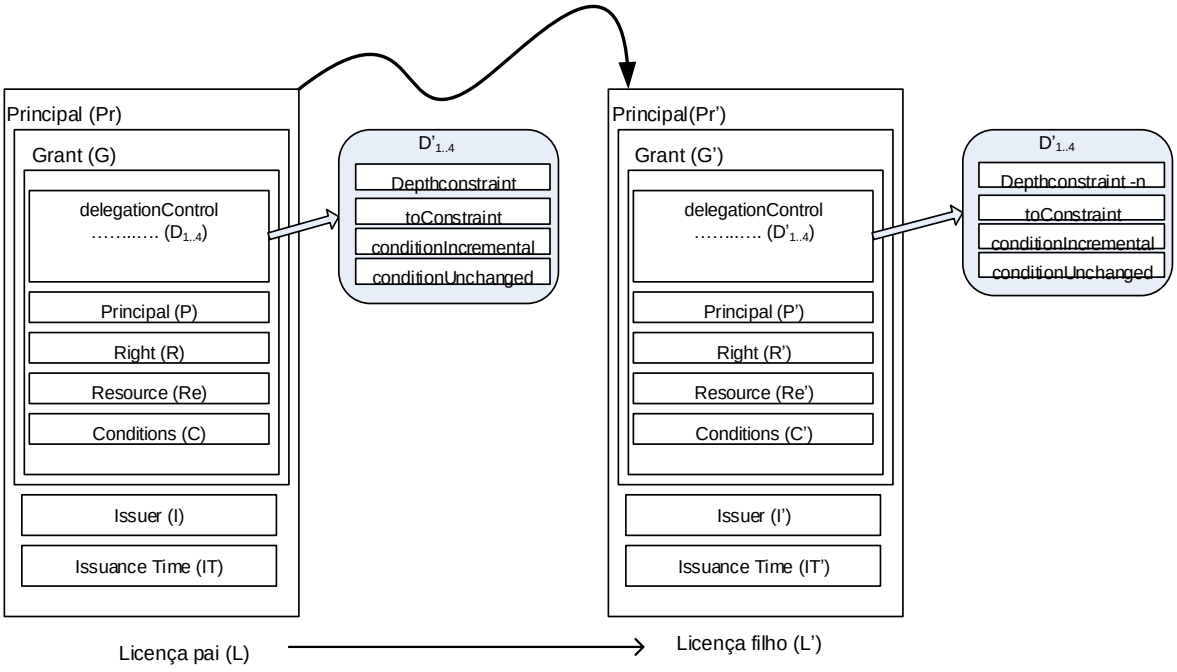


Figura 99 – Licenças pai/filho por controlo de delegação de direitos

Além disso, as seguintes regras também devem ser cumpridas:

1. Se o elemento "*toConstraint"* existir no "*delegationControl"* da licença pai, então o elemento "*principal"* da licença filho é permitido no controlo de delegação se obedecer à restrição definida em "*toConstraint*". Caso não exista, então pode ser qualquer um;

$$IF\ G(DtoConstraint) = True\ -> G'(P') = Allow$$

2. Se o elemento "*conditionUnchanged"* existir no "*delegationControl"* da licença pai, então as condições da licença filho permanecem iguais às da licença pai;

$$IF\ G(DconditionUnchanged) = True\ -> G'(C') = G(C)$$

3. Se o elemento "*conditionIncremental"* existir no "*delegationControl"* da licença pai, então as condições da licença filho são, no mínimo, idênticas às condições da licença pai;

$$IF\ G(DconditionIncremental) = True\ -> G'(C') >= G(C)$$

4. Se o elemento "*depthConstraint"* existir no "*delegationControl"* da licença pai e o seu valor for maior que zero, então o elemento "*depthConstraint"* na licença filho é reduzido de uma unidade (pelo menos),

$$IF\ [G(DdepthConstraint) = True \wedge G(DdepthConstraint(count) > 0] -> G'(D'depthConstraint - n)$$

5. O elemento "*right"* na licença filho é o mesmo da licença pai;

$$G'(R') = G(R) -> TRUE$$

6. O elemento "*resource*" da licença filho é igual ao elemento "*resource*" da licença pai;

$$G(Re') = G(Re) -> TRUE$$

7. O controlo da delegação da licença pai permite que as condições existam na licença filho se:

   O elemento "*toConstraint*" existir na licença pai;

   $$G'\ (C') = allow\ IF\ G(DtoConstraint) = True$$

   Tal implica que as condições da licença pai estejam sempre presentes na licença filho (G'(C')>= G(C)) e que o "*principal"* da licença filho seja permitido na delegação por controlo de direitos da licença pai da seguinte forma:

   Se o elemento "*principal"* na licença pai existir no elemento "*toConstraint"* então é igual ou engloba o elemento "*principal"* da licença filho.

8. O elemento emissor da licença filho (I') é igual ao elemento "*principal"* na licença pai;

   $$I' = (Pr) -> True$$

9. A data/hora de emissão da licença filho tem um valor posterior da data/hora de emissão da licença pai;

   $$Valor\ (IT'\ ) > valor\ (IT) -> True$$

3.2.1 Aplicação de regras de validação

A aplicação destas regras no exemplo anteriormente mencionado, em que o Professor emite uma licença aos seus Alunos e estes, por sua vez, a distribuem entre si (Figura 100), permite aplicar o mecanismo de controlo de delegação com concessão sem alterações ("*conditionUnchanged"*) com validação positiva das regras para a transmissão de direitos entre Professor $A->$ Aluno A, e entre Aluno A $->$ Aluno B.

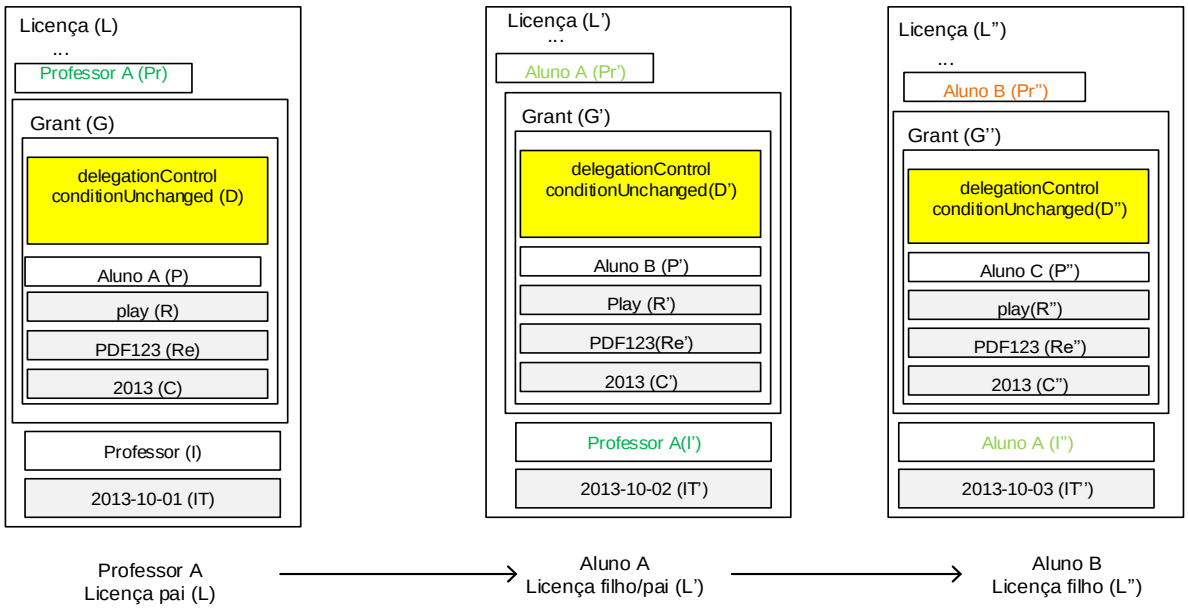


Figura 100 – Licenciamento com delegação de direitos sem alteração de condições

Transmissão: Licença pai (L) /(Professor A) $->$ Licença filho/pai (L') /(Aluno A)

a) $G(D1..4) = G(DconditionUnchanged) -> TRUE,$

1. não aplicável,
2. $IF\ [G(DconditionUnchanged) = True -> G'(C') = G(C) -> TRUE,$
3. não aplicável,
4. não aplicável,
5. $G'(R'\ play) = G(Rplay) -> TRUE,$
6. $G(Re'\ pdf123) = G(Re\ pdf123) -> TRUE,$
7. não aplicável,
8. $I' = Pr -> TRUE,$
9. $IT' > IT -> TRUE,$

Transmissão: Licença filho/pai (L') / (Aluno A) $->$ Licença filho (L'')(Aluno B)

> As mesmas regras são também cumpridas nesta situação e também quando o aluno B transmite os seus direitos para um Aluno C e devem ser verificadas sucessivamente.

Um outro caso de aplicação do mecanismo de controlo de delegação ("*delegationControl"*) na concessão de direitos pode ser exemplificado na situação em que o fornecedor de conteúdo (Professor) autoriza a editora da Universidade a emitir uma licença, concede-lhe o direito de delegar aos utilizadores o direito de visualizar um ficheiro PDF, de acordo com as condições por ele definidas. O Professor atua como um fornecedor de conteúdos permitindo ao distribuidor (a editora) emitir uma licença aos utilizadores (alunos) em que lhes concede o direito de poder visualizar o ficheiro PDF durante um ano e de estes poderem redistribuir a licença somente uma única vez. Ou seja, à editora ("*principal"*), na posse da licença de distribuição, é concedido o direito de emitir licenças para os utilizadores concedendo-lhes o direito de visualizar ("*right"*) o ficheiro PDF ("*resource"*) durante um ano ("*condition"*), mantendo as mesmas condições. Contudo, a editora está limitada pela delegação atribuída a ser a única a emitir licenças aos utilizadores e estes só a podem redistribuir uma única vez entre si. Para se poder fazer vigorar essa limitação é utilizado o elemento "*depthconstraint"* de "*delegationControl"* para restringir a profundidade da cadeia de delegação só até ao aluno (*delegationControl = depthConstraint -1*) que já recebeu uma licença de utilização de outro aluno, evitando que este possa redistribuir a licença (Marques & Serrão, 2015a). Assim,

definindo um único nível de delegação de direitos, faz-se o controlo da profundidade de distribuição por delegação (Figura 101).

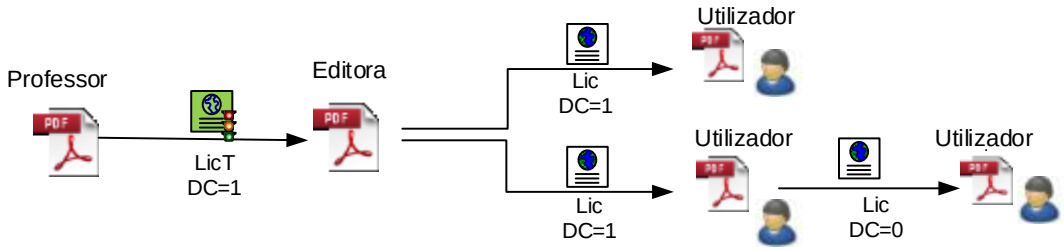


Figura 101 – Cenário de delegação controlada.

A licença de utilização emitida ao aluno final na cadeia contém uma concessão com o valor do elemento de controlo da delegação a zero, o que vai impedir a sua redistribuição (Figura 102).

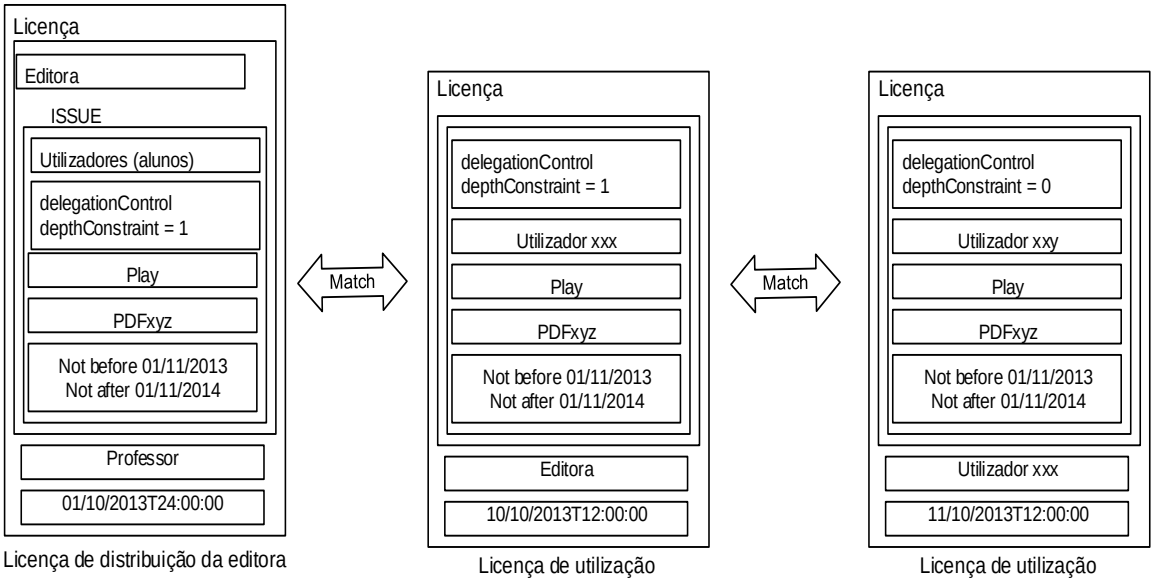


Figura 102 – Transmissão de direitos e controlo de níveis na delegação

A licença de distribuição da editora (Figura 103) contém os seguintes elementos:

```
<r:license...>
   <r:grant>
    <r:forAll varName="alunos"/>
      <r:forAll varName="ano">
            <r:anXmlExpression>2013<r:anXmlExpression>
      </r:forAll>
      <r:keyHolder>…Editora…</r:keyHolder>
      <r:issue/>
            <r:grant licPartId==”ReUsageGrant”>
          <r:keyHolder varRef=”alunos”/>
          <r:keyHolder varRef=”ano”/>
```

```
                <r:delegationControl>
                        <r:depthConstraint>
                           <count>1</count>
                        </r:depthConstraint>
                    </r:delegationControl>
              <mx:play/>
              <mx:diReference>urn:example:pdf123</mx:diReference>
              <r:validityInterval varRef="ano"/>
                </r:grant>
    </r:grant>
    <r:issuer>
       <dsig:Signature>
             <dsig:SignedInfo>...</dsig:SignedInfo>
             <dsig:SignatureValue>…</dsig:SignatureValue>
             <dsig:KeyInfo>...Professor A...</dsig:KeyInfo>
             <details>
                   <timeOfIssue>2013-10-01T01:25:00</timeOfIssue>
             </details>
       </dsig:Signature>
     </r:issuer>
</r:license>
```

Figura 103 – Licença de distribuição da editora

A licença de utilização (Figura 104) para o aluno contém os seguintes elementos:

```
</r:license>
<r:grant>
   <r:keyHolder>
       <r:info>
       <dsig:KeyValue>
             <dsig:RSAKeyValue>
                   <dsig:Modulus>…Aluno X…=</dsig:Modulus>
                   <dsig:Exponent>…</dsig:Exponent>
             </dsig:RSAKeyValue>
       </dsig:KeyValue>
       </r:info>
    </r:keyHolder>
    <mx:play/>
    <mx:diReference>
       <mx:identifier>urn:example:PDFxyz</mx:identifier>
```

```
    </mx:diReference>
    <r:validityInterval>
       <r:notBefore>2013-01-01T00:00:00</r:notBefore>
       <r:notAfter>2014-12-01T00:00:00</r:notAfter>
    </r:validityInterval>
   <r:forAll varName="alunos"/>
   <r:forAll varName="ano">
        <r:anXmlExpression>2013<r:anXmlExpression>
   </r:forAll>
          <r:grant licPartId=="ReUsageGrant">
                <r:delegationControl>
                        <r:depthConstraint>
                           <count>1</count>
                        </r:depthConstraint>
                   </r:delegationControl>
              <mx:play/>
              <mx:diReference>urn:example:pdf123</mx:diReference>
              <r:validityInterval varRef="ano"/>
             </r:grant>
</r:grant>
<r:issuer>
      <dsig:Signature>
            <dsig:SignedInfo>...</dsig:SignedInfo>
            <dsig:SignatureValue>…</dsig:SignatureValue>
            <dsig:KeyInfo>...Universidade...</dsig:KeyInfo>
            <details>
                  <timeOfIssue>2013-10-10T01:25:00</timeOfIssue>
            </details>
      </dsig:Signature>
     </r:issuer>
…
</r:license>
```

Figura 104 - A licença de utilização de aluno

Tal como anteriormente, o mecanismo de validação da distribuição será aplicado quando o utilizador fizer um pedido de emissão de licença ao LIS. Ao fazer o pedido, é verificada a elegibilidade do requerente e o LIS ativa o tipo de mecanismo adequado que vai verificar se é possível gerar a licença de acordo com os termos e condições especificados.

Numa primeira fase, é executada a validação das regras de distribuição por emissão ("*issue"*) de acordo com o mencionado no Capítulo 9. Caso exista validação positiva, dá seguimento à emissão da licença de utilização para o aluno requerente.

Numa segunda fase, se o aluno na posse desta licença de utilização receber um pedido de emissão de licença de outro utilizador, o mecanismo de validação valida as regras de distribuição por controlo de delegação:

a) validação da distribuição por controlo de delegação de direitos (*delegationControl*)

1. $$G(D1..4) = G(Ddepthconstraint) -> TRUE,$$
2. não aplicável
3. não aplicável
4. $$IF\ (G(DdepthConstraint) = TRUE \wedge G(DdepthConstraint(count)) > 0) = TRUE, -> DdepthConstraint(count)filho = DdepthConstraint(count)pai - 1$$
5. $$G'(R'play) = G(Rplay) -> TRUE,$$
6. $$G(Re'pdf_xyz) = G(Re\,pdf_xyz) -> TRUE,$$
7. não aplicável
8. $$I' = G(P) -> TRUE$$
9. $$IT' > IT -> TRUE$$

Neste caso de utilização, em que um aluno dá seguimento ao pedido de emissão de licença a outro utilizador, o valor de "<*count*>" diminui de uma unidade quando a licença é transmitida. Sempre que o utilizador que recebeu a licença de outro utilizador tenta emitir uma nova licença, a regra número quatro não é validada (o valor de "*depthConstraint*(*count*)" é nulo). Como o mecanismo só permite a geração da nova licença de utilização se todas as regras forem validadas, tal impede a geração de uma nova licença face ao pedido do outro utilizador. Por isso é invalidada a delegação de direitos e consequente emissão de licença. Se o valor de "*depthConstraint*(*count*)" fosse maior que zero, então o utilizador poderia emitir para outro utilizador uma licença estruturalmente semelhante à licença do progenitor. A profundidade da delegação vai assim depender do valor de "<*count*>" inicial, sendo este que determina o controlo do nível da delegação de direitos.

No ARMS, a interação entre o LIS e o SGA, quer na determinação da elegibilidade do utilizador quer na obtenção das variáveis necessárias ao mecanismo de distribuição da licença, é um dos aspetos mais importantes a considerar. A verificação perante o SGA é crucial para que o gerador de licenças faça a emissão quer da licença para os professores da unidade curricular X quer posteriormente para a distribuição da licença por delegação aos alunos (Figura 105), tendo sempre presente que o valor atribuído inicialmente ao elemento "<*count*>" irá determinar a profundidade da cadeia de distribuição. Quanto maior for este valor mais longa será a profundidade da cadeia.

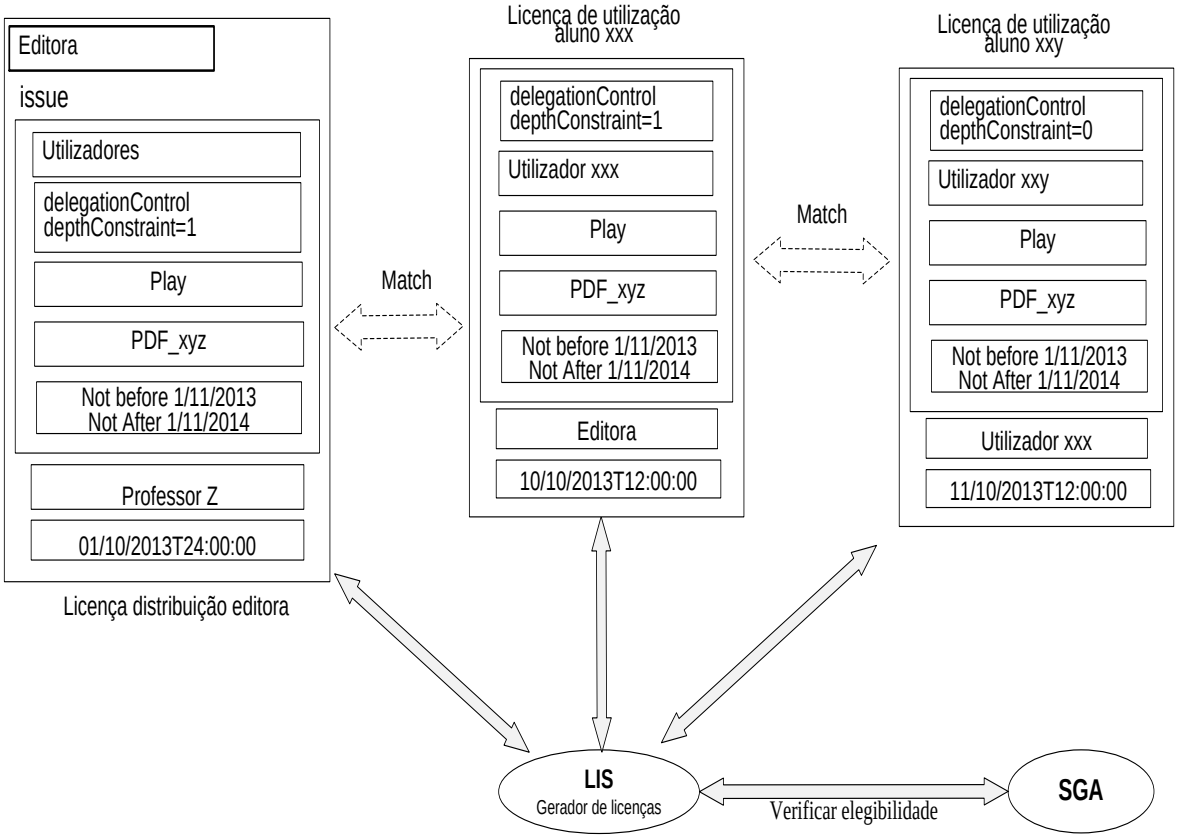


Figura 105 – Transmissão de licenças de distribuição e controlo de delegação de direitos

Alguns exemplos de licenciamento no meio académico onde se efetua o controlo de transmissão de direitos são apresentados no anexo A.

4 Processamento de licença

Na abordagem que foi seguida neste trabalho o componente que assegura e verifica a aplicação dos direitos é a aplicação cliente residente no dispositivo do utilizador. A licença e o conteúdo protegido estão embebidos num documento DID e são armazenados no dispositivo cliente.

Contudo, antes de a licença ser embebida no documento DID, um mecanismo de processamento de licenças é executado para verificar se as licenças são válidas face aos parâmetros XML definidos. Este mecanismo de processamento reside no lado servidor, mais precisamente no LIS, e é o responsável pela implementação das funcionalidades de gestão das licenças como a geração da licença a emitir, a interpretação, a validação e a revogação.

A geração de uma licença de utilização é completamente diferente da geração de uma licença de distribuição. Num caso, o fornecedor de conteúdo tem de lidar com as licenças modelo para gerar a licença de distribuição. No outro caso, o utilizador final deve lidar com as licenças de distribuição para gerar a licença de utilização, podendo então o tipo de controlo de distribuição embebido na licença ser diferente. O processo de validação da licença está intimamente relacionado com a licença de distribuição e a licença de utilização tal como foi referido anteriormente. O primeiro passo do processo verifica a elegibilidade do pedido de emissão da licença perante o SGA e, caso este seja legítimo, avança para a fase seguinte. A licença é então embebida no documento DID_L que contém a chave de proteção do conteúdo. Contudo, e para que esta chave seja reencriptada com a chave pública do novo utilizador recetor, o LIS dá início ao processo de reencriptação. Depois disso o utilizador que solicitou a licença pode então efetuar o seu descarregamento. Através da interação com o sistema DRM, em qualquer altura, o fornecedor de conteúdo também pode selecionar uma ferramenta adequada do LIS e verificar se as licenças filho armazenadas, idênticas às que já foram enviadas, são compatíveis com a licença pai correspondente à licença de distribuição.

Inicialmente assume-se que um utilizador obtém conteúdo sob a forma de um objeto conteúdo (DID_C) que fica armazenado no dispositivo cliente. Quando o utilizador realiza um pedido de emissão de licença para esse conteúdo, o dispositivo cliente verifica se a licença já existe internamente. Caso contrário, direciona o utilizador para o LIS correspondente e localiza a licença respetiva correspondente ao recurso. Se a licença for encontrada, então poderá prosseguir e descarregar o objeto licença (DID_L) correspondente e proceder ao consumo do conteúdo. Se a licença não for encontrada no LS, então o dispositivo cliente solicita a geração de uma nova licença.

Ao pedir uma licença perante o LIS, o utilizador ativa o mecanismo de geração de licenças, inserido num módulo específico residente no LIS (no ARMS é o ILM). É então inicializada uma procura pesquisando a base de dados pelo registo interno da licença que localiza a licença de distribuição para o recurso correspondente (se não a encontrar, o processo termina). Caso a

licença de distribuição seja encontrada, o módulo dá início ao processo de geração da licença para ser descarregada de acordo com as seguintes fases (Marques & Serrão, 2015a):

1 – Verificação da elegibilidade

Ao solicitar a criação de uma licença o utilizador interage com um formulário onde pode selecionar as condições predefinidas pelo detentor original do conteúdo através da licença modelo (no caso de uma licença de distribuição) ou predefinidas pelo distribuidor (no caso de uma licença de utilização) e envia o pedido para que seja autorizada a emissão de licença. Uma licença de utilização pode ser derivada de uma das licenças de distribuição armazenada no LIS ou de uma licença de utilização onde haja uma concessão de direitos de distribuição de licença. Face a um pedido de emissão de licença o módulo gerador de licenças residente no LIS verifica se o requerente é membro da comunidade, consultando o SGA. Se a resposta for negativa, o processo termina. Se resposta obtida for positiva, então dá-se início à procura da licença de distribuição no LIS. Caso esta seja localizada, é realizado um conjunto de pesquisas dinâmicas sobre a licença de distribuição que extrai os seus elementos principais com vista a gerar a licença temporária de utilização. Esta licença será gerada em conformidade com o tipo de concessão de direitos definidos na licença de distribuição: com o elemento "*issue*" ou com o elemento " *delegationControl*". Após este passo passa-se para a fase seguinte, a validação de licenças, que, por sua vez, se pode subdividir em duas: a validação da licença de distribuição e a validação da licença gerada.

2 -Validação de licenças

2a - Validação da licença de distribuição

Antes de a licença ser gerada, a licença progenitora precisa de ser validada. Três das principais razões para considerar uma licença inválida são:

a) Estar malformada – quando a licença não obedece às especificações do modelo de dados ou se há permissões concedidas que não estão presentes no conjunto de permissões originais antecessoras associadas ao acordo;
b) As restrições na licença não são satisfeitas – quando a licença possui restrições aplicáveis ao seu todo que não são observadas (como, por exemplo, o limite de tempo, o número de vezes que o conteúdo pode ser reproduzido, entre outros);
c) Estado da licença inválido – quando a licença foi revogada ou o licenciador não tinha autorização para emitir licenças.

Para validar a licença progenitora o módulo residente no LIS procede então à verificação da validade da assinatura na licença de distribuição (o que permite assegurar a sua integridade e autenticidade), verificação se a licença está malformada (interpretando os elementos constituintes), verificação de restrições e verificação se a licença ainda está ativa (inspecionando as listas de revogação).

2b – Validação da licença de utilização

Com o resultado obtido, ao aplicar o conjunto de pesquisas dinâmicas sobre a licença de distribuição, é gerado um documento XML correspondente a uma licença temporária, contendo os termos e as condições associadas às concessões da licença progenitora. Pode-se assim validar a licença gerada aplicando o mecanismo de validação da distribuição de licenças adequado. Cada uma das validações é realizada comparando os elementos respetivos da licença progenitora e licença temporária e se estão de acordo com as respetivas regras consoante o tipo de distribuição de licença. Se estas validações se realizarem com sucesso, então avança-se para o passo seguinte.

3 - Armazenamento e envio de licença

O LS regista e armazena a licença na base de dados interna e dá início ao processo de criação do documento DID contendo embebida a nova licença gerada e a chave de proteção do conteúdo reencriptada com a chave pública do utilizador que efetuou o pedido. Esta base de dados interna funciona com o intuito de disponibilizar funcionalidades de armazenamento, pesquisa e obtenção de licenças usando a identificação única do recurso e utilizadores associados à licença. O LIS disponibiliza o documento DID para que o utilizador o possa descarregar para o dispositivo cliente. A Figura 106 descreve o processo referente ao licenciamento.

Resumidamente, pode-se dizer que após o passo de verificação da elegibilidade do utilizador, e independentemente do tipo de distribuição, as fases principais que fazem parte do processamento da licença para distribuição são as seguintes:

a) Os elementos da licença de distribuição são extraídos;
b) É criada uma licença XML temporária baseada nos elementos extraídos;
c) Os elementos da licença XML temporária são extraídos;
d) Inicia-se o processo de geração da licença de utilização para ser descarregada.

Deste modo pode-se garantir que através da aplicação do mecanismo de validação não só o utilizador pertence ao domínio académico, como também obedece às condições definidas pelo

detentor original do conteúdo, estando os seus direitos preservados ao longo da cadeia sucessória de transmissão.

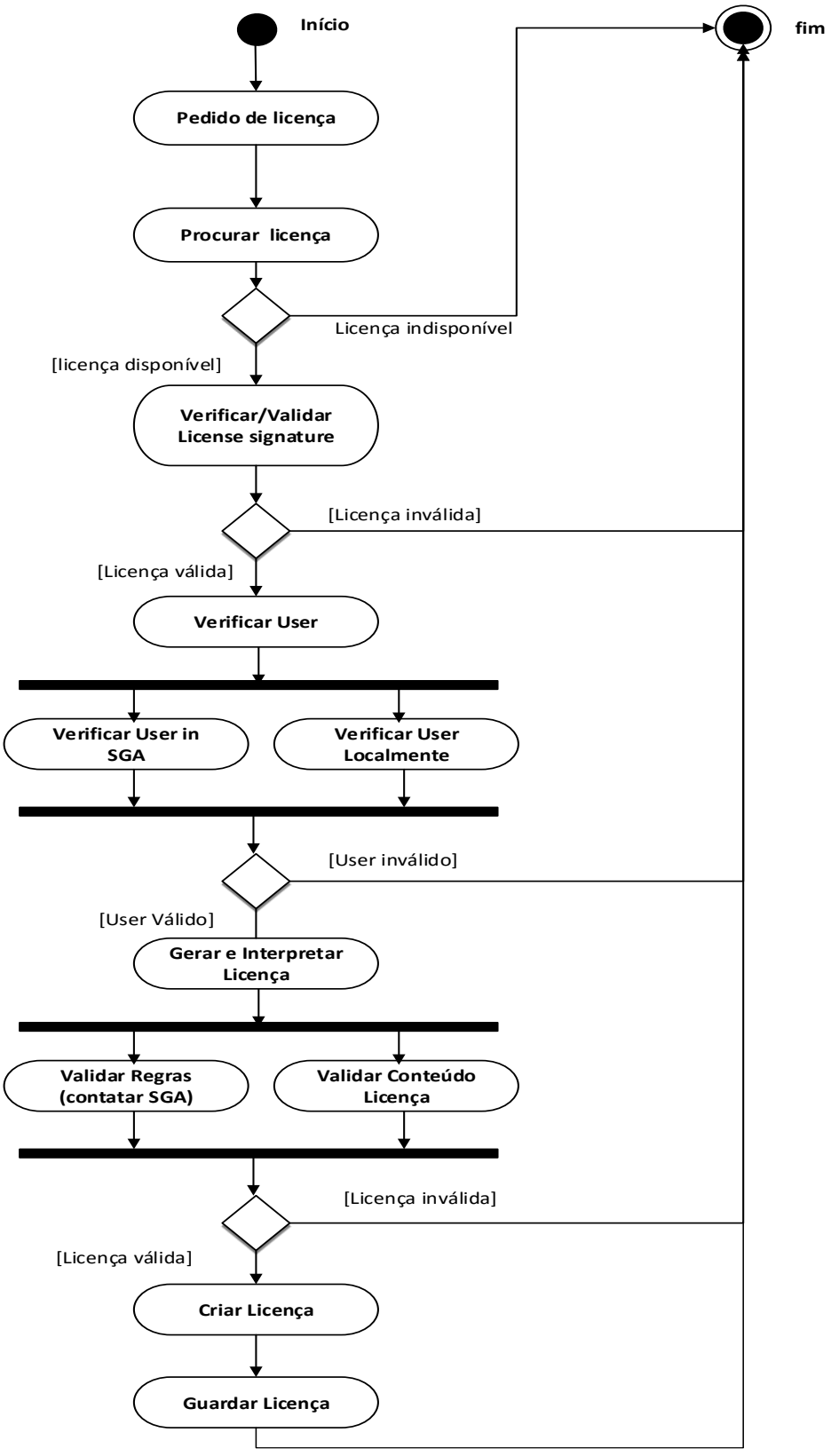


Figura 106 – Licenciamento: criação e obtenção de licenças

5 Conclusão

Os diferentes métodos de distribuição de licenças disponibilizados pelas normas MPEG-21, ao poderem adaptar-se às mais complexas situações, tornam necessária a aplicação de mecanismos de controlo sobre os direitos transmitidos nas licenças. A abordagem aqui seguida permite que esses diferentes tipos de licenciamento possam ser aplicados à proteção de conteúdos abrangidos por PI no contexto académico. Ao ser aqui apresentado mais um mecanismo de validação da distribuição de licença com controlo da profundidade da delegação de direitos, e de como pode ser utilizado no contexto educativo através da apresentação de casos de utilização, pretende-se demonstrar a viabilidade da integração da norma MPEG-21 em sistemas de DRM quando aplicados em ambiente académico. Este e o outro mecanismo anteriormente apresentado no capítulo nono têm por objetivo simplificar a automatização da gestão de direitos controlando quais os direitos transmitidos em vez de restringir as licenças emitidas pelos diferentes distribuidores ao longo da cadeia de distribuição. Estes mecanismos vêm assim viabilizar a superdistribuição de conteúdos contribuindo para uma melhor aceitação por parte dos intervenientes no fluxo de conteúdo e direitos associados.

A proposta aqui apresentada, em que se faz recurso à interação com o SGA via serviços *Web*, permite contornar os problemas relacionados com a complexidade da gestão adicional de credenciais no respeitante a certificados digitais X.509 (Morin, 2009), quer de licenças de certificação de membro MPEG-21 (Yang, et. al., 2008; Sheppard J., et. al., 2006), quer de licenças agregadas (Sachan et al., 2010).

A incorporação do SGA, além de diminuir a complexidade da gestão associada aos diversos papeis dos intervenientes na cadeia de distribuição, permite a integração do módulo de geração de licenças de forma transparente no sistema DRM com as vantagens inerentes ao nível de coordenação, interoperabilidade, privacidade e segurança (Kwok & Chi, 2006), simplificando a emissão de licenças e consequente utilização dos conteúdos.

Ao permitir viabilizar a validação da emissão da licença para utilizadores num determinado domínio, consegue-se assim estabelecer uma maior granularidade sobre o controlo de direitos evitando as complexidades associadas à gestão de certificados comprovativos da pertença a um determinado domínio. Por outro lado, a implementação de mecanismos que fazem garantir o respeito dos direitos ao longo da linha sucessória vai ao encontro de uma das necessidades do criador em preservar os seus direitos a partir do instante que os transmite a terceiros. Estes mecanismos acabam por permitir um maior controlo dentro do domínio académico, pois a

transmissão de direitos passa a ser exclusivamente realizada entre os seus membros e nas condições especificadas originalmente.

Este capítulo é baseado nas publicações de Marques et al. (2015a) e Marques.& Serrão (2015c).

PARTE V

Conclusão e Investigação Futura

Capítulo 11

Conclusões e Contribuição Científica

Apesar do entusiamo provocado por algumas iniciativas no meio académico intencionadas à preservação de direitos de PI, como, por exemplo, o *Creative Commons***,** estas não podem garantir uma proteção completamente eficaz, pois são meramente descritivos dos direitos a transmitir. O DRM apresenta-se como a solução capaz de dar resposta a este problema, pois além de poder garantir a descrição destes direitos a serem transmitidos, permite assegurar a sua persistência através da implementação de medidas tecnológicas que asseguram a transmissão e vigência de forma correta de acordo com o estipulado pelo criador e/ou detentor do conteúdo. Contudo, a utilização destes sistemas no meio académico, não tendo merecido a devida atenção, tem sido bastante escassa, tendo resultado num certo desconforto e desconfiança perante este tipo de sistemas a que não são estranhos experiências menos bem-sucedidas com a exploração comercial de conteúdos. A isso não é alheia a reduzida literatura existente sobre o DRM no contexto em causa, o que se reflete na existência de vários sistemas e modelos orientados para uma vertente de exploração de conteúdos demasiado focados na implementação de modelos de negócio com uma estratégia eminentemente comercial.

A investigação orientou-se no sentido de encontrar uma resposta à problemática de "como efetuar a partilha de conteúdo em contexto académico através de um sistema de DRM baseado em normas internacionais, de forma a preservar os direitos de PI, nomeadamente a preservação dos direitos de autoria e o respeito pela integridade do conteúdo" e "como controlar a transmissão de direitos entre os participantes num sistema DRM preservando a linha sucessória de direitos". Centrando-se nesta questão foi possível dar-se respostas às questões iniciais da investigação, indicando não só os mecanismos que permitem a transmissão segura de licenças e os mecanismos de concessão controlada de direitos com respeito da linha sucessória, mas também dando resposta a outras questões relevantes como (a) saber a forma mais adequada de gerar as chaves de cifra/decifra de conteúdo de forma automatizada, (b) saber como proteger as licenças (ou objeto de direitos) que guardam as chaves de cifra/decifra do conteúdo, (c) saber qual a forma e o formato mais adequados para o "transporte" de conteúdos e licenças, (d) saber como se processa a

transmissão de direitos entre os vários intervenientes durante o ciclo de vida do conteúdo (e) saber como se pode verificar se as licenças emitidas são corretamente atribuídas relativamente aos direitos originais concessionados (f) saber como assegurar que as licenças geradas são atribuídas aos utilizadores legítimos elegíveis do domínio académico e (g) saber como assegurar a utilização dos conteúdos dentro desse domínio assegurando a linha sucessória de direitos.

No decorrer deste trabalho, e perante este contexto em que os sistemas DRM não estão especificamente orientados com modelos nem sistemas que permitissem a resolução das questões de investigação, a solução aqui proposta procura dar uma resposta. Nesse sentido foram identificadas as tecnologias e os principais intervenientes e necessidades sentidas, propôs-se um modelo generalista, o qual serviu de referência para a implementação de uma solução genérica de DRM para o contexto académico. Esta mesma solução, resultante de um processo iterativo de refinamento ao longo do tempo, assenta em dois pressupostos básicos no seu desenvolvimento:

- Suporte numa solução existente que se possa adaptar ao contexto académico.
- Suporte em normas internacionais suficientemente flexíveis para se poderem integrar com a solução anterior e no contexto em causa.

Com base nas suas características e funcionalidades, o OpenSDRM e a norma ISO 21001 (MPEG-21) foram aqui selecionados dando azo à implementação de um solução final, o ARMS, capaz de garantir não só a proteção de conteúdos e direitos, mas também de assegurar a transmissão dos mesmos através de uma forma neutra no que respeita ao seu formato. O ARMS, por ter particularidades únicas, permite estabelecer um ambiente controlado dentro do domíno educacional e académico, onde graças à interação com o SGA mecanismos de validação permitem controlar a emissão de licenças verificando a elegibilidade dos utilizadores como membros do domínio e se estes satisfazem as condições iniciais definidas pelo autor/detentor de direitos.

Independentemente das medidas tecnológicas de proteção aplicadas e do suporte fornecido pela norma MPEG-21, o ARMS, ao permitir controlar os utilizadores no domínio académico vem abrir portas a que este tipo de sistemas se possa vir a implementar neste meio. Para dar resposta à enorme variedade e complexidade de situações de preservação de direitos sentidos pelos principais intervenientes, a instituição académica pode adotar o modelo de negócio mais adequado definindo as regras básicas de utilização através de licenças modelo que o ARMS suporta. Ao longo deste trabalho

foram analisados vários métodos de concessão e delegação de direitos e mecanismos de controlo associados suportados pela norma MPEG-21 que se podem adaptar ao contexto educacional e académico, implementados no ARMS em módulos específicos que controlam a transmissão de direitos. A sua importância é inquestionável pois assim consegue-se dar o apoio necessário ao fenómeno transmissão de direitos na partilha do conteúdo e do seu controlo com vista a satisfazer os anseios de uma grande parte da comunidade académica e académico; ou seja preservar os direitos do autor/detentor de direitos sempre que estes são transmitidos a terceiros.

Com a implementação da solução foi possível perceber da aceitabilidade do sistema perante a comunidade académica. Algumas das críticas sobre o sistema em si relacionam-se com o reduzido leque de opções disponíveis para realizar a transmissão de direitos entre o fornecedor e utilizadores do meio académico. Contudo, esta é uma questão a ser explorada em situações mais realistas onde se poderão implementar variados e mais complexos modelos de negociação de conteúdos consoante as reais necessidades sentidas pelos principais intervenientes no ciclo de vida dos conteúdos abrangidos por PI da entidade académico.

O desenvolvimento desta tese contribui assim para o enriquecimento da reflexão científica em torno das questões relacionadas com a proteção de direitos de PI sobre conteúdos educacionais. Além da proposta de um modelo, foi possível definir uma forma de representar o conteúdo e direitos associados baseada em normas internacionais que permitem a sua transmissibilidade nas atuais infraestruturas de comunicação como a Internet. A adaptação de uma plataforma de DRM aberta ao contexto académico foi aqui tomada em consideração e colocada em destaque dando-se especial importância aos aspetos de proteção e transmissão de conteúdos e direitos tendo por base normas internacionais. Destaca-se a contribuição resultante da aplicação de mecanismos de controlo de transmissão de direitos que permitem controlar o processo de concessão de direitos na linha sucessória entre as partes envolvidas dentro do domínio académico. A aplicação destes mecanismos vem satisfazer os anseios do detentor no que se refere à garantia de preservação dos seus direitos, estabelecendo níveis aceitáveis de controlo e governo sempre que o conteúdo é partilhado.

A investigação decorrente desta tese deu lugar a uma publicação em revista e várias comunicações científicas internacionais que se passam a citar:

Marques, J., & Serrão, C. (2011). Academic Context and rights enforcement on knowledge based content. *ICERI2011 Proceedings*, 618-628.

Marques, J., Serrão, C. (2012a). Rights Management and Technological Protection Measures in Educational Field.In proceedings of the *11th European Conference on e-Learning*, 327

Marques, J. & Serrão C. (2012b, September). Technological protection measures on knowledge based content in academia. In proceedings of the *15th International Conference on Interactive Collaborative Learning (ICL)*, pp. 1-4. IEEE.

Marques, J., & Serrão, C. (2014). Improving user content privacy on social networks using rights management systems. In *Annals of telecommunications-annales des télécommunications*, *69*(1-2), 37-45.

Marques, J. & Serrão C. (2015a). ARMS – A new approach to control content sharing and rights distribution. In proceedings *7th Int. Conf. on Education and new Learning Technologies- Edulearn15*. pp 5597-5607. Barcelona.

Marques, J. & Serrão C. (2015b). Enabling Content and rights transmission in the Educational field with ARMS. In proceedings of *14th Int Conf. WWW/Internet 2015*, ICWI, Dublin.

Marques, J. & Serrão C. (2015c). Digital Rights in the Educational field - Mechanisms for licensing validation. In proceedings of *8th annual International Conference of Education, Research and Innovation –ICERI15*, Seville.

Marques, J., Serrão C. & Metrolho J. (2015). Content Related Rights Transmission with MPEG-21 in the Educational Field. In proceedings of the *14th European Conference on e-Learning, ECEL-2015*, London.

No decorrer da apresentação destas comunicações, a comunidade académica tem demonstrado um grande interesse, gerando debate e apresentando críticas normalmente bastante positivas. Contudo, é preciso estar consciente que a investigação foi realizada no contexto de caso de estudo devendo a sua generalização e aplicação prática ser tomada com as devidas precauções a outras realidades.

Em suma, pode-se afirmar que as perspetivas criadas pela implementação do sistema ARMS vão de encontro aos objetivos iniciais desta investigação, contribuindo para a exploração de novas formas de abordagem da resolução dos problemas sentidos no meio académico no que diz respeito à preservação de direitos de PI sobre conteúdos partilhados, nomeadamente os direitos de autoria e integridade do conteúdo. Ao abrir novos horizontes à expansão e aplicabilidade do modelo e da solução proposta no contexto académico, espera-se que esta tese possa contribuir para que este tipo de sistemas venham a ter maior aplicabilidade sendo objeto de uma maior atenção neste importante meio responsável pela disseminação de conhecimento.

Trabalho futuro

Apesar de existirem várias leis internacionais que protegem os interesses dos detentores de direitos sobre conteúdos (DMCA, 1998; DACA, 2000; EUCD, 2001), os sistemas de DRM, face à evolução tecnológica, nem sempre conseguem dar resposta a todas as solicitações. Embora coloquem à margem da lei formas de contornar os sistemas de DRM e tecnologias de proteção associadas, não são suficientemente dissuasoras e torna-se necessário aplicar formas de controlar e detetar possíveis violações. Ao mesmo tempo, é premente uma constante adaptação à mudança do paradigma que a tecnologia dos dispositivos móveis trazem na utilização do conteúdo e necessidades sentidas pelos utilizadores mesmo no meio académico. Assim, e relativamente a uma linha de continuidade da investigação, é possível vislumbrar possíveis caminhos que podem contribuir para a expansão deste tipo e sistemas, nomeadamente:

- Investigar a aplicação do ARMS na área dos dispositivos móveis;
  - como oportunidade a explorar são de citar as novas especificações MPEG-M (MPEG-M, 2013) e a sua aplicabilidade na área do DRM no contexto em causa.
- Investigar a aplicação de novas técnicas de reencriptação sem recorrer a *proxy;*
  - como oportunidade a explorar é de citar a aplicação das novas técnicas de reencriptação e de reassinatura que atualmente se encontram em desenvolvimento e que poderão ter aplicabilidade na área de DRM, nomeadamente no sistema ARMS.
- Investigar a implementação de novos mecanismos de rastreio de utilização de conteúdos;
  - como oportunidade a explorar é de citar a verificação da aplicabilidade das especificações MPEG-21 ER (MPEG-21:ER, 2006) no ARMS que permitem criar condições de monitorização de eventos relacionados com a utilização de conteúdos sob governo do DRM.
- Investigar a interoperabilidade com outras linguagens de expressão de direitos, nomeadamente a versão do ODRL mais recente.

Referências Bibliográficas

Abbadi, M. & Alawneh M. (2008, August). DRM domain authentication using electronic payment systems. In *Proceedings of the 10th international conference on Electronic commerce* (p. 17). ACM.

Abie, H. (2007). Frontiers of DRM knowledge and technology. *International Journal of Computer Science and Network Security*, *7*(1), 216-231.

Abie, H., Spilling, P., & Foyn, B. (2004). A distributed digital rights management model for secure information-distribution systems. *International Journal of Information Security*, *3*(2), 113-128.

AES – Advanced Encryption Standard (2001). Available from: http://csrc.nist.gov/ CryptoToolkit/aes/.

Alanazi, H., Zaidan, B. B., Zaidan, A. A., Jalab, H. A., Shabbir, M., & Al-Nabhani, Y. (2010). New comparative study between DES, 3DES and AES within nine factors. *arXiv preprint arXiv:1003.4085*.

Amit, S. (2012). Rights violation detection in multi-level digital rights management systems. Doctoral thesis, Nanyang Technological University, Singapore.

Anderson, B. F. (2009). Modern digital rights management methods. Doctoral dissertation. Worcester Polythecnical Institute. Retrieved from http://www.wpi.edu/Pubs/E-project/Available/E-project-051109135624/ unrestricted/modern_DRM_methods.pdf.

Angelides, C., & Agius, H. (Eds.). (2010). *The handbook of MPEG applications: standards in practice*. John Wiley & Sons.

Anido-Rifón, L. E., Fernández-Iglesias, M. J., Caeiro-Rodríguez, M., Santos-Gago, J. M., Llamas-Nistal, M., Sabucedo, L. Á., & Pérez, R. M. (2014). Standardization in computer-based education. *Computer Standards & Interfaces*, *36*(3), 604-625.

Arnab, A., & Hutchison, A. (2005). Requirement Analysis of Enterprise DRM Systems. In *ISSA* (pp. 1-14).

Ateniese, G., & Hohenberger, S. (2005, November). Proxy re-signatures: new definitions, algorithms, and applications. In *Proceedings of the 12th ACM conference on Computer and communications security* (pp. 310-319). ACM.

Ateniese, G., Fu K., Green M., Hohenberger S. (2005). Improved proxy re-encryption schemes with applications to secure distributed storage. In *IN NDSS*.

Banzato, M. (2012, September). Barriers to teacher educators seeking, creating and sharing open educational resources: An empirical study of the use of OER in education in Italy. In *Interactive Collaborative Learning (ICL), 2012 15th International Conference on* (pp. 1-6). IEEE.

Barhoush, M., Atwood, J. (2010). Requirements for enforcing digital rights management in multicast content distribution. *Telecommunication Systems,45*(1), 3-20.

Barik, N., & Karforma, S. (2012). Risks and remedies in e-learning system. *International Journal of Network Security & Its Applications, 4*(1), 51-59.

Barlas, C. (2006). Digital Rights Expression Languages (DRELs). *JISC Technology and Standards Watch, 6*(3), 1-42.

Bartel, M, Boyer J., Fox B., LaMacchia B., & Simon E. (2002, February) XML-signature syntax and processing. In D. Eastlake, J. Reagle, and D. Solo, editors, W3C Recommendation.

Bates, M., Loddington, S., Manuel, S., & Oppenheim, C. (2007). Attitudes to the rights and rewards for author contributions to repositories for teaching and learning. *Association for Learning Technology Journal, 15*(1), 67-82.

Bekaert, J., Hochstenbach P., & Van de Sompel H. (2003). Using MPEG-21 DIDL to represent complex digital objects in the Los Alamos National Laboratory Digital Library. *D-Lib Magazine*, *9*(11).

Bekaert, J., De Kooning, E., & Van de Sompel, H. (2006). *Representing digital assets using MPEG-21 Digital Item Declaration*. International Journal on Digital Libraries, *6*(2), 159-173.

Bekaert, J., De Kooning, E., & Van de Walle, R. (2005). Packaging models for the storage and distribution of complex digital objects in archival information systems: a review of MPEG-21 DID principles. *Multimedia Systems*, *10*(4), 286-301.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS quarterly*, 369-386

Blanchi, C., & Petrone, J. (2001). An Architecture for Digital Object Typing.*Corporation for National Research Initiatives. Reston, Virginia*.

Blaze, M., Bleumer, G., & Strauss, M. (1998). Divertible protocols and atomic proxy cryptography. In *Advances in Cryptology—EUROCRYPT'98* (pp. 127-144). Springer Berlin Heidelberg.

Bretag, T. (2013). Challenges in addressing plagiarism in education. PLoS Med 10(12): e1001574.

Brown, A., Fox, B., Hada, S., LaMacchia, B., & Maruyama, H. (2001). SOAP security extensions: Digital signature. Retrieved from http://www.w3.org/TR/SOAP-dsig.

Buhse, W., van der Meer J. (2007). The Open Mobile Alliance Digital Rights Management [Standards in a Nutshell]. *Signal Processing Magazine, IEEE*,*24*(1), 140-143.

Burnett, I., Davis S., Drury M. (2005). MPEG-21 digital item declaration and Identification-principles and compression. *Multimedia, IEEE Transactions on*, *7*(3), 400-407.

Buyens, K., Michiels, S., & Joosen, W. (2007, January). "A software architecture to facilitate the creation of DRM systems." *In 4th IEEE Consumer Communications and Networking Conference (CCNC 2007).* (Vol. 4, pp. 955-959).

Camp, L. J. (2003). First principles of copyright for DRM design. *Internet Computing, IEEE*, *7*(3), 59-65.

Campidoglio, M., Frattolillo, F., & Landolfi, F. (2008). Security and privacy in *Web*-oriented watermarking protocols. In *Proc. 10th Int. Conf. on the Social and Ethical Impacts of Information and Communication Technology*.

Campidoglio, M., Frattolillo F., & Landolfi F. (2009, May). The copyright protection problem: Challenges and suggestions. In *Internet and Web Applications and Services, 2009. ICIW'09. Fourth International Conference on* (pp. 522-526). IEEE.

Cappaert, J., Preneel, B., Anckaert, B., Madou, M., & De Bosschere, K. (2008). Towards tamper resistant code encryption: Practice and experience. In *Information Security Practice and Experience* (pp. 86-100). Springer Berlin Heidelberg.

Castelluccia, C., Francillon, A., Perito, D., & Soriente, C. (2009). On the difficulty of software-based attestation of embedded devices. In *Proceedings of the 16th ACM conference on Computer and communications security* (pp. 400-409). ACM.

Castro, D. (2011, Feb.) "*Targeting Websites Dedicated To Stealing American Intellectual Property*". www.itif.org/files/2011-coica-testimony.pdf

Chaudhuri, S. K. (2007). Digital rights management: a technological measure for copyright protection and its possible impacts on libraries. *Modernisation of libraries: a challenge in digital era*.

Cheng, S., Rambhia, A. (2003). DRM and Standardization–Can DRM Be Standardized?. In *Digital rights management* (pp. 162-177). Springer Berlin Heidelberg.

Cheung, S., Curreem, H. (2002). Rights protection for digital contents redistribution over the Internet. In *Computer Software and Applications Conference, 2002. COMPSAC 2002. Proceedings. 26th Annual International* (pp. 105-110). IEEE.

Chiariglioni, F. (2008). "Technologies and platform to manage rights and value of digital media", PhD dissertation, Universita Degli Studi di Firenzi, Italy

Cisco VNI. (2014) - Cisco Visual Networking Index: Forecast and Methodology, 2013-2018. 2014. Retrieved from http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.pdf.

Cohen, J. E. (2003). DRM and Privacy. *Communications of the ACM*, *46*(4), 46-49.

Collier, G., & Robson, R. (2004). Digital Rights Management for Research and Education. *Macquarie E-learning Centre of Excellence White Paper*.

Collier, G., Piccariello H., Robson R. (2004a). "Digital Rights Management: An Ecosystem Model and Scenarios for Higher Education", *EDUCAUSE Center for Applied Research*, Research Bulletin, Issue 21.

Collier, G., Piccariello H., Robson R. (2004b). "Digital Rights Management: Tools and Applications for Implementing DMR in a Digital Ecosystem", *EDUCAUSE Center for Applied Research*, Research Bulletin, Issue 22.

Conrado, C., Kamperman, F., Schrijen, G. J., & Jonker, W. (2003, September). Privacy in an Identity-based DRM System. In *Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on* (pp. 389-395). IEEE.

Cooper, A., Martin A. (2006, October). Towards an open, trusted digital rights management platform. In *Proceedings of the ACM workshop on Digital rights management* (pp. 79-88). ACM.

Cox, I., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2007). *Digital watermarking and steganography*. Morgan Kaufmann.

Coyle, K., (2003). The technology of rights: Digital rights management. *Berkeley Technology Law Journal*, vol. 12, no. 1, pp. 1–20.

DACA. Copyright Amendment (Digital Agenda) Act 2000 (2000). Australian Governement Commonlaw. Retrieved from https://www.comlaw.gov.au/Details/C2004C01235/Download.

DCMI, (2013a). DCMI. Dublin core specifications. Retrieved from http://dublincore.org/specifications/

DCMI, (2013b). DCMI. Dublin core element set. Retrieved from: http://dublincore.org/documents/dces/.

Delgado, J., Llorente S., Rodriguez E. (2012, January). Digital rights and privacy policies management as a service. In *Consumer Communications and Networking Conference (CCNC), 2012 IEEE* (pp. 527-531).

Delgado, J., Torres, V., Llorente, S., & Rodríguez, E. (2011). Rights management in architectures for distributed multimedia content applications. In *Trustworthy Internet* (pp. 335-347). Springer Milan.

Delgado, J., Torres V., Llorente S., Rodríguez, E. (2005a, January). Rights and trust in multimedia information management. In *Communications and Multimedia Security* (pp. 55-64). Springer Berlin Heidelberg.

Delgado, J., Prados J., Rodríguez, E. (2005b). A new Approach for Interoperability between ODRL and MPEG-21 REL. In *Proc. 2nd Intl. ODRL Workshop*

Dhamija, R., & Wallenberg, F. (2003, August). A framework for evaluating digital rights management proposals. In *International Mobile IPR Workshop: Rights Management OF Information Products ON THE Mobile Internet* (p. 13).

Diaz, V., (2009) Intellectual Property Policies, e-learning, and *Web* 2.0: intersections and open questions". EDUCAUSE Center for Analysis and Research (ECAR), Research Bulletins, vol. 2009 issue 7. Retrieved from http://net.educause.edu/ir/library/pdf/ERB0907.pdf.

Diehl, E. (2012*), Securing Digital Video - Techniques for DRM and Content Protection*, Springer.

Diehl, E. (2008), October. A four-layer model for security of digital rights management. In *Proceedings of the 8th ACM workshop on Digital rights management* (pp. 19-28). ACM.

DMAG - Distributed Multimedia Applications Group. (n.d.). Retrieved September 25, 2015.

DMCA. The digital millenium copyright act of 1998 (1998). Retrieved from http://www.cisco.com/.

DMP. Digital Media project. http://www.dmpf.org/

Doërr, G., & Kalker, T. (2008, October). Design rules for interoperable domains: controlling content dilution and content sharing. In *Proceedings of the 8th ACM workshop on Digital rights management* (pp. 39-50). ACM.

DOI, International DOI foundation (IDF), www.doi.org.

DReAM. https://dream.dev.java.net/.

Dukhi, R. (2011, April). Watermarking: A copyright protection tool. In *Electronics Computer Technology (ICECT), 2011 3rd International Conference on* (Vol. 5, pp. 36-41). IEEE.

Dutta, R., Mukhopadhyay S., Dowling T. (2009, August). Key management in multi-distributor based DRM system with mobile clients using IBE. In*Applications of Digital Information and Web Technologies, 2009. ICADIWT'09. Second International Conference on the* (pp. 597-602). IEEE.

Earnings, A. (2014). July 2014. Author Earnings Report, Retrieved from http://authorearnings.com/report/july-2014-author-earnings-report/.

Erickson, J. S. (2003). Fair use, DRM, and trusted computing. *Communications of the ACM*, *46*(4), 34-39.

Etinger, D., Vitasović, A., & Šehanović, J. (2009). Digital Rights Management potentials and knowledge sharing in higher education. *Znanstvena konferenca z mednarodno udeležbo: Management, izobraževanje in turizem-kreativno v spremembe*.

EUCD. (2001). "Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society" Retrieved from http://eurlex.europa.eu/LexUriServ/ LexUriServ.do?uri=CELEX:32001L0029:EN:HTML

Favale, M. (2014). Death and resurrection of copyright between law and technology. *Information & Communications Technology Law*, *23*(2), 117-135.

Feigenbaum, J., Freedman, M. J., Sander, T., & Shostack, A. (2002). Privacy engineering for digital rights management systems. In *Security and Privacy in Digital Rights Management* (pp. 76-105). Springer Berlin Heidelberg.

Felten, E. W. (2003). A skeptical view of DRM and fair use. *Communications of the ACM*, *46*(4), 56-59.

Felten, E., (2003). Understanding trusted computing: will its benefits outweigh its drawbacks?. *Security & Privacy, IEEE*, *1*(3), 60-62.

Fernando, G., Jacobs, T., & Swaminathan, V. (2005). Project dream: an architectural overview. *Sun Microsystems White Paper*.

Fragopoulos, A., Gialelis J., Serpanos D. (2009, March). Adaptive DRM framework in user-converged multimedia ecosystems, utilizing MPEG-21 semantics. In *Autonomous Decentralized Systems*, 2009. ISADS'09. International Symposium on (pp. 1-6). IEEE.

Francillon, A., Nguyen Q., Rasmussen K. B., Tsudik G. (2014, March). A minimalist approach to remote attestation. In *Proceedings of the conference on Design, Automation & Test in Europe* (p. 244). European Design and Automation Association.

Gadd, E., Oppenheim, C., & Probets, S. (2003a). RoMEO Studies 2: How academics want to protect their open-access research papers. *Journal of information science*, *29*(5), 333-356.

Gadd, E., Oppenheim, C., & Probets, S. (2003b). Romeo Studies 3 How Academics Expect to Use Open access Research Papers. *Journal of Librarianship and Information Science*, *35*(3), 171-187.

Gadd, E., Loddington S., Oppenheim C. (2007). A comparison of academics' attitudes towards the rights protection of their research and teaching materials. *Journal of Information Science*.

Gayathri, K. S., Thomas, T., & Jayasudha, J. (2012). Security issues of media sharing in social cloud. *Procedia Engineering*, *38*, 3806-3815.

González, G., & Gil R. (2008). Semantic copyright management for internet-wide knowledge sharing and reuse. *Online Information Review*, *32*(5), 585-595.

Grzonkowski, S. (2010). A privacy-enhanced usage control model. Doctoral dissertation, National University of Ireland, Galway.

Guang-yuan, S., & Bei, G. (2013, January). A TPM-Based Protection Mechanism for Remote Attestation Evidence. In *2012 International Conference on Information Technology and Management Science (ICITMS 2012) Proceedings* (pp. 509-520). Springer Berlin Heidelberg

Guibault, L., Angelopoulos C. (Eds.) (2011). Open content licensing: from theory to practice. *Amsterdam University Press.*

Hahn, K., Lowry, C., Lynch, C., Shulenberger, D., & Vaughn, J. (2009). The University's Role in the Dissemination of Research and Scholarship--A Call to Action. *Association of American Universities*.

Halpin, J., Kelso K., (2010). "Digital Content & Learning Management Systems. *Converge Special report, issue 4*, Center for Digital Education. Retrieved from:

http://usa.canon.com/CUSA/assets/app/pdf/education_sales/Converge_2010SPECIALREPORT_Q4.pdf.

Hess, L., (2001). Engineering & Programming Project. Retrieved from http://www.sciencebuddies. org/science-fair-projects/project_engineering.shtm

Hietanen, H. & DeRosnay M., (2006, May). Legal Metadata for Semantic *Web* Applications. In *Symposium on Digital Semantic Content across Cultures*.

Horne, B., Matheson, L., Sheehan, C., & Tarjan, R. E. (2002). Dynamic self-checking techniques for improved tamper resistance. In *Security and privacy in digital rights management* (pp. 141-159). Springer Berlin Heidelberg.

Huang, X., & Peng, Y. (2009, May). An Effective Approach for Remote Attestation in Trusted Computing. In *WISA 2009: Proceedings of the 2nd International Symposium on Web Information Systems and Applications* (pp. 80-83).

Hwang, S. O. (2009). How Viable Is Digital Rights Management?. *Computer*,*4* (4), 28-34.

Hwang, S. O., Yoon, K. S., Jun, K. P., & Lee, K. H. (2004). Modeling and implementation of digital rights. *Journal of Systems and Software*, *73*(3), 533-549.

Iannella, R. (2001). Digital rights management (DRM) architectures, *D-Lib Magazine* vol 7, n 6. Available from http://www.dlib.org/ dlib/june01/iannella/ 06iannella.html.

Iannella, R., Mclean N. (2002). "Digital Rights Management (DRM) in Education - The Need for Standardisation" A Briefing Paper for IMS, *IMS Australia Centre*. IPR Systems.

Iannella, R. (2008). Rights management and licensing multimedia services. In*Multimedia Services in Intelligent Environments* (pp. 327-349). Springer Berlin Heidelberg.

IMS - IMS Global Learning Consortium. Content packaging specification (2009). http://www.imsglobal.org/content/packaging/

Insider Monkey, (April, 2013) "Electronic Arts Inc. (EA), Microsoft Corporation (MSFT): Should Investors Worry About Always-On DRM?" *The Motley Fool, LLC*, retrieved from: http://www.insidermonkey.com/blog/electronic-arts-inc-ea-microsoft-corporation-msft-should-investors-worry-about-always-on-drm-1263832013.

ISAN. International Standard Audiovisual Number, http://www.isan.org.

ISBN. International Standard Book Number, https://www.isbn-international.org.

ISMA. Internet Streaming Media Alliance, "Encryption & Authentication Specification 2.0" (ISMA Crypt 2.0). Available from: http://www.mpegif.org/m4if/bod/ISMA /ISMA_E&Aspec2.0.pdf

ISO/IEC 11889-1:2009. (2009) *Information technology - Trusted Platform Module - Part 1: Overview*. ISO/IEC, 2009.

ISO/IEC 11889-2:2009. (2009) *Information technology - Trusted Platform Module - Part 2: Design principles*. ISO/IEC, 2009.

ISO/IEC 11889-3:2009. (2009) *Information technology - Trusted Platform Module - Part 3: Structures*. ISO/IEC, 2009.

ISO/IEC 11889-4:2009. (2009) *Information technology - Trusted Platform Module - Part 4: Commands*. ISO/IEC, 2009.

ISSN. International Standard Serial Number, www.issn.org

ISWC. International Standard Musical Work Code, http://www.iswc.org/.

Iwakiri, M., & Thanh, T. M. (2015, July). Fragile watermarking based on incomplete cryptography for copyright protection. In *Applied Informatics* (Vol. 2, No. 1, pp. 1-20). Springer Berlin Heidelberg.

Jamkhedkar, A., Heileman, G., (2008, October). A formal conceptual model for rights. In *Proceedings of the 8th ACM workshop on Digital rights management* (pp. 29-38). ACM.

Jamkhedkar, P. A., Heileman, G., (2004, October). DRM as a layered system. In *Proceedings of the 4th ACM workshop on Digital rights management* (pp. 11-21). ACM.

Jamkhedkar, A., Heileman, L. (2009). Rights Expression Languages. *Handbook of Research on Secure Multimedia Distribution*, 1.

Jamkhedkar, P. A., & Heileman, G. L. (2009). Digital rights management architectures. *Computers & Electrical Engineering*, *35*(2), 376-394.

Jeong, Y., Park, J., Kim, J., & Yoon, K. (2007, July). DRM content adaptation scheme between different DRM systems for seamless content service. In*Multimedia and Expo, 2007 IEEE International Conference on* (pp. 867-870). IEEE.

Jeong, Y., Yoon, K. & Ryou J. (2005). A trusted key management scheme for digital rights management. *ETRI journal*, *27*(1), 114-117.

Jin, H., Myles, G., & Lotspiech, J. (2005). Towards better software tamper resistance. In *Information Security* (pp. 417-430). Springer Berlin Heidelberg.

Jin, J., Lin, H., Liu, Q., Zhao, G., & Wu, D. (2006). License Management Scheme for Learning Resources Delivery in P2P Networks. In *PDPTA* (pp. 212-220).

Johns, A. (2010). Piracy: The intellectual property wars from Gutenberg to Gates. *University of Chicago Press.*

Jonker, L. & Mauw S. (2004, June). Core security requirements of DRM systems. In *Symposium on Information theory in the Benelux*.

Jonsson, J., B. (2003). Public-key cryptography standards (PKCS)#1: RSA cryptography specifications version 2.1.

Josefsson, S. (2006). The base16, base32, and base64 data encodings. Retrieved from https://tools.ietf.org/html/rfc4648.

Kahn, R., Wilensky, R. (1995). A framework for distributed digital object services. Corporation for National Research Initiatives. Retrieved from.*http://www. cnri.reston.va.us/kw.html*.

Kamperman, F. L., Szostek, L., & Baks, W. (2007, January). Marlin common domain: authorized domains in marlin technology. In *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE* (pp. 935-939). IEEE.

Kang, M., Kim, S., Park, G. C., Lee, G., & Kil, M. (2006, January). Design of DRM-LMS model in m-learning environment. In *Knowledge-Based Intelligent Information and Engineering Systems* (pp. 1075-1082). Springer Berlin Heidelberg.

Karaganis, J., & Renkema, L. (2013). *Copy Culture in the US & Germany*., Retrieved from http://piracy.americanassembly.org/wp-content/uploads/2013/01/Copy-Culture.pdf

Kawahara, M. (1990). Superdistribution: the concept and the architecture.*IEICE TRANSACTIONS (1976-1990), 73*(7), 1133-1146.

Keoh, S. L. (2011). Marlin: Toward seamless content sharing and rights management. *Communications Magazine, IEEE, 49*(11), 174-180.

Keoh, S. L., & Vrielink, K. (2009, November). An implementation experience of domain management in marlin. In *Proceedings of the nineth ACM workshop on Digital rights management* (pp. 29-38). ACM.

Kim, J., Jeong, Y., Yoon, K., & Ryou, J. (2006, October). A trustworthy end-to-end key management scheme for digital rights management. In *Proceedings of the 14th annual ACM international conference on Multimedia* (pp. 635-638). ACM.

Koenen, R.. Overview of the MPEG-4 standard. (2002). Retrieved from http://mpeg.chiariglione .org/sites/default/files/files/standards/docs/w4668.zip.

Koenen, R., Lacy, J., MacKay, M., & Mitchell, S. (2004). The long march to interoperable digital rights management. *Proceedings of the IEEE*, *92*(6), 883-897.

Koster, P. (2007). Person-based and domain-based digital rights management. In *Security, Privacy, and Trust in Modern Data Management* (pp. 303-316). Springer Berlin Heidelberg. (Koster, 2007)

Koster, P., Montaner, J., Koraichi N., Iacob S. (2007, January). Introduction of the domain issuer in OMA DRM. In *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE* (pp. 940-944). IEEE.

Ku, W., & Chi, C. H. (2004). Survey on the technological aspects of digital rights management. In *Information Security* (pp. 391-403). Springer Berlin Heidelberg.

Kwok, H. & Chi R., (2006). Digital Rights Management for Mobile Commerce Using *Web* Services. *Journal of Electronic Commerce Research,7*(1), 1-13.

Lee, J., Lee S., Shin S., (2007). A Secure DRM Framework for User's Domain and Key Management. In *Autonomic and Trusted Computing* (pp. 420-429). Springer Berlin Heidelberg.

Lee, J., Hwang, S. O., Jeong, S. W., Yoon, K. S., Park, C. S., & Ryou, J. C. (2003). A DRM framework for distributing digital contents through the Internet. *ETRI journal*, *25*(6), 423-436.

Lee, S., Park H., Kim J. (2010, June). A secure and mutual-profitable DRM interoperability scheme. In *Computers and Communications (ISCC), 2010 IEEE Symposium on* (pp. 75-80). IEEE.

Lee, W. B., Wu, W. J., & Chang, C. Y. (2007). A portable DRM scheme using smart cards. *Journal of Organizational Computing and Electronic Commerce*, *17*(3), 247-258.

Li, H., Zhao, L., Wang, C., & Ma, F. (2010, July). DRM system for multiple cascaded business operators. In *Multimedia and Expo (ICME), 2010 IEEE International Conference on* (pp. 1651-1654). IEEE.

Libert, B., & Vergnaud, D. (2008, October). Multi-use unidirectional proxy re-signatures. In *Proceedings of the 15th ACM conference on Computer and communications security* (pp. 511-520). ACM.

Liu, Q., Safavi-Naini, R., & Sheppard, N. P. (2003, January). Digital rights management for content distribution. In *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003-Volume 21*(pp. 49-58). Australian Computer Society, Inc.

Liu, Z., Wang, B., Lee, B., & Han, M. M. (2007, August). Security license distribution mechanism for rights delegation models of group distribution between consumers. In *Computational Science and its Applications, 2007. ICCSA 2007. International Conference on* (pp. 144-152). IEEE.

Llorente, S., Delgado, J., Maroñas X., & Florido J. (2014). Definition of standards-based building blocks for multimedia content management. *Multimedia Tools and Applications*, 1-23.

Llorente, S., Rodríguez, E., Delgado, J., & Torres-Padrosa, V. (2013). Standards-based architectures for content management. *MultiMedia, IEEE*, *20*(4), 62-72.

Llorente, S., Rodríguez, E., & Delgado, J. (2004, January). Workflow description of digital rights management systems. In *On the Move to Meaningful Internet Systems 2004: OTM 2004 Workshops* (pp. 581-592). Springer Berlin Heidelberg.

Löytynoja, M., & Cvejic, N. (2003). Experimental DRM architecture using watermarking and PKI. In *In: First International Mobile IPR Workshop: Rights Management of Information Products on the Mobile Internet*.

Mampaey, M., & Villegas, Á. N. (2012). A Network-Centric DRM for Online Scenarios. *Bell Labs Technical Journal*, *17*(3), 129-133.

Mark Stefik (Ed.). (1997). *Internet dreams: archetypes, myths, and metaphors*. MiT Press.

Marlin Developer Community (MDC). (2006). The Role of Octopus in Marlin. Retrieved from http://www.marlin-community.com/public/RoleofOctopusinMarlin.pdf

Marlin Developer Community (MDC). (2007). Marlin Broadband Architecture. Overview for Marlin Adopters. Retrieved from http://www.marlin-community.com/public/ MarlinBroadbandArchitectureOverview .pdf.

Marlin Developer Community (MDC). (n.d.) Marlin Architecture Overview. Retrieved from http://www.marlin-community.com/public/MarlinArchitecture Overview .pdf

Maroñas X., Rodríguez E., Delgado J. (2009, September). An architecture for the interoperability between Rights Expression Languages based on XACML. In *Proceedings of the 7th International Workshop for technical, economic and legal aspects of business models for virtual goods, Virtual Goods*.

Marques, J., Serrão C. (2009). Rights management on Knowledge-based content. In proceedings of Cisti 2009 - 4ª Conf. Ibérica de sistemas e tecnologias de Informação, Póvoa de Varzim, Portugal, 2009.

Marques, J., & Serrão, C. (2011). Academic Context and rights enforcement on knowledge based content. *ICERI2011 Proceedings*, 618-628.

Marques, J., Serrão, C. (2012a). Rights Management and Technological Protection Measures in Educational Field.In proceedings of the *11th European Conference on e-Learning*, 327

Marques, J. & Serrão C. (2012b, September). Technological protection measures on knowledge based content in academia. In proceedings of the *15th International Conference on Interactive Collaborative Learning (ICL)*, pp. 1-4. IEEE.

Marques, J., & Serrão, C. (2014). Improving user content privacy on social networks using rights management systems. In *Annals of telecommunications-annales des télécommunications*, *69*(1-2), 37-45

Marques, J. & Serrão C. (2015a). ARMS – A new approach to control content sharing and rights distribution. In proceedings *7th Int. Conf. on Education and new Learning Technologies- Edulearn15*. pp 5597-5607. Barcelona.

Marques, J. & Serrão C. (2015b). Enabling Content and rights transmission in the Educational field with ARMS. In proceedings of *14th Int Conf. WWW/Internet 2015*, ICWI, Dublin.

Marques, J. & Serrão C. (2015c). Digital Rights in the Educational field - Mechanisms for licensing validation. In proceedings of *8th annual International Conference of Education, Research and Innovation –ICERI15*, Seville.

Marques, J., Serrão C. & Metrolho J. (2015). Content Related Rights Transmission with MPEG-21 in the Educational Field. In proceedings of the *14th European Conference on e-Learning, ECEL-2015,* London.

Martin, M., Agnew, G., Boyle, J., McNair, J., Page, M., & Rhodes, W. (2002, September). DRM Requirements for Research and Education Discussion Paper. In *The NSF Middleware Initiative and Digital Rights Management Workshop*.

McGeveran, W., & Fisher, W. W. (2008). The Digital Learning Challenge: Obstacles to Educational Uses of Copyrighted Material in the Digital Age. *SSRN Working Paper Series*.

METS. (2014). Library of Congress, Metadata Encoding and Transmission Standard., retrieved 10/01/2015 from http://www.loc.gov/standards/mets/

Michiels, W., & Gorissen, P. (2007, October). Mechanism for software tamper resistance: an application of white-box cryptography. In *Proceedings of the 2007 ACM workshop on Digital Rights Management* (pp. 82-89). ACM.

Michiels, S., Verslype, K., Joosen, W., & De Decker, B. (2005, November). Towards a software architecture for DRM. In *Proceedings of the 5th ACM workshop on Digital rights management* (pp. 65-74). ACM.

Miller R., (2001). The OSI Model: An Overview-GSEC Practical Assignment Version 1.2e, SANS Institute.

Miniwatts Marketing Group. (2013). Internet world states: usage and population statistics, retrieved from: http://www.internetworldstats.com/stats.htm, 2013 Q4.

Morin, J. H., (2009). Exception based enterprise rights management: Towards a paradigm shift in information security and policy management. *International Journal On Advances in Systems and Measurements*, *1*(1), 40-49. [69]

MOSES. (2004) - MPEG Open Security for Embedded Systems project. http://www.crl.co.uk/projects/moses/.

MPEG-21:DID, (2005). - ISO/IEC:2005. Information Technology – Multimedia framework – (MPEG-21) Part 2: Digital Item Declaration, ISO/IEC 21000-2:2005.

MPEG-21:DII, (2005). - ISO/IEC:2005. Information Technology – Multimedia framework (MPEG-21) - Part 3: Digital Item Identification, ISO/IEC 21000-3:2005.

MPEG-21:ER, (2006). - ISO/IEC:2006). ISO/IEC IS 21000:15 – (MPEG-21) Part 15: Event Reporting.

MPEG-21:IPMP, (2006). - ISO/IEC:2006. Information Technology – Multimedia framework (MPEG-21) – Part 4: Intellectual Property Management and Protection Components, ISO/IEC 21000-4:2006.

MPEG-21:RDD, (2006). - ISO/IEC:2004. Information Technology – Multimedia framework (MPEG-21) - Part 6: Rights Data Dictionary. ISO/IEC 21000-6:2006

MPEG-21:REL, (2005). - ISO/IEC:2005. Information technology – Multimedia framework (MPEG-21) - Part 5: *Rights Expression Language*, ISO/IEC 21000-5:2005.

MPEG-21:VTS, (2004) - ISO/IEC:2004. Information Technology – Multimedia framework (MPEG-21) – Part 1*: Vision, Technologies and Strategy*, ISO/IEC 21000-1:2004.

MPEG-4:IPMP-X (2005). - MPEG4, IPMP-X (Intellectual Property Management and Protection Extension), Retrieved from: http://www.mpeg.org/.

MPEG-M, (2013). - ISO/IEC IS 23006- (all parts): 2013– MPEG-M (MPEG Extensible Middleware). MXM protocols.

Mullan, E., (2011). What is Digital Content? *EContent, Dec 19*, Retrieved from http://www. econtentmag.com/Articles/Resources/Defining-EContent/What-is-Digital-Content-79501.htm

Mussinelli, C. (2010). Digital publishing in Europe: a focus on France, Germany, Italy and Spain. *Publishing research quarterly*, *26*(3), 168-175.

Nadah. N., deRosnay, M. & Bachimont, B. (2007, June). Licensing digital content with a generic ontology: escaping from the jungle of rights expression languages. In *Proceedings of the 11th international conference on Artificial intelligence and law* (pp. 65-69). ACM.

Nasereddin, H. H. (2011). DIGITAL WATERMARKING A TECHNOLOGY OVERVIEW. *International Journal of Research and Reviews in Applied Sciences*, *6*(1).

Nelson, L., & Sompel H. V. D. (2006). IJDL special issue on complex digital objects: Guest editors' introduction. *International Journal on Digital Libraries*, *6*(2), 113-114.

Nelson, M. R. (2006). Digital content delivery trends in higher education.*Research Bulletin*, (9), 12-18.

Nickolova, M., & Nickolov, E. (2007). Conceptual model and security requirements for DRM techniques used for e-learning objects protection.

OMA - Open Mobile Alliance, (2004a). Digital Rights Management. Approved Version 1.0 – 15 Jun 2004

OMA - Open Mobile Alliance, (2010b). DRM specification. Approved version 2.1.1. Open Mobille Alliance, 2010

OMA - Open Mobile Alliance, (2011a). DRM architecture. Candidate version 2.2. *Open Mobille Alliance, 2011*.

OMA - Open Mobile Alliance, (2011b). DRM content format. Candidate version 2.2. *Open Mobille Alliance, 2011*.

OMA - Open Mobile Alliance, (2011c). DRM Rights Expression Language. Candidate version 2.2, Open Mobille Alliance, 2011.

OMA - Open Mobile Alliance, (2011d). DRM Architecture v2.2, Candidate Version 2.2. 19 Apr 2011. Available from http://technical.openmobilealliance.org/Technical/

Release_Program/docs/DRM/V2_2-20110419-C/OMA-AD-DRM-V2_2-20110419C.pdf

OMA - Open Mobile Alliance, (2011e). DRM specification", candidate version 2.2, *Open Mobille Alliance, 2011*.

OpenIPMP (n.d.). Retrieved September 25, 2015.

OpenSDRM, (2005). OpenSDRM API Specification. (2005). ADETTI, Version: 20051011, Retrieved from http://www.opensdrm.org/files/OpenSDoRM_API_Specification.pdf.

Oppliger, R., Rytz, R. (2005). Does trusted computing remedy computer security problems?. *IEEE Security & Privacy*, *3*(2), 16-19.

Palavalli, S., Srinivas, U. S., & Pais, A. R. (2008). Identity based DRM system with total anonymity and device flexibility using IBES. *HIGH PERFORMANCE COMPUTING & SIMULATION (HPCS 2008)*, 213.

Park, T. K. (2011). The visibility of Wikipedia in scholarly publications. *First Monday*, 16(8). Retrieved from http://www.ojphi.org/ojs/index.php/fm/article/view/3492/3031

Paskin, N. (2003). Components of drm systems identification and metadata. In *Digital Rights Management* (pp. 26-61). Springer Berlin Heidelberg.

Patriciu, V., Bica, I., Togan, M., & Ghita, S. V. (2011). A generalized drm architectural framework. *Advances in Electrical and Computer Engineering,11*(1), 43-48.

Petkovic, M., & Jonker, W. (2007). *Security, Privacy, and Trust in Modern Data Management*. Springer.

Piva, A., Bartolini, F., & Barni, M. (2002). Managing copyright in open networks. *Internet Computing, IEEE*, *6*(3), 18-26.

Popescu, B. C., Crispo, B., Tanenbaum, A. S., & Kamperman, F. L. (2004, October). A DRM security architecture for home networks. In *Proceedings of the 4th ACM workshop on Digital rights management* (pp. 1-10). ACM.

Prados, J., Rodriguez, E., & Delgado, J. (2005, November). Interoperability between different rights expression languages and protection mechanisms. In *Automated Production of Cross Media Content for Multi-Channel Distribution, 2005. AXMEDIS 2005. First International Conference on* (pp. 8-pp). IEEE.

Prihandoko, C., Ghodosi, H., Litow, B. (2013) White-box Implementation to Improve DRM. Retrieved from: http://www.researchgate.net/publication/ 256498011_White-box_Implementation_to_Improve_DRM/file/60b7d5232553444df1.pdf

Prihandoko, A. C., Litow, B., & Ghodosi, H. (2012). DRM's rights protection capability: a review. In *The First International Conference on Computational Science and Information Management* (pp. 12-17)

Pucella, R., & Weissman, V. (2006). A formal foundation for ODRL. arXiv preprint cs/0601085.

RDF (2014), World Wide Web Consortium, Resource Description Framework, Retrieved from http://www.w3.org/standards/techs/rdf#w3c_all

Ridzon, R. L. (2009, September). Multimedia security and multimedia content protection. ELMAR, 2009. ELMAR'09. International Symposium.

Rodríguez, E., Delgado J. (2006, December). Towards the interoperability between MPEG-21 REL and Creative Commons Licenses. In *Automated Production of Cross Media Content for Multi-Channel Distribution, 2006. AXMEDIS'06. Second International Conference on* (pp. 45-52). IEEE.

Rodriguez, E., & Delgado, J. (2007a). Verification algorithms for governed use of multimedia content. *Online Information Review*, *31*(1), 38-58.

Rodríguez, E., Delgado J. (2007b, January). Trust in event reporting mechanisms for DRM. In *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE* (pp.1058-1062). IEEE.

Rodríguez, E., Gallego, I., & Delgado, J. (2007c, November). Use of MPEG-21 for License Protection and Key Management in DRM Systems. In *Automated Production of Cross Media Content for Multi-Channel Distribution, 2007. AXMEDIS'07. Third International Conference on* (pp. 163-170). IEEE.

Rosenblatt, B. (2009). Digital Rights and Digital Television. In *Television Goes Digital* (pp. 209-223). Springer New York.

Rosenblatt, W., Mooney, S., & Trippe, W. (2004). *Digital rights management: business and technology*. John Wiley & Sons, Inc.

Rosenblatt, B., & Dykstra, G. (2003). Integrating content management with digital rights management-imperatives and opportunities for digital content lifecycles. *White paper, Giantsteps Media Technology Strategies*.

Ross, V., (2013). Intellectual Property Policies in Academe: Issues and Concerns with Digital Scholarship. In *Accentuate the Positive: Charleston Conference Proceedings, 2012* (p. 397). Purdue University Press.

Rosset, V., Filippin, V., & Westphall, M. (2005, July). A DRM architecture to distribute and protect digital contents using digital licenses. In *Telecommunications,* pp. 422-427.

Rump, N. (2003). Digital rights management: Technological aspects. In *Digital rights management* (pp. 3-15). Springer Berlin Heidelberg.

Sachan, A., & Emmanuel, S. (2011). Rights violation detection in multi-level digital rights management system. *Computers & Security*, *30*(6), 498-513.

Sachan, A., Emmanuel, S., & Kankanhalli, M. S. (2010, January). Efficient aggregate licenses validation in DRM. In *Database Systems for Advanced Applications* (pp. 313-319). Springer Berlin Heidelberg.

Sachan, A., Emmanuel, S., & Kankanhalli, M. S. (2009, November). Efficient license validation in MPML DRM architecture. In *Proceedings of the nineth ACM workshop on Digital rights management* (pp. 73-82). ACM.

Sachan, A., Emmanuel, S., & Kankanhalli, M. S. (2012). Aggregate licenses validation for digital rights violation detection. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 8(2S)*, 37.

Sadeghi, A. R. (2008). Trusted computing-special aspects and challenges. In*SOFSEM 2008: Theory and Practice of Computer Science* (pp. 98-117). Springer Berlin Heidelberg.

Safavi-Naini, R., Sheppard P. (2010). Digital rights management. In Rosenberg, Burton (Ed.) *Handbook of Financial Cryptography and Security*. CRCPress.

Safavi-Naini, R., Sheppard, N. P., & Uehara, T. (2004, October). Import/export in digital rights management. In *Proceedings of the 4th ACM workshop on Digital rights management* (pp. 99-110). ACM.

Sandvine. Global Internet Phenomena Report, H1, (2014). Retrieved from https://www.sandvine.com/downloads/general/global-internet-phenomena/2014/1h-2014-global-internet-phenomena-report.pdf

Sans, T., Cuppens, F., & Cuppens-Boulahia, N. (2007). OPA: Onion Policy Administration Model-Another approach to manage rights in DRM. In *New Approaches for Security, Privacy and Trust in Complex Environments* (pp. 349-360). Springer US.

Schmidt, A. U., Tafreschi, O., & Wolf, R. (2004, May). Interoperability challenges for DRM systems. In *IFIP/GI workshop on virtual goods, Ilmenau, Germany*.

Schneier, B. (2007). *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons.

Schreiner, F. (2011). *Content management and protection using Trusted Computing and MPEG-21 technologies* (Doctoral dissertation, Technische Universität München).

Serrão, C., Neves, D., Kudumakis, P., Barker, T., & Balestri, M. (2003, June). Open SDRM–an open and secure digital rights management solution. In *Proceedings of the International Association for Development of the Information Society (IADIS'03), International Conference on e-Society, Lisbon, Portugal*.

Serrão, C., Siegert G. (2004). Open Secure Infrastructure to control User Access to multimedia content. *Security In Information Systems*, 180.

Serrão, C., Dias M., Delgado J. (2005a, July). Using ODRL to express rights for different content usage scenarios. In *ODRL2005–2nd International ODRL Workshop* (pp. 7-8).

Serrão, C., Dias, M., & Delgado, J. (2005b). Using *Web*-Services to Manage and Control Access to Multimedia Content. In *ISWS05-The 2005 International Symposium on Web Services and Applications, Las Vegas, USA*.

Serrão, C., Fonseca, P., Dias, M., & Delgado, J. (2006a). The *Web* Services growing importance for DRM interoperability. In *Proceedings of the IADIS International Conference Internet/WWW -ICWI2006-, Murcia, Spain* (pp. 5-8).

Serrão, C., Marques, J., Dias, M., & Delgado, J. (2006b, October). Open-Source Software as a driver for digital content e-Commerce and DRM interoperability. In *Proceedings of the Europe-China Conference on Intellectual Property in Digital Media, Shangai, China*.

Serrão, C., Serra, A., Dias, M., & Delgado, J. (2006c, December). Protection of MP3 Music Files Using Digital Rights Management and Symmetric Ciphering. In *Automated Production of Cross Media Content for Multi-Channel Distribution, 2006. AXMEDIS'06. Second International Conference on* (pp. 128-135). IEEE.

Serrão, C., Torres, V., Delgado, J., & Dias, M. (2006d). Interoperability mechanisms for registration and authentication on different open DRM platforms. *IJCSNS*, *6*(12), 291-303.

Serrão, C., Serra A., Dias M., Delgado J. (July, 2007). PKI as a way to leverage DRM interoperability. In *Proceedings of the IADIS International Conference on Telecommunications, Networks and Systems 2007 (TNS2007)*, Lisboa, Portugal, 3-5

Serrão, C. (2008)." iDRM – Interoperability Mechanisms for Open Rights Management Platforms". Ph.D. dissertation. Universitat Politècnica de Catalunya.

Serrão, C., Rodriguez, E., & Delgado, J. (2011). Approaching the rights management interoperability problem using intelligent brokerage mechanisms. *Computer Communications*, *34*(2), 129-139.

Shao, B., Mattavelli M., Renzi D., Andrade M. T., Battista S., Keller, S., Carvalho, P. (2008, June). A multimedia terminal for adaptation and end-to-end Qos control. In *Multimedia and Expo, 2008 IEEE International Conference on* (pp. 433-436). IEEE.

Sheppard, P. (2007, October). On implementing MPEG-21 intellectual property management and protection. In *Proceedings of the 2007 ACM workshop on Digital Rights Management* (pp. 10-22). ACM.

Sheppard, N. P., & Safavi-Naini, R. (2006a, January). Protecting privacy with the MPEG-21 IPMP framework. In *Privacy Enhancing Technologies* (pp. 152-171). Springer Berlin Heidelberg.

Sheppard, N. P., & Safavi-Naini, R. (2006b, October). Sharing digital rights with domain licensing. In *Proceedings of the 4th ACM international workshop on Contents protection and security* (pp. 3-12). ACM.

Sim, S., Oh, Y., & Lee, S. (2006). Extending DRM Features to Distributed Environments. *Journal of Multimedia*, *1*(5), 36-41.

Snodgrass, R. T., Yao, S. S., & Collberg, C. (2004, August). Tamper detection in audit logs. In *Proceedings of the Thirtieth international conference on Very large data bases-Volume 30* (pp. 504-515). VLDB Endowment.

SOAP. Simple Object Access Protocol (2007). World Wide *Web* Consortium (W3C). SOAP Version 1.2 Part 1: Messaging Framework (Second Edition). http://www.w3.org/TR/soap12-part1/.

Solo, D., Reagle & J. D. Eastlake, (June 2008). XML-Signature Syntax and Processing ", W3C REC-xmldsig-core-20080610,.

Stamp, M. (2002). Risks of digital rights management. *Communications of the ACM*, *45*(9), 120.

Strauss, A., & Corbin, J. M. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Sage Publications, Inc.

Stumpf, F., Tafreschi, O., Röder, P., & Eckert, C. (2006, November). A robust integrity reporting protocol for remote attestation. In *Second Workshop on Advances in Trusted Computing (WATC'06 Fall)* (pp. 25-36).

Subramanya, S. R., & Yi, B. K. (2006). Digital rights management. *Potentials, IEEE*, *25*(2), 31-34.

Sumita, M., Ishikawa N., & Ueno (n.d.), H. Standardization of OMA DRM. NTT DoCoMo Technical Journal vol.6 Nº4. Retrieved from: https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/rd/technical_journal/bn/vol6_4/vol6_4_043en.pdf.

Sun, H., Yang, K., & Wang, K. (2005, June). Transferable DRM system for two new business models. In *Information Security Conference* (pp. 9-10).

Sun, J. C., & Baez, B. (2009). Intellectual Property in the Information Age: Knowledge as Commodity and Its Legal Implications for Higher Education: ASHE Higher Education Report (1st ed.). Jossey-Bass.

Taban, G., Cárdenas, A. A., & Gligor, V. D. (2006, October). Towards a secure and interoperable DRM architecture. In *Proceedings of the ACM workshop on Digital rights management* (pp. 69-78). ACM.

Thomas, T., Emmanuel, S., Das, A., & Kankanhalli, M. S. (2009, June). Secure multimedia content delivery with multiparty multilevel DRM architecture. In *Proceedings of the 18th international workshop on Network and operating systems support for digital audio and video* (pp. 85-90). ACM.

Torres, V., Rodríguez E., Llorente S., & Delgado J. (2004). Architecture and protocols for the protection and management of multimedia information. In *Interactive Multimedia and Next Generation Networks* (pp. 252-263). Springer Berlin Heidelberg.

Torres, V., Serrão C., Dias, M. S., & Delgado, J. (2008). Open DRM and the Future of Media. *MultiMedia, IEEE*, *15*(2), 28-36.

Torres, V., Tous, R., Delgado, J. (2010). Reliable scholarly objects search and interchange framework. A International Conference on Electronic Publishing. "14th International Conf. on Electronic Publishing". Helsinki: 2010, p.57-68.

Trusted Computing Group, (2011a). TPM Main Specification - Part 1 Design Principles. Available from: http://www.trustedcomputinggroup.org/files/static_page_files/72C26AB5-1A4B-B294-D002BC0B8C062FF6/TPM%20Main-Part%201%20Design%20Principles_ v1.2_rev116_01032011.pdf

Trusted Computing Group, (2011b). TPM Main Specification - Part 2 TPM Structures. Available from: http://www.trustedcomputinggroup.org/files/static_page_files/E55A303C-1A4B-B294-D066E66A82DAE27D/TPM%20Main-Part%202%20TPM%20Structures_v1.2_rev116_01032011.pdf

Trusted Computing Group, (2011c), TPM Main Specification - Part 3 Commands. Retrieved from: http://www.trustedcomputinggroup.org/files/static_page_files/72C33D71-1A4B-B294-D02C7DF86630BE7C/TPM%20Main-Part%203%20Commands_v1.2_rev116_01032011.pdf

Unlu, V., Hess T. (2005, July). The access-usage-control-matrix: A heuristic tool for implementing a selected level of technical content protection. In *E-Commerce Technology, 2005. CEC 2005. Seventh IEEE International Conference on* (pp. 512-517). IEEE.

Van de Walle, R., Koenen, R. (2006). *The MPEG-21 book* (pp. 35-37). Chichester: Wiley.

VanOorschot, P. C., Somayaji, A., & Wurster, G. (2005). Hardware-assisted circumvention of self-hashing software tamper resistance. *Dependable and Secure Computing, IEEE Transactions on*, *2*(2), 82-92.

Verslype, K., & De Decker, B. (2006, January). A flexible and open DRM framework. In *Communications and Multimedia Security* (pp. 173-184). Springer, Berlin Heidelberg.

Wang, X., (2006). Rights expression languages in digital rights management. in *Proceedings of the Europe-China Conference on Intellectual Property in Digital Media – Optimisation of Intellectual Property in Digital Media (IPDM06)*, Shangai, China.

Wang, B., Liu, Z., & Lee, B. (2007, August). A Study of Superdistribution Model for Family Domain in DRM System. In *Computational Science and its Applications, 2007. ICCSA 2007. International Conference on* (pp. 133-138). IEEE.

Wang, X., Lao, G., DeMartini, T., Reddy, H., Nguyen, M., & Valenzuela, E. (2002, November). XrML-eXtensible rights Markup Language. In *Proceedings of the 2002 ACM workshop on XML security* (pp. 71-79). ACM.

Wang, X. (2004). MPEG-21 Rights Expression Language: enabling interoperable digital rights management. *MultiMedia, IEEE*, *11*(4), 84-87.

Wang, X. (2005, July). Design principles and issues of rights expression languages for digital rights management. In *Visual Communications and Image Processing 2005* (pp. 59603C-59603C). International Society for Optics and Photonics.

Wang, X., DeMartini, T., Wragg, B., Paramasivam, M., & Barlas, C. (2005). The MPEG-21 rights expression language and rights data dictionary. *Multimedia, IEEE*

Wegner, S. (2003). OPERA-Interoperability of Digital Rights Management (DRM) Technologies: An Open DRM Architecture. *Eurescom report*.

Weise, J. (2001). Public key infrastructure overview. *Sun BluePrints OnLine, August*.

Wenqing, C., Wanting, D., & Di, D. (2005, July). A rights managing model in learning resource distribution. In *Information Technology Based Higher Education and Training, 2005. ITHET 2005. 6th International Conference on* (pp. S2A-12). IEEE.

Win, L. L., Thomas, T., Emmanuel, S., & Kankanhalli, M. S. (2009). Secure domain architecture for interoperable content distribution. In *Advances in Multimedia Information Processing-PCM 2009* (pp. 1313-1318). Springer, Berlin Heidelberg.

WIPO. World Intellectual Property Organization. Understandind Copyright and related rights. (n.d.,b). *WIPO Publication No. 909(E)*. Available from http://www.wipo.int/edocs/pubdocs/en/intproperty/909/wipo_pub_909.pdf

WIPO. World Intellectual Property Organization. What is intellectual property. (n.d.,a). *WIPO Publication No. 450(E)*. Available from http://www.wipo.int/edocs/ pubdocs/en/intproperty/450/wipo_ pub_ 450.pdf

Wu, Y., & Bao, F. (2008, October). Enriched Trusted Platform and its Application on DRM. In *Trusted Infrastructure Technologies Conference, 2008. APTC'08. Third Asia-Pacific* (pp. 91-97). IEEE.

Yan, J., & Peng, X., (2011). Security Strategy of DRM Based on Trusted Computing. *Journal of Computational Information Systems*, *7*(9), 3226-3234.

Yang, Z., Wei, X., & Zhang, Y. (2008, December). Research on REL Connecting with Application Scenarios in Education. In *Knowledge Acquisition and Modeling, 2008. KAM'08. International Symposium on* (pp. 472-475). IEEE.

Yen, Liaw, & Lo (2014). Digital rights management system with user privacy, usage transparency, and superdistribution support. *International Journal of Communication Systems*, 27(10), 1714-1730.

Yin, R. K., (2009). *Case study research: Design and methods*. Fourth Edition. Sage publications

Yu, Y., & Chiueh T., (2004). Enterprise digital rights management: Solutions against information theft by insiders. *Experimental Computer Systems Lab, Department of Computer Science of the State University of New York (SUNY).* Available from http://www.ecsl.cs.sunysb.edu/tr/TR169.pdf.

Yuan, J., Zhao F., Zhang W., & Tian W. (2012). A Profile-based Interoperable DRM System Framework. *International Journal of Digital Content Technology & its Applications*, *6* (4).

Zeng, W., Yu, H., & Lin, C. Y., (Eds.). (2011). *Multimedia Security Technologies for Digital Rights Management*. (Vol. 18). Academic Press.

Zhang, ZY., (2011). Digital rights management ecosystem and its usage controls: a survey. *Int. Journal of Digital Content Technololgy Appl.* 5(3): 255–272

Zhang, J., Wu, N. S., Luo, J. G., & Yang, S. Q. (2005, December). A scalable digital rights management framework for large-scale content distribution. In *Intelligent Signal Processing and Communication Systems, 2005. ISPACS 2005. Proceedings of 2005 International Symposium on* (pp. 761-764). IEEE.

Zhang, X., (2013). A Survey of Digital Rights Management Technologies. *Available from http://www.cse.wustl.edu/~jain/cse571-11/ftp/drm/ index.html*.

Zhang, Z., Pei, Q., Ma, J., & Yang, L. (2009). Security and Trust in Digital Rights Management: A Survey. *IJ Network Security*, *9* (3), 247-263.

Anexo A

Exemplificação de distribuição de licença por emissão e por controlo de delegação.

Caso 1

Considere-se o cenário em que um professor concede o direito à sua Universidade de emitir licenças sobre um ficheiro PDF para os seus professores, em que estes por sua vez podem emitir licenças para alunos do seu curso matriculado no corrente ano letivo. Sendo normal a existência de situações em que os alunos (e/ou professores) transmitem direitos entre si, para que o aluno (Aluno_111) que recebeu a licença do seu professor a possa emitir a licença para outro aluno (p.ex: Aluno_222) então teria que ter esse privilégio embebido na licença que recebeu do seu professor. Para tal deve ser indicado ao aluno se lhe foi delegado esse direito e em que condições. A funcionalidade *delegationControl* permite atribuir esse privilégio a todos os alunos desde que haja respeito pelo *constraint* definida. Desta forma pode-se delegar no aluno o direito de emitir uma licença e o aluno recetor também a poder delegar noutro aluno e assim sucessivamente. Uma licença de distribuição deste tipo pode ser:

```
<r:license licenseID=”001”>
   <r:Grant licPartId=”issueGrant”>
      <r:forAll varName="ProfessorX"/>
      <r:forAll varName=”cursoX”>
        <r:anXmlExpression>curso123<r:anXmlExpression>
      </r:forAll>
      <r:forAll varName="anoX">
            <r:anXmlExpression>2013<r:anXmlExpression>
      </r:forAll>
      <r:keyHolder>...Universidade...</r:keyHolder>
      <r:issue/>
            <r:grant licPartId=”UsageGrant”>
                  <r:keyHolder varRef="ProfessorX"/>
                  <mx:play/>
                  <mx:diReference>urn:example:pdf123</mx:diReference>
                  <r:validityInterval varRef="anoX"/>
                  <r:forAll varName=”cursoX”>
                    <r:anXmlExpression>curso123<r:anXmlExpression>
                  </r:forAll>
                  <r:forAll varName="anoX">
```

```
                        <r:anXmlExpression>2013<r:anXmlExpression>
                    </r:forAll>
                    <r:forAll varName="alunoXY"/>
                    <r:issue/>
                        <r:grant licPartId==”ReUsageGrant”>
                            <r:keyHolder varRef=”alunoXY”/>
                            <r:delegationControl>
                              <r:conditionUnchanged/>
                            </r:delegationControl>
                            <mx:play/>
                            <mx:diReference>urn:example:pdf123</mx:diReferen
                            ce>
                            <r:validityInterval varRef="anoX"/>
                           </r:grant>
            </r:grant>
    </r:grant>
    <r:issuer>
      <dsig:Signature>
            <dsig:SignedInfo>...</dsig:SignedInfo>
            <dsig:SignatureValue> … </dsig:SignatureValue>
            <dsig:KeyInfo>...Professor..</dsig:KeyInfo>
      </dsig:Signature>
    </r:issuer>
</r:license>
```

A licença de utilização a emitir pela Universidade para o Professor_111 recetor poderia ser:

```
<r:license licenseID=”0001_1”>
   <r:Grant LicPartId=”usageGrant”>
      <r:keyHolder licPartId=”Professor_111”>
            <r:info>
                  <dsig:KeyValue>
                        <dsig:RSAKeyValue>
                              <dsig:Modulus>…</dsig:Modulus>
                              <dsig:Exponent>…</dsig:Exponent>
                        </dsig:RSAKeyValue>
                  </dsig:KeyValue>
            </r:info>
      </r:keyHolder>
```

```
      <mx:play/>
      <mx:diReference>
            <mx:identifier>urn:example:pdf123</mx:identifier>
      </mx:diReference>
      <r:validityInterval>
            <r:notBefore>2013-09-01T00:00:00</r:notBefore>
            <r:notAfter>2014-09-01T00:00:00</r:notAfter>
      </r:validityInterval>
      <r:forAll varName=”cursoX”>
        <r:anXmlExpression>curso123<r:anXmlExpression>
      </r:forAll>
      <r:forAll varName="anoX">
            <r:anXmlExpression>2013<r:anXmlExpression>
      </r:forAll>
      <r:forAll varName="alunoXY"/>
      <r:issue/>
                        <r:grant licPartId==”ReUsageGrant”>
                            <r:keyHolder varRef=”alunoXY”/>
                            <r:delegationControl>
                               <r:conditionUnchanged/>
                            </r:delegationControl>
                            <mx:play/>
                            <mx:diReference>urn:example:pdf123</mx:diReferen
                            ce>
                            <r:validityInterval varRef="anoX"/>
                           </r:grant>
   </r:grant>
   <r:issuer>
      <dsig:Signature>
            <dsig:SignedInfo>...</dsig:SignedInfo>
            <dsig:SignatureValue> … </dsig:SignatureValue>
            <dsig:KeyInfo>...University...</dsig:KeyInfo>
      </dsig:Signature>
</r:issuer>
</r:license>
```

Quando um Professor X (colega do dono do conteúdo) emite esta licença para um seu aluno matriculado num curso, a licença do aluno recetor (Aluno_111) pode apresentar-se da seguinte forma:

```
<r:license licenseID=”0001_2”>
   <r:Grant LicPartId=”ReusageGrant”>
   <r:keyHolder varRef=”alunoXY”/>
    <r:delegationControl>
      <r:conditionUnchanged/>
    </r:delegationControl>
      <r:keyHolder licPartId=”Aluno_111”>
            <r:info>
                  <dsig:KeyValue>
                        <dsig:RSAKeyValue>
                              <dsig:Modulus>…</dsig:Modulus>
                              <dsig:Exponent>…</dsig:Exponent>
                        </dsig:RSAKeyValue>
                  </dsig:KeyValue>
            </r:info>
      </r:keyHolder>
      <mx:play/>
      <mx:diReference>
            <mx:identifier>urn:example:pdf123</mx:identifier>
      </mx:diReference>
      <r:validityInterval>
            <r:notBefore>2013-09-01T00:00:00</r:notBefore>
            <r:notAfter>2014-09-01T00:00:00</r:notAfter>
      </r:validityInterval>
   </r:grant>
   <r:issuer>
      <dsig:Signature>
            <dsig:SignedInfo>...</dsig:SignedInfo>
            <dsig:SignatureValue> … </dsig:SignatureValue>
            <dsig:KeyInfo>...Professor X...</dsig:KeyInfo>
      </dsig:Signature>
</r:issuer>
</r:license>
```

O Aluno_111 pode por sua vez emitir uma licença estruturalmente idêntica à que recebeu para um seu colega (Aluno_222), e este por sua vez emitir novamente para outros alunos (Aluno_n) e assim sucessivamente desde que a limitação (*constraint*) seja respeitada.

Caso 2

Outro caso de utilização em que o Professor A concede à Universidade o direito de emitir licenças para um determinado conteúdo aos seus alunos X, válida para o corrente ano, mas autorizando a que os seus colegas professores, tenham acesso ao conteúdo mas só com o direito de impressão e permitindo que os alunos possam distribuir a licença nas mesmas condições. Nesta situação a licença poderia conter o elemento *grantGroup* como a seguinte estrutura:

```
<r:license...>
   <r:grant>
    <r:forAll varName="alunos"/>
      <r:forAll varName="anoX">
            <r:anXmlExpression>2013<r:anXmlExpression>
      </r:forAll>
      <r:forAll varName="Professores"/>
      <r:keyHolder>UniversityABC</r:keyHolder>
      <r:issue/>
            <r:grantGroup>
                 <r:grant>
                  <r:keyHolder varRef="alunos"/>
                  <mx:play/>
                  <mx:diReference>urn:example:pdf123</mx:diReference>
                  <r:validityInterval varRef="anoX"/>
                       <r:grant licPartId==”ReUsageGrant”>
                           <r:keyHolder varRef=”alunos”/>
                           <r:forAll varName="anoX">
                               <r:anXmlExpression>2013<r:anXmlExpression>
                           </r:forAll>
                           <r:delegationControl>
                              <r:conditionUnchanged/>
                           </r:delegationControl>
                           <mx:play/>
                           <mx:diReference>urn:example:pdf123</mx:diReferen
                           ce>
                           <r:validityInterval varRef="anoX"/>
                          </r:grant>
```

```
                </r:grant>
                <r:grant>
                  <r:keyHolder varRef="Professores"/>
                  <mx:print/>
                  <mx:diReference>urn:example:PDFxyz</mx:diReference>
                </r:grant>
            </r:grantGroup>
    </r:grant>
    <r:issuer>
       <dsig:Signature>
              <dsig:SignedInfo>...</dsig:SignedInfo>
              <dsig:SignatureValue>…</dsig:SignatureValue>
              <dsig:KeyInfo>...Professor A...</dsig:KeyInfo>
       </dsig:Signature>
     </r:issuer>
</r:license>
```

A licença que a universidade emite divide-se em duas: uma para os professores e outra para alunos.

```
</r:license>
<r:grantGroup>
<r:grant>
   <r:keyHolder>
       <r:info>
       <dsig:KeyValue>
              <dsig:RSAKeyValue>
                     <dsig:Modulus>…Aluno X…=</dsig:Modulus>
                     <dsig:Exponent>…</dsig:Exponent>
              </dsig:RSAKeyValue>
       </dsig:KeyValue>
       </r:info>
    </r:keyHolder>
    <mx:play/>
    <mx:diReference>
       <mx:identifier>urn:example:PDFxyz</mx:identifier>
    </mx:diReference>
    <r:validityInterval>
       <r:notBefore>2013-01-01T00:00:00</r:notBefore>
       <r:notAfter>2014-12-01T00:00:00</r:notAfter>
```

```
    </r:validityInterval>
   <r:forAll varName="alunos"/>
   <r:forAll varName="anoX"/>
          <r:grant licPartId==”ReUsageGrant”>
              <r:keyHolder varRef=”alunos”/>
                <r:forAll varName="anoX">
                    <r:anXmlExpression>2013<r:anXmlExpression>
                </r:forAll>
                 <r:delegationControl>
                       <r:conditionUnchanged/>
                 </r:delegationControl>
              <mx:play/>
              <mx:diReference>urn:example:pdf123</mx:diReference>
              <r:validityInterval varRef="anoX"/>
             </r:grant>
</r:grant>
<r:grant>
   <r:keyHolder>
       <r:info>
       <dsig:KeyValue>
             <dsig:RSAKeyValue>
                   <dsig:Modulus> ….Professor X…=</dsig:Modulus>
                   <dsig:Exponent>…</dsig:Exponent>
             </dsig:RSAKeyValue>
       </dsig:KeyValue>
       </r:info>
    </r:keyHolder>
    <mx:print/>
    <mx:diReference>
       <mx:identifier>urn:example:PDFxyz</mx:identifier>
    </mx:diReference>
</r:grant>
</r:grantGroup>
<r:issuer>
       <dsig:Signature>
             <dsig:SignedInfo>...</dsig:SignedInfo>
             <dsig:SignatureValue>…</dsig:SignatureValue>
             <dsig:KeyInfo>...Universidade...</dsig:KeyInfo>
       </dsig:Signature>
```

```
     </r:issuer>
…
</r:license>
```

A licença emitida de um aluno para um outro seu colega é estruturalmente idêntica à anterior, mudando os emissores e o *principal*.

```
</r:grant>
<r:grant>
   <r:keyHolder>
       <r:info>
       <dsig:KeyValue>
              <dsig:RSAKeyValue>
                     <dsig:Modulus>…Aluno Y…</dsig:Modulus>
                     <dsig:Exponent>…</dsig:Exponent>
              </dsig:RSAKeyValue>
       </dsig:KeyValue>
       </r:info>
    </r:keyHolder>
    <mx:print/>
    <mx:diReference>
       <mx:identifier>urn:example:PDFxyz</mx:identifier>
    </mx:diReference>
    <r:validityInterval>
       <r:notBefore>2013-01-01T00:00:00</r:notBefore>
       <r:notAfter>2014-12-01T00:00:00</r:notAfter>
    </r:validityInterval>
   <r:forAll varName="alunos"/>
   <r:forAll varName="anoX"/>
          <r:grant licPartId=="ReUsageGrant">
              <r:keyHolder varRef="alunos"/>
              <r:forAll varName="anoX">
                    <r:anXmlExpression>2013<r:anXmlExpression>
                </r:forAll>
                 <r:delegationControl>
                       <r:conditionUnchanged/>
                 </r:delegationControl>
              <mx:play/>
              <mx:diReference>urn:example:pdf123</mx:diReference>
```

```
              <r:validityInterval varRef="anoX"/>
             </r:grant>
</r:grant>
<r:grantGroup>
</r:license>
```