UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

MECANISMOS DE PROTEÇÃO DE CONTEÚDO E MODELAMENTO DE DRM EM TV DIGITAL

ANA CLÁUDIA DYTZ BARBOSA

ORIENTADOR: PAULO ROBERTO DE LIRA GONDIM

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGENE.DM 342/08

BRASÍLIA / DF: JULHO - 2008

FICHA CATALOGRÁFICA

DYTZ BARBOSA, ANA CLÁUDIA
Mecanismos de Proteção de Conteúdo e Modelamento de DRM em TV Digital: [Distrito Federal] 2008.
95p, 210 x 297 mm (ENE/FT/Unb, Mestre, Dissertação de Mestrado – Universidade de Brasília. Faculdade de Tecnologia.
Departamento de Engenharia Elétrica
1. Televisão digital
2. Tratamento de Direitos Autorais em mídia digital
3. Mecanismos de Proteção em Televisão digital
I. ENE/FT/UnB II. Título
(série)

REFERÊNCIA BIBLIOGRÁFICA

DYTZ BARBOSA, A. C. (2008). Mecanismos de Proteção de Conteúdo e Modelamento de DRM em TV Digital. Dissertação de Mestrado em Engenharia Elétrica, Publicação PPGENE.DM-342/08, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 95p.

CESSÃO DE DIREITOS

AUTOR: Ana Claudia Dytz Barbosa
TÍTULO: Mecanismos de Proteção de Conteúdo e Modelamento de DRM em TV Digital
GRAU: Mestre ANO: 2008

_____

Ana Cláudia Dytz Barbosa
CLS 210 Bloco B, 12
CEP: 70.273-520
Brasília – DF – Brasil.

AGRADECIMENTOS

Ao professor e orientador Doutor Paulo Roberto de Lira Gondim pelo substancial apoio e atenção no desenvolvimento da tese;

Aos meus pais, Edison Dytz e Nilda Bastos Dytz por todo incentivo e estímulo em todos os momentos e pelo voto de confiança inabalável;

Ao meu marido Sergio Ricardo Barbosa e meu filho Samuel Dytz Barbosa pelo amor, paciência e compreensão em todos os momentos;

A Deus pela presença e cuidado constantes.

Dedicado aos meus pais, Edison Dytz e Nilda Bastos Dytz por toda motivação e incentivo em todos os momentos.

RESUMO

MECANISMOS DE PROTEÇÃO DE CONTEÚDO E MODELAMENTO DE DRM EM TV DIGITAL

Autora: Ana Claudia Dytz Barbosa

Orientador: Paulo Roberto de Lira Gondim

Programa de Pós-graduação em Engenharia Elétrica

Brasília, Julho de 2008.

A presente dissertação traz uma pesquisa bibliográfica ampla referente às técnicas utilizadas no tratamento dos direitos digitais de acesso e utilização de conteúdos multimídia.

São apresentados inicialmente os padrões dos Sistemas de Televisão Digital e respectivos *middlewares* atualmente empregados no mundo, porém com ênfase no sistema japonês e europeu por ser o primeiro padrão a base para o atual Sistema de Televisão Digital Brasileiro e o segundo padrão, por ser atualmente o padrão mais utilizado nesta área. Neste contexto, serão explorados os processos que compõem a cadeia de valores da Televisão Digital, partindo desde a fase de produção de conteúdo, passando pelas fases de programação, distribuição e consumo. Será abordada ainda a tecnologia de IPTV como alternativa de transporte de conteúdo para TV digital.

Posteriormente são apresentados os principais mecanismos de proteção de conteúdo digital e sua utilização no contexto de proteção de direitos de acesso ao conteúdo restrito ao longo da cadeia de valores da Televisão Digital. As técnicas abordadas abrangem a utilização dos descritores das tabelas do sistema de informação, o processo de criptografia do conteúdo associada ao sistema de acesso condicional, inserção de informações através de técnicas de marca d'água digital, geração de licenças criadas a partir de descritores pré-definidos trazendo informações sobre as condições de acesso, dentre outros.

Finalmente é apresentado um estudo de caso propondo uma arquitetura genérica para o acesso de conteúdo restrito com direitos digitais associados. A proposta se baseia nas principais funções de um sistema de acesso a conteúdo restrito que são: Autenticação, gerenciamento de usuários, tratamento de direitos digitais, contabilização financeira e autorização para acesso.

Palavras-chave: Televisão Digital, DRM, direitos digitais, metadados.

ABSTRACT

CONTENT PROTECTION MECANISMS AND DIGITAL TV DRM MODELING

Author: Ana Claudia Dytz Barbosa

Supervisor: Paulo Roberto de Lira Gondim

Programa de Pós-graduação em Engenharia Elétrica

Brasília, July of 2008.

Due to the difficulty of finding bibliographic solid references about the multimedia content protection at the Digital Television environment, the actual work brings a wide bibliographic research referencing the used technology for the digital access and use rights of multimedia contents.

Initially the actual world Digital Television Standards and respective middlewares are presented with emphasis on the Japanese and European systems, as the first one was used as base to the Brazilian Digital Television and the second one is the most used Digital Television System in the world.

On this context, the processes that compose the Digital Television value chain are exploited, from the initial content production phase, passing through programming, distribution and consumption phases. Also IPTV technology is presented as a content transport alternative for Digital Television.

The main digital content protection mechanisms used are presented through the Digital TV value chain. The presented techniques embrace System Information tables descriptors use, content cryptography related to conditional access system, watermarking information included in the content itself, license creation based on predefined descriptors that brings access condition information, among others.

Finally a case study is presented as proposition of a generic architecture to restrict content access based on digital rights associated to those contents. The proposal is based on the main functions of restrict content access system which are Authentication, user management, digital rights, Accounting and access authorization.

Keywords: Digital television, DRM, digital rights, metadata.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SÍMBOLOS, NOMENCLATURA E ABREVIAÇÕES

8-VSB	8 Vestigial Side Band
AAF	Advanced Authoring Format
API	Application Programming Interface
ARIB	Association of Radio Industries and Businesses
ATSC	Advanced Television Systems Commitee
BAT	Bouquet Association Table
BIT	Broadcaster Information Table
CA	Conditional Access
CAM	Conditional Access Message
CAS	Conditional Access System
CAT	Conditional Access Table
CI	Common Interface
COFDM	Coded Orthogonal Frequency Division Multiplexing
CPE	Customer Premises Equipment
CSS	Content Scrambling System
DASE	Digital TV Application Software Environment
DDL	Description Definition Language
DES	Data Encryption Standard
DI	Digital Item
DID	Digital Item Declaration
DII	Digital Item Identification
DIP	Digital Item Processing
DRM	Digital Rights Management
DS	Description Scheme
DSL	Digital Subscriber Line
DTCP	Digital Transmission Content Protection
DTD	Document Type Definition
DTLA	Digital Transmission Licensing Administrator
DVB	Digital Video Broadcasting
DVI	Digital Video Interface
EBU	European Broadcast Union
ECM	Entitlement Control Messages

EE	Executive Engine
EIT	Event Information Table
EMM	Entitlement Management Messages
ERT	Event Relation Table
ES	Elementary Stream
GEM	Globally Executable MHP
GXF	General Exchange Format
HDCP	High-bandwidth Digital Content Protection System
HDMI	High-Definition Multimedia Interface
IP	Internet Protocol
IPMP	Intellectual Property Management and Protection
IPR	Intellectual Property Rights
IPTV	Internet Protocol Television
ISDB	Integrated Services Digital Broadcasting
ISP	Internet Service Provider
ITT	Index Transmission Table
JVM	Java Virtual Machine
LIT	Local Event Information Table
MD5	Message-Digest algorithm 5
MHP	Multimedia Home Plataform
MPEG	Moving Pictures Expert Group
MXF	Material eXchage Format
NBIT	Network Board Information Table
NIT	Network Information Table
NRSS	National Renewable Security Standard
OCAP	OpenCable Application Platform
ODRL	Open Digital Rights Language
PAT	Program Association Table
PCAT	Partial Content Announcement Table
PE	Presentation Engine
PES	Packetized Elementary Stream
PID	Packet Identifier
PKI	Public Key Infrastructure

PMT	Program Map Table
PSI	Program Specific Information
PVR	Personal Video Recorder
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RBAC	Role Based Access Control
RDD	Rights Data Dictionary
REL	Rights Expression Language
RMP	Rights Management and Protection
RST	Running Status Table
RTCP	Real-Time Control Protocol
RTP	Real-Time Protocol
RTSP	Real-Time Streaming Protocol
RUP	Rational Unified Process
SBTVD	Sistema Brasileiro de Televisão Digital
SDT	Service Description Table
SI	Service Information
SMPTE	Society of Motion Picture and Television Engineers
ST	Stuffing Table
STB	Set-Top Box
SVC	Scalable Video Coding
TCP	Transport Control Protocol
TDB	Technical Disclosure Bulletin
TDT	Time Date Table
TOT	Time Offset Table
TS	Transport Stream
TTP	Trusted Third Party
TVA	TV - Anytime
TVD	Televisão Digital
TVDI	Televisão Digital Interativa
UDP	User Datagram Protocol
UIT	União Internacional de Telecomunicações
UML	Unified Modeling Language

URD	Unidade de Recepção e Decodificação (Set-Top Box)
URI	Uniform Resource Identifier
URN	Uniform Resource Name
VOD	Video on Demand
XML	Extensible Markup Language
XrML	eXtensible rights Markup Language

1 - INTRODUÇÃO

A televisão, em sua forma clássica, sempre funcionou como um dispositivo de comunicação unidirecional que oferece um conjunto de informações pré-definidas aos seus telespectadores [1].

A digitalização de conteúdos transmitidos nos sistemas de televisão já vem ocorrendo em algumas áreas como, por exemplo, na captura, edição e armazenamento de vídeo e áudio.

A televisão digital aumenta a atratividade e o potencial competitivo da televisão ao oferecer uma melhoria considerável na qualidade da imagem e do som, além de eliminar ruídos de sinal e de oferecer serviços novos e diferenciados como transmissão de vários programas em um só canal, acesso à Internet, interatividade, aplicações computacionais, gravação de programas em um disco rígido no aparelho receptor para exibição posterior e recepção móvel. A qualidade da tecnologia da TV digital vem do fato de que mesmo sendo a transmissão realizada de forma analógica, a informação contida nela consiste de dados digitais modulados que, por sua vez, estão menos sujeitos a interferências.

A TV Digital Interativa representa a evolução da transmissão de multimídia em larga escala consumida em meio passivo para um ambiente interativo, revolucionando assim, a forma como as pessoas utilizam a TV e trazendo novas perspectivas para a sociedade moderna e, em especial, para a economia. Uma possível junção da Internet com a tecnologia de TV Digital permite um conjunto de serviços relacionados a fluxos específicos da programação das emissoras de TV determinados por ações dos usuários, com base no emprego do protocolo IP.

A partir desta nova tecnologia, a indústria de televisores vislumbra uma perspectiva de expandir mercados através da oferta de novos produtos, tais como o televisor digital e o S*et-Top Box* (STB) (aparelho conversor de sinais digitais para analógicos que permite que um televisor comum receba a transmissão digital). Além disto, no caso específico do Brasil, a capacidade de penetração da TV Digital traz a possibilidade de acesso às facilidades da informática e Internet a grande parte da população brasileira, num processo de inclusão digital. Segundo o IBGE (2006), 95,2% da população possui acesso à televisão, enquanto que apenas 16,9% possui acesso à Internet [2].

A cadeia produtiva da televisão digital abrange diversos setores da economia além das próprias emissoras e fabricantes de televisores. É possível delimitar, sob uma

perspectiva mais abrangente e superficial, este processo em três áreas sendo estas referentes à geração, transmissão e consumo de conteúdo.

A geração de conteúdo diz respeito à produção do mesmo e está vinculada principalmente à própria rede de serviço das emissoras. A transmissão se refere à distribuição do conteúdo tendo como principal figura as chamadas retransmissoras de sinais as quais podem utilizar diversos meios para este fim como transmissão por rádio, satélite, cabo, etc. Por fim, o consumo ou recepção do conteúdo está relacionado ao usuário final. É neste contexto que as aplicações voltadas para televisão digital têm seu potencial de mercado, através da oferta de serviços personalizados, levando-se em conta o perfil do consumidor e características do dispositivo receptor.

De forma geral, a configuração do dispositivo receptor é em essência o que estabelece as linhas gerais de comportamento das aplicações para TV Digital, principalmente no que se refere ao nível de interação do usuário, ou seja, a tecnologia relacionada à TV interativa utiliza a capacidade de processamento da TV em conjunto com o armazenamento de bits na memória local de forma que a TV possua funcionalidades similares às de um computador. A interação é feita com o controle remoto ou um teclado sem fio, dentre outras possibilidades.

A interatividade pode se dar em âmbito local ou remoto, e é neste contexto que surge a necessidade de proteção do conteúdo tanto sob a ótica do proprietário ou criador como também do consumidor. Basicamente, o desafio na transmissão e consumo do conteúdo se dá no âmbito de assegurar a identificação proprietária, autenticação, integridade e acesso do mesmo somente por parte de quem adquiriu tal direito no momento da aquisição do direito de acesso. Além disto, os mecanismos de segurança do conteúdo devem assegurar a forma de uso estabelecida na aquisição do direito de acesso ao mesmo, permitindo, ou não, cópia e superdistribuição. O processo de superdistribuição corresponde à redistribuição dos conteúdos adquiridos por parte do consumidor para outros usuários [3] e, quando aplicável, o rastreamento de cópias não autorizadas.

2 - MOTIVAÇÃO

Devido à entrada do Brasil na era da TV Digital a necessidade da multiplicação de conhecimentos nesta área torna-se imprescindível. Desta forma, a escolha do tema então apresentado deu-se em tempo aprazível a fim de possibilitar material de referência a ser utilizado por terceiros, material este que abrange desde as informações gerais sobre a TV Digital, características do padrão europeu, do padrão japonês e do padrão brasileiro.

Além disto, o levantamento de informações sobre as técnicas de segurança utilizadas para gerenciamento de direitos autorais torna-se bastante pertinente. Com a facilidade de acesso ao conteúdo digital, a necessidade de controle deste acesso cresce proporcionalmente, devendo ser levadas em conta as condições de acesso estabelecidas por parte do proprietário dos direitos digitais de acesso, quando existentes.

3 - OBJETIVO

A TV Digital tem grande potencial para ser utilizada em larga escala nos diversos setores e classes sociais, tanto em ambiente privado como público, devido, entre outros, à cultura de utilização da TV já existente em nosso país. Desta forma, é de se esperar que a adaptação necessária para utilização de aplicações disponíveis que permitam a interação do usuário se dê de forma relativamente natural.

As aplicações envolvendo esta nova tecnologia possuem grandes perspectivas de aceitação no uso cotidiano, não só pelas vantagens representadas pela qualidade do sinal, quantidade de informações disponíveis e novas possibilidades de interação por parte dos usuários, mas também pelas perspectivas de disseminação de conhecimento e facilitação do acesso a determinados serviços em larga escala.

O objetivo principal desta pesquisa é apresentar uma referência bibliográfica sólida e ampla sobre os mecanismos de proteção utilizados no tratamento de direitos digitais de conteúdo multimídia.

4 - ORGANIZAÇÃO

A presente dissertação está organizada da seguinte forma: o item 5 dispõe sobre os atuais Sistemas de Televisão Digital, abrangendo aspectos da arquitetura, sistemas de transmissão, padrões e *middlewares*.

O item 6 aborda os mecanismos de proteção de conteúdo digital focando principalmente nas formas de proteção de direitos digitais no ambiente da Televisão Digital.

O item 7 traz a base conceitual sobre metadados indicando os tipos mais utilizados atualmente no ambiente da Televisão Digital.

O item 8 traz um estudo de caso genérico referente ao processo de acesso a conteúdo restrito, envolvendo os processos de autenticação de usuário, gerenciamento de usuários, gerenciamento de segurança, contabilização financeira e autorização de acesso a conteúdo restrito.

5 – SISTEMAS DE TELEVISÃO DIGITAL

5.1 – ARQUITETURA DA TV DIGITAL

As atuais tecnologias referentes à televisão digital convergem no contexto da integração entre os serviços convencionais de radiodifusão (*broadcasting*) com aplicações interativas e acesso à Internet. As aplicações interativas necessitam basicamente de um canal de retorno (*uplink*) para o usuário além dos canais de *broadcasting* para transmissão de dados e conteúdo das geradoras de programação de TV (*downlink*), os quais podem ser dedicados ou agregados aos fluxos (*streams*) de vídeo digital.

A TV Digital diferencia-se da televisão tradicional basicamente devido ao formato de sinal transmitido pela operadora de TV (*headend*) até o receptor do usuário final. No caso da TV Digital, os sinais de áudio e vídeo são distribuídos normalmente no padrão MPEG o qual permite a execução de aplicações de dados simultaneamente com a apresentação de áudio e vídeo. Na Figura 5.1, podem ser observadas as entidades mínimas no processo de geração de conteúdo, distribuição e recepção do sinal transmitido.

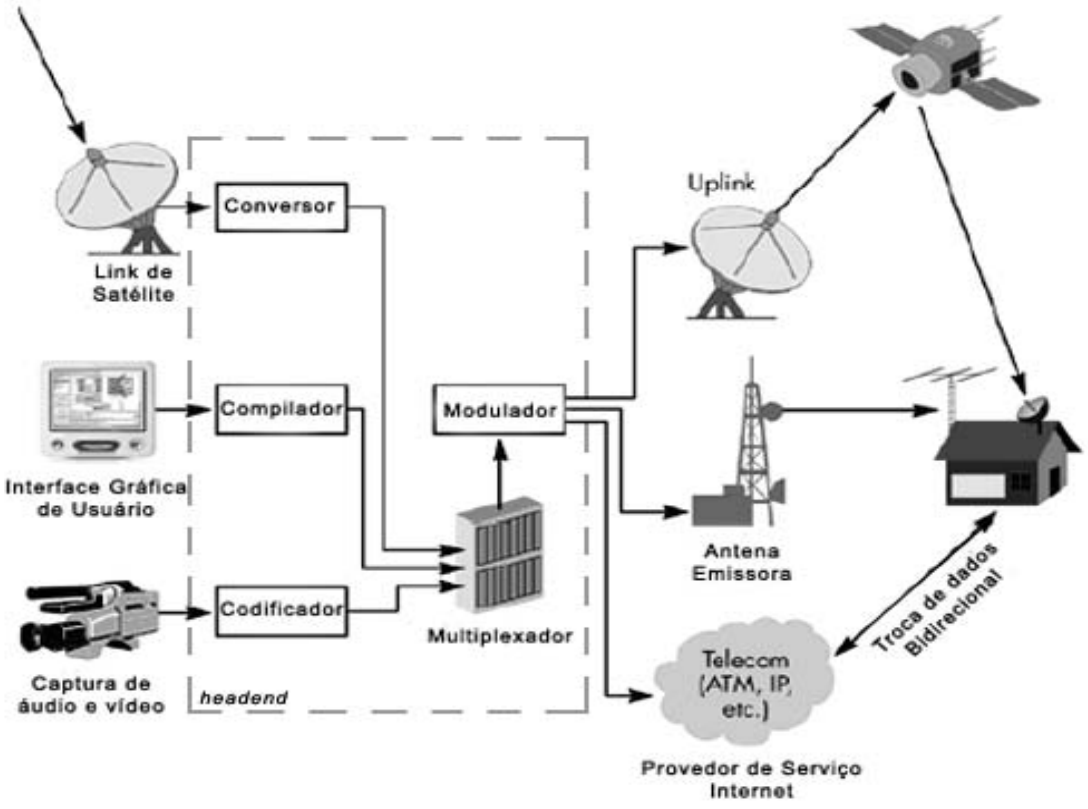


Figura 5.1 - Transmissão de conteúdo desde a produção até o usuário final [5]

O sistema de TV é formado basicamente por três subsistemas principais: Central de Produções, Radiodifusão e Recepção Doméstica. A Central de Produções é responsável pela criação dos programas de TV que serão veiculados através do sistema de Radiodifusão e é composta por vários Estúdios. O subsistema de Radiodifusão é responsável por receber o sinal a ser difundido, realizar a modulação de acordo com o meio utilizado e transmitir o sinal para a Recepção Doméstica (audiência).

5.2 - A CADEIA DE VALOR DA TV DIGITAL INTERATIVA

Conforme pode ser visto nas Figuras 5.2 e 5.3, o conteúdo transmitido passa por diversas etapas desde a sua criação até o acesso por parte do usuário.

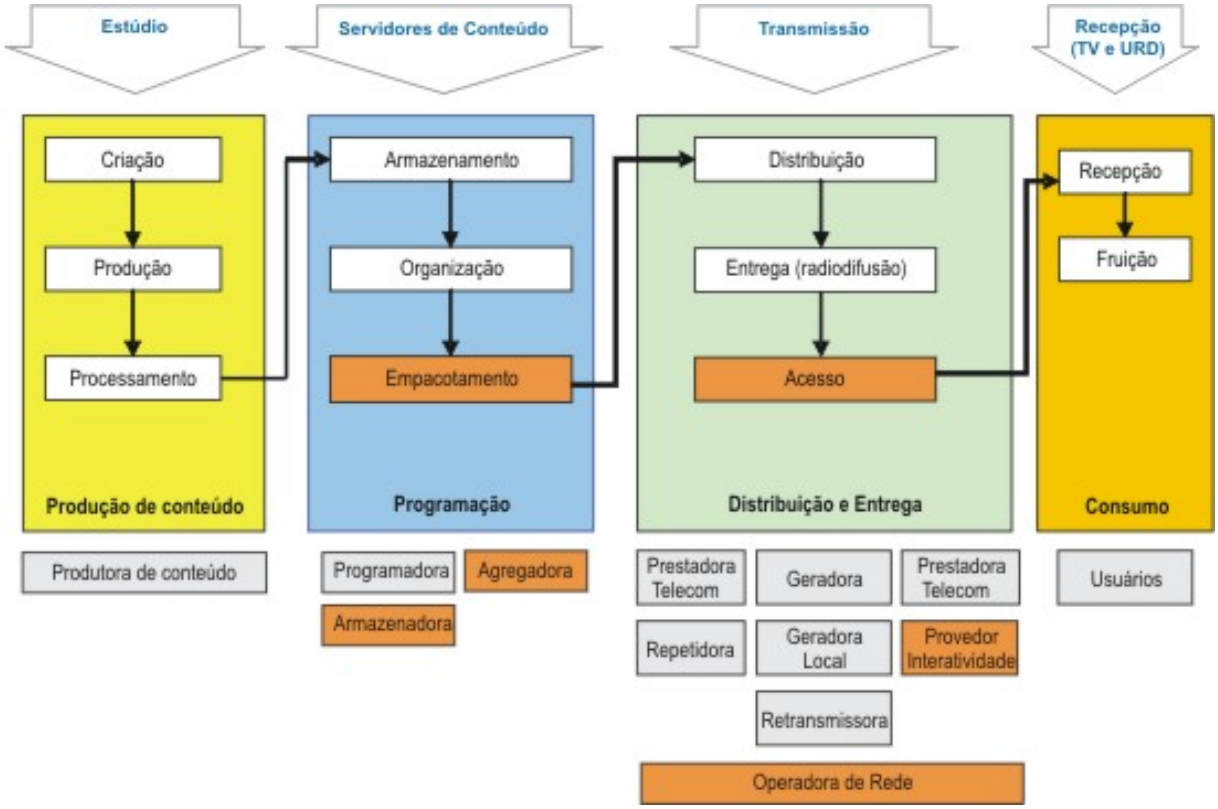


Figura 5.2 - Cadeia de valor da TV Digital Interativa [44]

A primeira etapa corresponde à produção do conteúdo. É nesta etapa que áudio e vídeo são produzidos, bem como as aplicações a serem enviadas juntamente com os conteúdos multimídia, ou seja, esta é a fase onde ocorrem a gravação das cenas, edição e criação dos programas. A partir daí o conteúdo passa para a etapa de programação nos servidores de conteúdo onde é armazenado, organizado e empacotado.

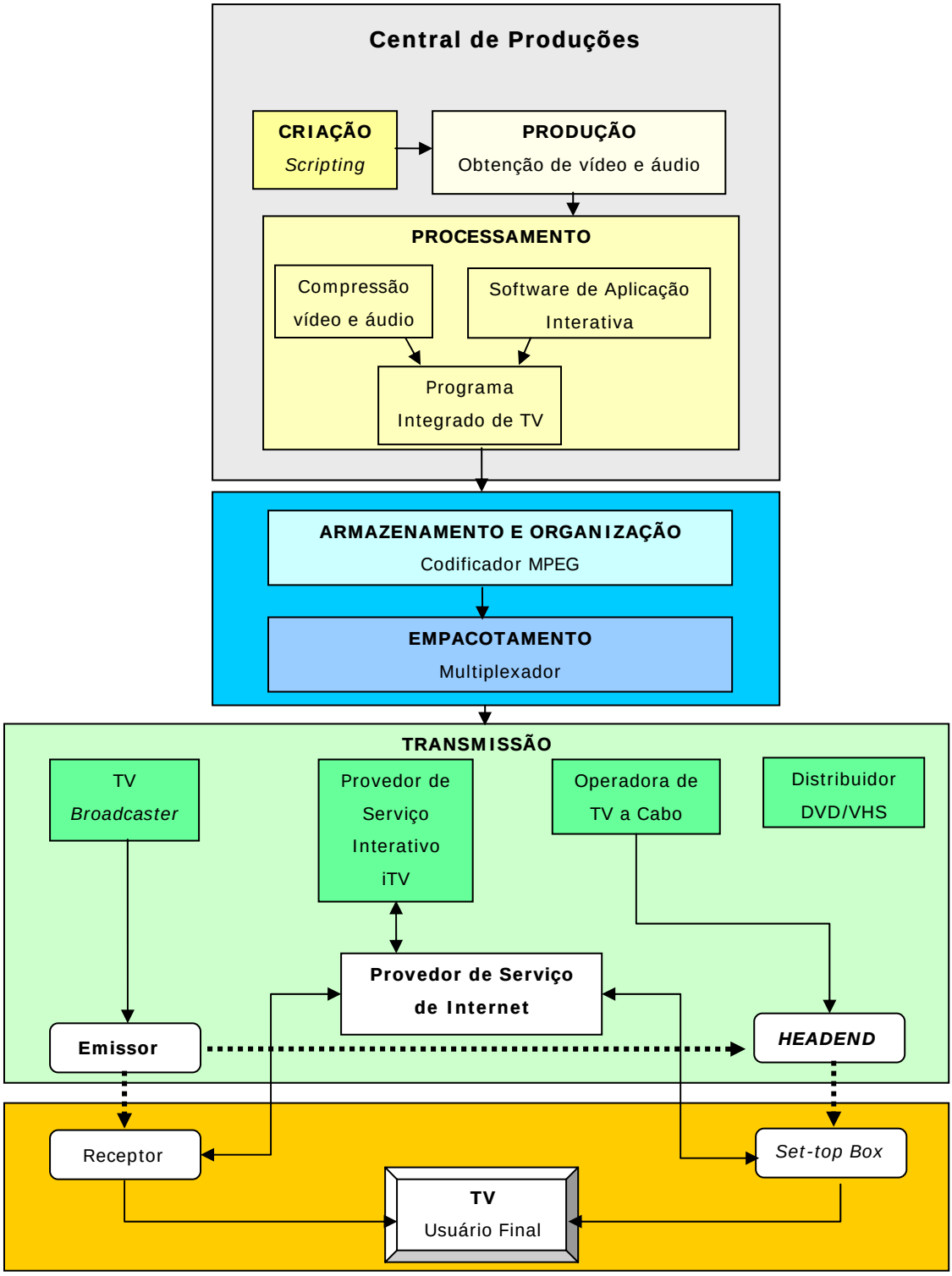


Figura 5.3 - Detalhamento da cadeia de valor da TV Digital Interativa [5]

Da mesma forma, o sinal de áudio é codificado, mas a grande inovação da TV Digital é a possibilidade de transmissão de dados digitais, além dos sinais de áudio e vídeo.

Os dados digitais podem tanto estar relacionados ao conteúdo audiovisual transmitido como também podem ser completamente desvinculados do mesmo.

Os padrões de codificação utilizados em TV Digital têm por função comprimir a informação a ser transmitida a fim de oferecer ao consumidor alta qualidade de áudio e vídeo fazendo uso da menor largura de banda possível.

Uma vez obtidos os fluxos elementares de áudio, vídeo e dados comprimidos e codificados, o multiplexador transforma-os em um único fluxo de dados para que seja realizada a transmissão digital ou armazenamento. O método de multiplexação atualmente utilizado é definido pelo padrão MPEG-2 parte 6 onde o único fluxo de dados (MPEG-2 *System Transport Stream*) é dividido em pacotes de 188 bytes que são transmitidos aos receptores [5]. Os receptores, por sua vez, realizam a demultiplexação deste fluxo extraindo assim as informações de áudio, vídeo e dados originais.

A próxima etapa corresponde ao processo de distribuição e entrega do conteúdo. O sinal multiplexado a ser transmitido é modulado, ou seja, é acoplado a uma portadora onde são acrescidos de informações para facilitar a detecção de erros e o aumento na taxa de transmissão. Os métodos de modulação digital mais utilizados são: *Quadrature Amplitude Modulation* (QAM), *Quadrature Phase Shift Keying* (QPSK), *Coded Orthogonal Frequency Division Multiplexing* (COFDM) e *8 Vestigial Side Band* (8-VSB). A transmissão para Recepção Doméstica pode se dar a partir de quatro meios: terrestre, satélite, cabo e rede IP. A Figura 5.3 permite contemplar os diversos tipos de distribuição.

A última etapa corresponde ao consumo por parte dos usuários. O *Set-Top Box* (Figura 5.4) realiza a sintonização para captar os sinais transmitidos, a demodulação para recuperar o fluxo de dados modulado, a demultiplexação para separar cada tipo distinto de fluxo de dados e a decodificação dos sinais de vídeo, áudio e dados disponibilizando-os para a exibição e/ou serem utilizados pela aplicação.

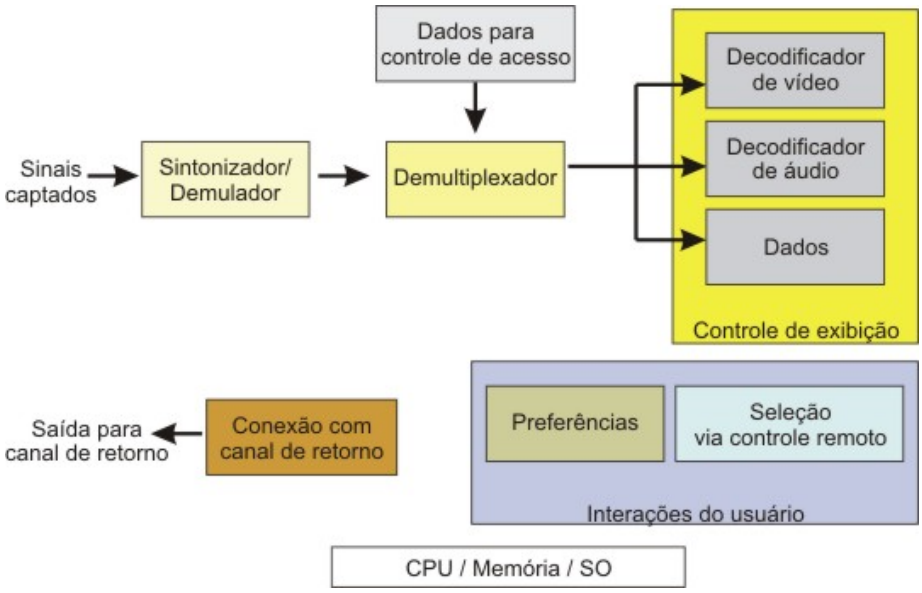


Figura 5.4 - Esquema em módulos de um STB [6]

5.2.1 - O processo de transmissão e distribuição de conteúdo na TV Digital

Inicialmente todas as partes (áudio, vídeo e dados) que compõem um serviço ou canal de TV são codificadas para o padrão MPEG-2 gerando então os chamados *elementary streams* (ES). O agrupamento dos *streams* elementares é conhecido como evento, que no modelo de consumo de serviços da TV digital, corresponde ao elemento atômico de produção de mídia [4].

Um programa corresponde ao encadeamento de um ou mais eventos produzidos por um estúdio, como por exemplo, um *show*. A seqüência de programas controlada pela difusora corresponde ao serviço o qual corresponde à principal unidade de produção e consumo na TV digital. Uma Central de Produções pode fazer uso de um conjunto de serviços produzidos por vários estúdios compondo então o chamado *Bouquet*. Em outras palavras, o *Bouquet* é o agrupamento lógico dos serviços e corresponde à unidade de distribuição das programações de uma Central de Produções.

Um fluxo único de transporte, ou seja, o *Transport Stream* (TS) é gerado, através de um multiplexador MPEG-2, e posteriormente dividido em pacotes de tamanho fixo de 188 bytes os quais possuem um identificador de pacote (PID) no cabeçalho a fim de diferenciá-los dentro do TS que os contém.

As seqüências elementares de bits podem ser organizadas, antes mesmo da multiplexação e formatação em pacotes de transporte, em segmentos *Packetized*

Elementary Stream (PES) de tamanho variável a partir dos pacotes TS que possuem um mesmo PID. A principal finalidade do PES é viabilizar a sincronização das seqüências elementares de bits de um mesmo programa. Obrigatoriamente, as seqüências de áudio e vídeo passam por essa etapa. Cada PES contém em seu cabeçalho informações referentes ao algoritmo de compressão e marcas de temporização do áudio e vídeo (*timestamps*) os quais são utilizados posteriormente na decodificação a fim de sincronizar os sinais recebidos.

É importante salientar que um componente de vídeo de um programa MPEG-2 é disposto em um único *stream* elementar possuindo um único PID. De forma análoga, o componente de áudio associado ao componente de vídeo descrito acima também é disponibilizado em um único *stream* elementar que possui um único PID. Por outro lado, a transmissão de dados pode ser mais complexa que a transmissão de ambos áudio e vídeo pois uma única aplicação pode ser transmitida com vários PIDs associados, assim como várias aplicações podem compartilhar PIDs.

O sinal de TV Digital é então transmitido através do *Transport Stream* (TS) que é gerado a partir do agrupamento dos serviços. Cada TS pode chegar a uma taxa de transmissão efetiva de até 55 Mbps em meio físico de TV a cabo ou de até 25 Mbps em sistemas de distribuição terrestres. A emissora pode ainda transmitir simultaneamente vários TS desde que devidamente modulados em diferentes portadoras.

Juntamente com o conteúdo, são transmitidos pacotes contendo informações específicas sobre a programação MPEG, conhecidos como *Program Specific Information* (PSI). Os pacotes PSI incluem as tabelas de associação de programa (PAT), tabelas de mapeamento de programas (PMT), tabelas com descrição sobre o acesso condicional aos conteúdos transmitidos (CAT), tabela da descrição de organização dos fluxos de transporte na rede (NIT), dentre outras conforme a Tabela 5.1. O processo de criação e empacotamento das tabelas SI juntamente com o conteúdo na composição do fluxo de transporte se dá na etapa de Programação (Figura 5.3).

A fim de viabilizar a transmissão, cada tabela é quebrada em uma determinada quantidade de pacotes chamados seções. A maior parte dos pacotes que contém dados SI utiliza o formato de seção MPEG-2. Uma vez divididas as tabelas em seções, elas são transmitidas como parte de um fluxo MPEG elementar. A tabela completa é transmitida em intervalos regulares de forma a garantir que o receptor receba a cópia da tabela completa. Algumas tabelas são transmitidas em PIDs pré-determinados para que os receptores saibam

onde localizá-las, desta forma, elas podem informar ao receptor onde localizar as outras tabelas das quais necessitam. Adicionalmente, o receptor continua a monitorar os PIDs pré-determinados das tabelas SI pois a emissora pode atualizar o conteúdo de uma tabela SI a qualquer instante. Cada tabela possui um número de versão que é alterado quando a emissora atualiza o conteúdo da tabela. Sendo assim, quando um receptor identifica a alteração da versão da tabela, ele elimina os dados da tabela original e os substitui com a nova cópia.

A estrutura lógica de um fluxo de transporte MPEG-2 exibindo a vinculação da tabela PAT com as tabelas PMT pode ser observada na Figura 5.5.

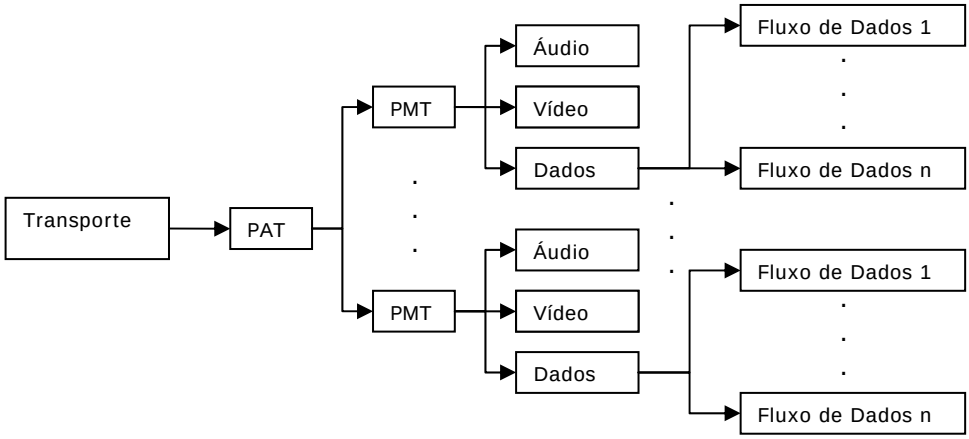


Figura 5.5 - Esquema da estrutura lógica de um fluxo de transporte MPEG-2

Além das tabelas SI, existem diversas outras tabelas utilizadas no ambiente de radiodifusão incluindo as tabelas que transportam informações sobre a ECM, EMM, *downloads* e outras.

Tabela 5.1 - Nomes e funções das tabelas SI [7]

Nome da Tabela	Funções
PAT (*Program Association Table*)	Tabela transmitida em um PID fixo (0x0000) que descreve o PID do pacote do fluxo de transporte da PMT relacionada ao programa transmitido.
CAT (*Conditional Access Table*)	Determina o PID do pacote do fluxo de transporte que contém informações individuais sobre conteúdo de acesso restrito.
PMT (*Program Map Table*)	Contém uma estrutura de dados que especifica os PIDs dos pacotes de vídeo, áudio e dados que constituem o programa transmitido.
NIT (*Network Information Table*)	Contém informações sobre a transmissão como freqüência de modulação e sua vinculação aos programas transmitidos.
SDT (*Service Description Table*)	Contém informações relacionadas ao canal de programação, tais como nome do canal e nome da emissora.
BAT (*Bouquet Association Table*)	Contém informações relacionadas ao *Bouquet*, tais como nome do *Bouquet* e canais de programa contidos no mesmo.
EIT (*Event Information Table*)	Contém informações relacionadas aos programas, tais como nome do programa, data e hora de transmissão, explicação de conteúdo.
RST (*Running Status Table*)	Indica informação do status do programa em execução.
TDT (*Time Date Table*)	Indica a data e hora atual.
TOT (*Time Offset Table*)	Indica a data e hora atual além da diferença entre a hora atual e a indicação de hora local.
LIT (*Local Event Information Table*)	Contém informações relacionadas ao local de evento, tais como discriminação (hora), nome e explicações sobre o local do evento (cena, etc.) no programa.
ERT (*Event Relation Table*)	Indica o relacionamento entre programas e eventos locais, tais como grupos e atributos dos mesmos.
ITT (*Index Transmission Table*)	Descreve as informações relacionadas ao índice de programas no envio dos mesmos.
PCAT (*Partial Content Announcement Table*)	Indica a programação da transmissão de conteúdo parcial na emissão de dados.
ST (*Stuffing Table*)	Torna uma tabela inválida.
BIT (*Broadcaster Information Table*)	Determina os parâmetros sobre a rede de cada emissora.
NBIT (*Network Board Information Table*)	Contém informações sobre a rede da emissora.

Cada uma das tabelas descritas na Tabela 5.1 possui um conjunto de descritores que definem parâmetros com as informações sobre os componentes, acesso condicional dos conteúdos, controle de cópia, tipo de criptografia utilizado, dentre outros.

As estruturas de dados das tabelas PAT, CAT e PMT devem estar de acordo com o formato especificado nos Sistemas MPEG-2 (ITU-T H.222.0, ISO/IEC 13818-1 [8]) e podem ser observadas nas Figuras 5.6, 5.7 e 5.8.

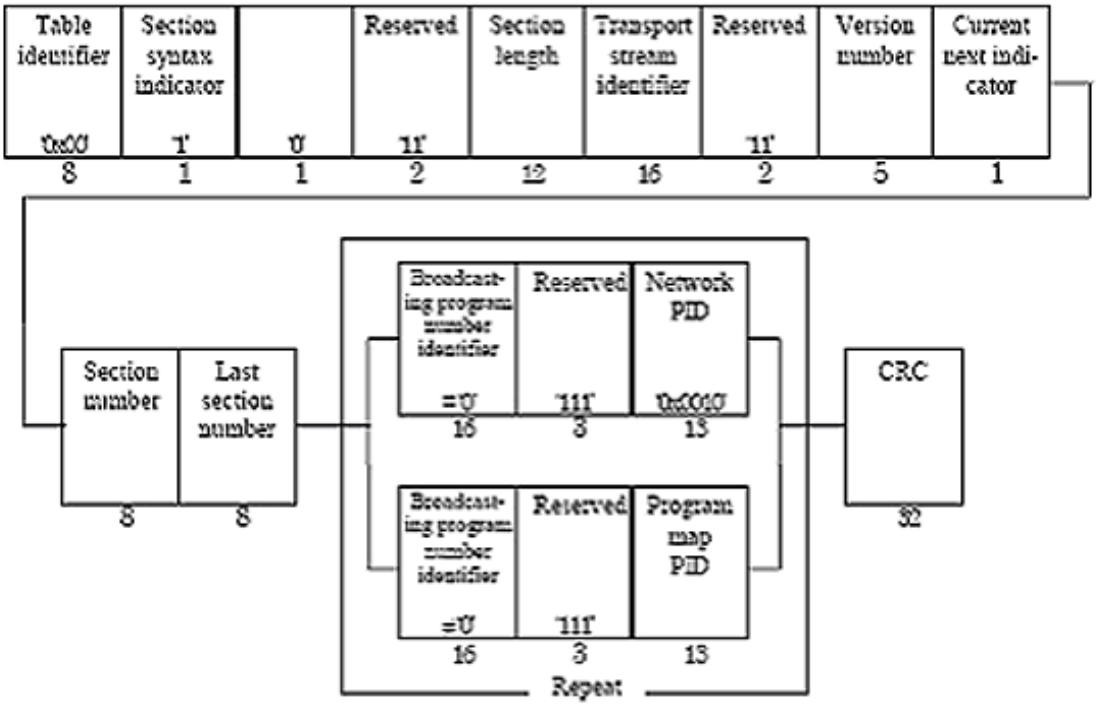


Figura 5.6 - Estrutura de dados da PAT [7]

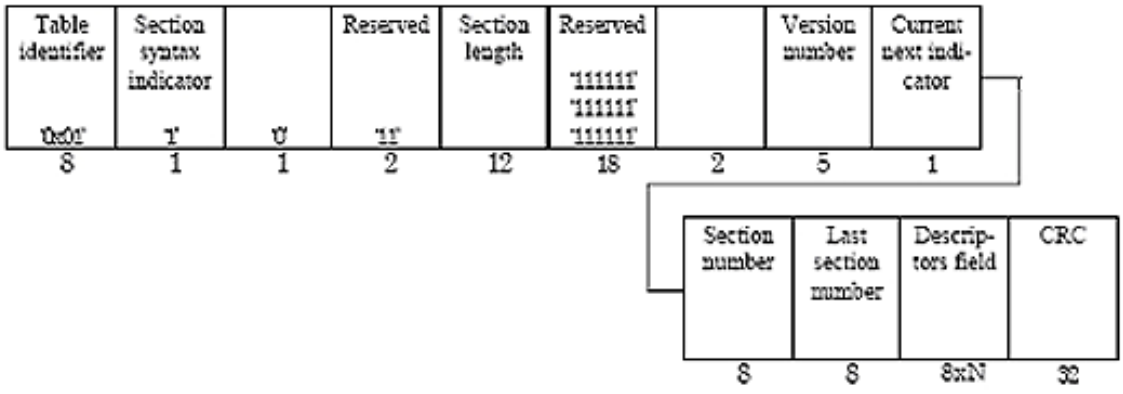


Figura 5.7 - Estrutura de dados da CAT [7]

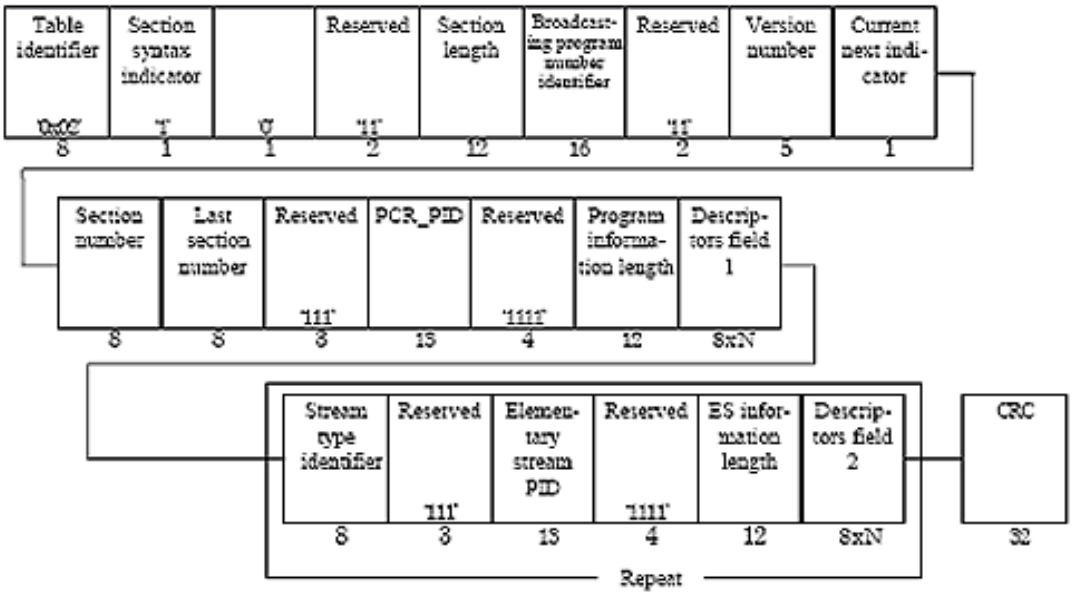


Figura 5.8 - Estrutura de dados da PMT [7]

5.2.2 - Os padrões de TV Digital

Atualmente existem três padrões mundiais para sistema de televisão digital interativa que, definem seus próprios padrões para modulação do sinal de difusão, transporte de fluxos elementares de áudio, vídeo, dados e aplicações, codificação e qualidade de áudio e vídeo. São eles: *Digital Video Broadcasting* (DVB) [9] – padrão predominantemente europeu, mas que também é utilizado em diversos outros países, principalmente na Ásia e Oceania; o padrão *Advanced Television Systems Commitee* (ATSC) [10] – padrão tipicamente americano, mas que também é utilizado no Canadá, Coréia do Sul, Taiwan e Argentina; e por último o padrão *Integrated Services Digital Broadcasting* (ISDB) [11] – padrão japonês de TV Digital. Além destes, existe a versão do padrão europeu utilizada na Austrália, pois o padrão europeu aceita que sejam feitas alterações em suas configurações. Outros países já procuram desenvolver padrões próprios, adaptados desde o começo às suas necessidades, como é o caso da China e do Brasil.

A Tabela 5.2 resume os aspectos mais relevantes que caracterizam os três principais sistemas da TV digital disponíveis atualmente no mundo:

Tabela 5.2 - Padrões internacionais de TV Digital [9][10][11]

Aspecto	ATSC	DVB	ISDB
Modulação	8-VSB	COFDM	COFDM
Codificação de Áudio	Dolby AC-3 (proprietário)	MPEG-2 *Digital sound* (aberto)	MPEG-2 AAC
Codificação de Vídeo	MPEG-2	MPEG-2	MPEG-2
Tipos de Sistema	ATSC-C ATSC-T	DVB-C DVB-S DVB-T	ISDB-C ISDB-S ISDB-T
Middleware	DASE	MHP	ARIB
Ênfase	TV de alta definição; TV aberta	Multiprogramação, interatividade e novos serviços; TV paga	TV de alta definição, recepção móvel e portátil; TV paga
Adotado	Estados Unidos, Canadá, Coréia do Sul, Taiwan, México	Europa, Austrália, Nova Zelândia, Rússia	Japão

A convergência buscada em termos de tecnologia referente a Televisão Digital Interativa (TVDI) também procura abranger aspectos relacionados aos STBs que podem ter diferentes arquiteturas, capacidades de processamento, armazenamento e comunicação, além de sistemas operacionais incompatíveis.

Neste cenário de *hardware* e *software* heterogêneos, as aplicações devem ser escritas em versões compatíveis para cada combinação de *hardware* e sistema operacional dos diversos tipos de STBs. Desta forma, a heterogeneidade de plataformas faz do desenvolvimento de aplicações para TVDI uma atividade que requer a utilização de padrões “de direito” (propostos por organizações normativas ou órgãos governamentais) e/ou “de fato” (adotados de forma prevalente pelo mercado), permitindo viabilizar a sua adoção em larga escala.

Para tornar mais eficiente e portável o processo de desenvolvimento de aplicações, resultando na consolidação do TVDI, os STBs devem prover às aplicações um conjunto de interfaces genéricas, padronizadas e bem detalhadas – a *Application Programming Interface* (API) – a qual deve abstrair as especificidades e heterogeneidades de *hardware* e *software* dos diversos tipos de dispositivos receptores.

A fim de prover esta API genérica, uma camada de *software* adicional - o *middleware* ou *software* de interface - deve ser incluído entre o sistema operacional e as aplicações, conforme visto na Figura 5.9. Desta forma, o *middleware* oferece um serviço padronizado às aplicações, ocultando as peculiaridades das camadas de *hardware* e sistema

operacional, que dão suporte às facilidades primordiais de codificação, transporte e modulação de um sistema de televisão digital.

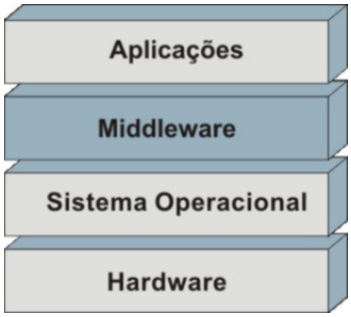


Figura 5.9 – O *middleware* na arquitetura do terminal de acesso

5.2.2.1 - *Middlewares*

Existem diversos *middlewares* proprietários, tais como o OpenTV da empresa OpenTV [45], o MediaHighway da empresa NDS [46] e o MicrosoftTV [47]. Da mesma forma existem os *middlewares* abertos (Tabela 5.2), que são o DASE no padrão ATSC, o *Multimedia Home Plataform* (MHP) no padrão DVB e o ARIB-STD-B24 no padrão ISDB sendo estes, em maior ou menor grau, baseados na linguagem de programação Java.

É notória a tendência mundial para a adoção de padrões abertos onde, segundo Morris e Smith-Chaigneau [12] o MHP é atualmente o padrão mais aceito neste mercado.

O MHP é uma API desenvolvida pelo projeto DVB que define uma interface genérica entre as aplicações digitais interativas e os terminais onde estas aplicações são executadas. A arquitetura do MHP é definida em termos de três camadas: recursos, software de sistema e aplicações, conforme descrito na Figura 5.10.

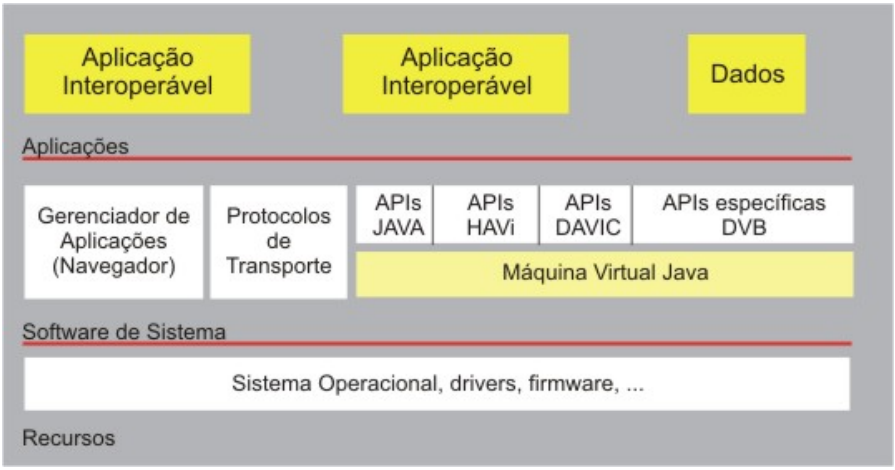


Figura 5.10 - Arquitetura MHP [13][14]

Os recursos incluem recursos de hardware e software, e são acessados pelo MHP de forma transparente, ou seja, uma aplicação deve ter acesso a todos os recursos conectados localmente como se fossem elementos de uma única entidade. Exemplos típicos de recursos MHP são processamento MPEG, dispositivos I/O, CPU, memória e sistema gráfico.

O software de sistema usa os recursos disponíveis a fim de prover para as aplicações uma visão abstrata da plataforma e inclui um navegador cujo objetivo principal é controlar o MHP e aplicações em execução.

As aplicações implementam serviços interativos como os softwares que são executados em uma ou mais partes de hardware.

O MHP é baseado na plataforma DVB-J que inclui uma máquina virtual similar à *Java Virtual Machine* (JVM) especificada pela *Sun Microsystems* [14].

Os arquivos necessários para executar uma aplicação em um receptor MHP são acessados pelo receptor via download a partir da emissora. A aplicação é executada pela máquina virtual do Java e utiliza as funcionalidades do dispositivo receptor através da implementação das interfaces descritas na especificação MHP.

O DVB criou três perfis de aplicação procedural MHP conforme o grau de interatividade da mesma, conforme descrito na Figura 5.11 [14]:

- ***Enhanced Broadcast Profile*** **(ES 201 812 – MHP 1.0**): o qual define as aplicações baixadas diretamente via radiodifusão permitindo apenas interatividade local. Corresponde ao perfil de aplicações para STBs de configuração mais simples**;**

- ***Interactive Broadcast Profile*** **(ES 201 812 – MHP 1.0**): o qual prevê a existência de um Canal de Interatividade permitindo a interatividade do usuário com o programa baixado. Sendo assim, as aplicações podem ser baixadas tanto por radiodifusão como através do próprio canal de interatividade e desta forma acessar dados remotos através do mesmo;
- ***Internet Access Profile*** **(TS 102 812 – MHP 1.1**): o qual dá acesso pleno à Internet via TV Digital ou STB**.**

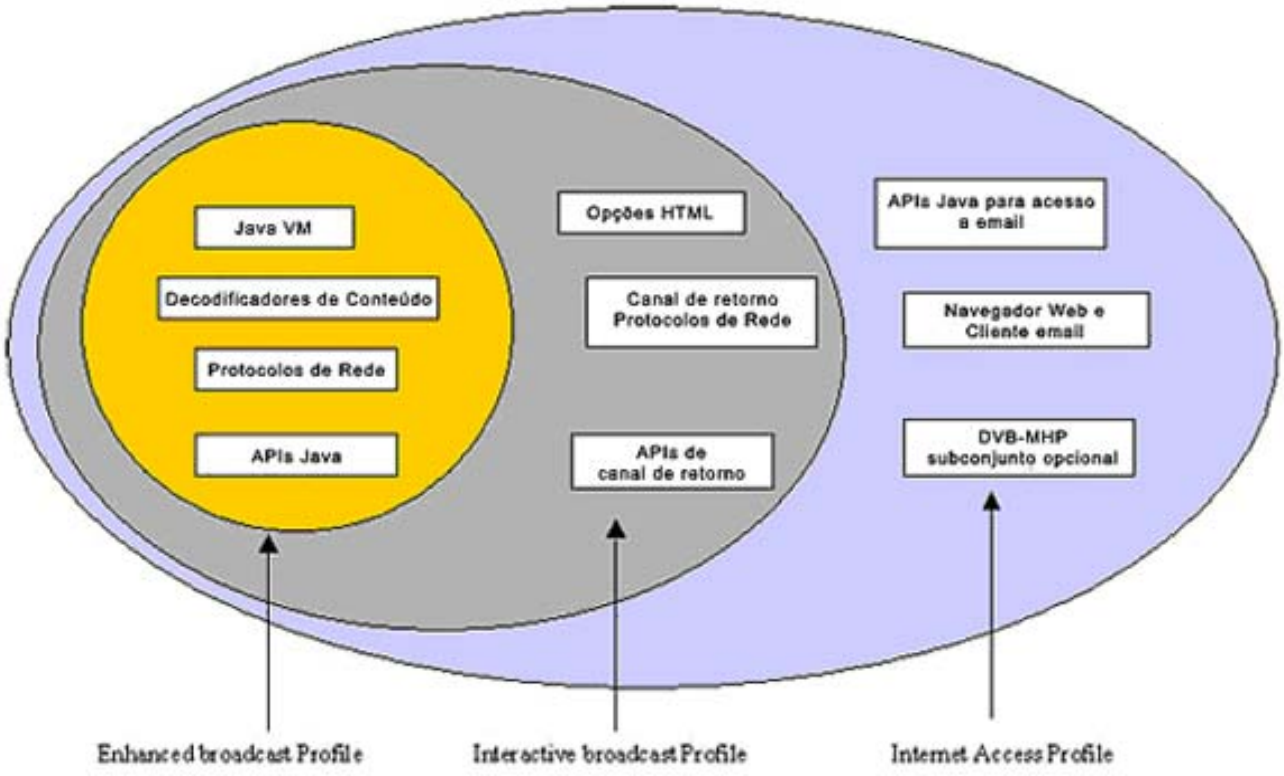


Figura 5.11 - Perfis de aplicação procedural MHP [14]

Inicialmente, o MHP foi projetado para implementar as plataformas DVB, mas acabou se tornando referência mundial tendo como conseqüência uma demanda para oferecer interoperabilidade a outras plataformas de TV digital. Tal demanda originou o *Globally Executable MHP* (GEM).

O GEM é um subconjunto do MHP que foi designado levando-se em consideração as especificações de interoperabilidade nos vários padrões de *middleware* abertos [15].

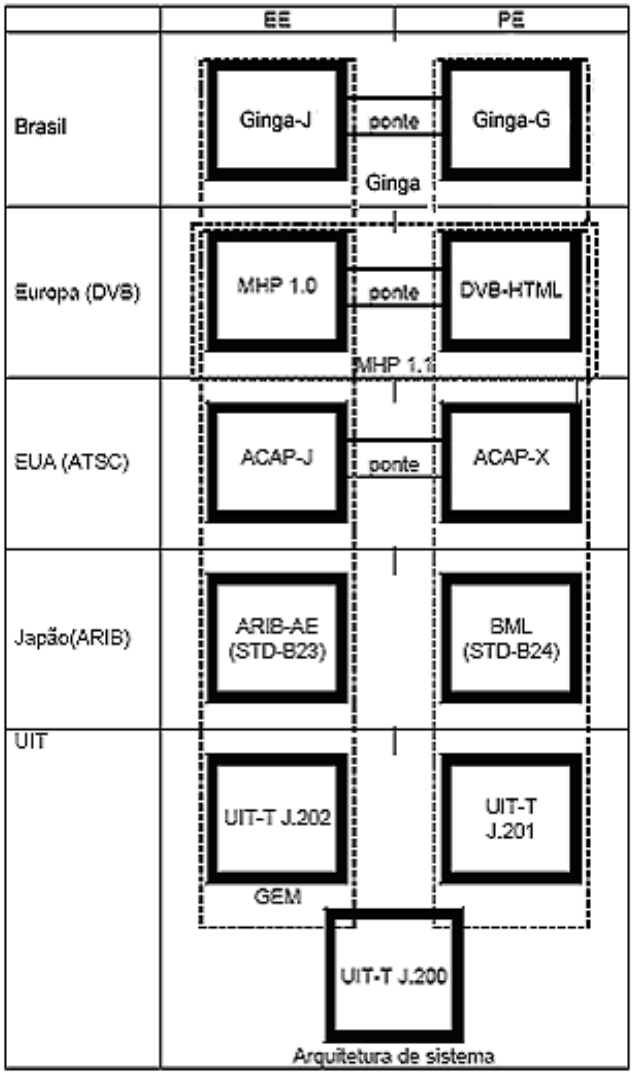
Tais especificações incluem: especificações técnicas de interoperabilidade levantadas de padrões de *middlewares* já existentes como *OpenCable Application Platform* (OCAP) e *Digital TV Application Software Environment* (DASE), especificações relacionadas a sistemas de transmissão individual como a escolha do sistema de modulação, mecanismos de entrega de conteúdo e sistemas de acesso condicional, requisições diversas de mercado por parte das operadoras de rede.

Pode-se afirmar que o GEM é um *framework* cujo objetivo principal é permitir que várias organizações possam harmonizar as especificações técnicas tais como a seleção de um único dispositivo de execução e, quando possível, um conjunto de funções (API) comuns aos diferentes *middlewares* resultando na interoperabilidade entre os tipos heterogêneos de terminais de acesso.

O *middleware* de referência desenvolvido para o Sistema Brasileiro de TV Digital inicialmente batizado como FlexTV e depois tendo o nome alterado para Ginga, foi implementado de forma a manter a compatibilidade com o GEM, além de incluir características adicionais a fim de suprir requisitos apontados pelo Governo Brasileiro, incorporando inovações não disponíveis em nenhum outro *middleware* de TV Digital [16].

A Figura 5.12 apresenta um diagrama que descreve a situação atual da padronização do ambiente de aplicação multimídia na UIT (União Internacional de Telecomunicações) e em regiões específicas tanto para aplicativos baseados em linguagem procedural, os quais são processados em uma máquina de execução – *executive engine (EE)*, como também aplicativos baseados em codificação declarativa, os quais são processados em uma máquina de apresentação – *presentation engine (PE)*.

O conjunto de recomendações publicado pela UIT, UIT-T: J.200 [48], J.201 [49] e J.202 [50] têm como objetivo a harmonização dos sistemas de TV Digital em diferentes níveis (Figura 5.12).



J.200 Worldwide common core - Application environment for digital interactive television services
J.201 Harmonization of declarative content format for interactive TV applications
J.202 Harmonization of procedural content formats for interactive TV applications

Figura 5.22 - Padrões do ambiente de aplicação multimídia (EE e PE) atualmente disponíveis

A recomendação J.200 define uma arquitetura de alto nível para um conjunto de componentes de forma a prover uma variedade de funcionalidades requeridas por aplicações interativas conforme a Figura 5.13. As recomendações J.201 e J.202 especificam um núcleo comum para execução de aplicações declarativas e procedurais, respectivamente.

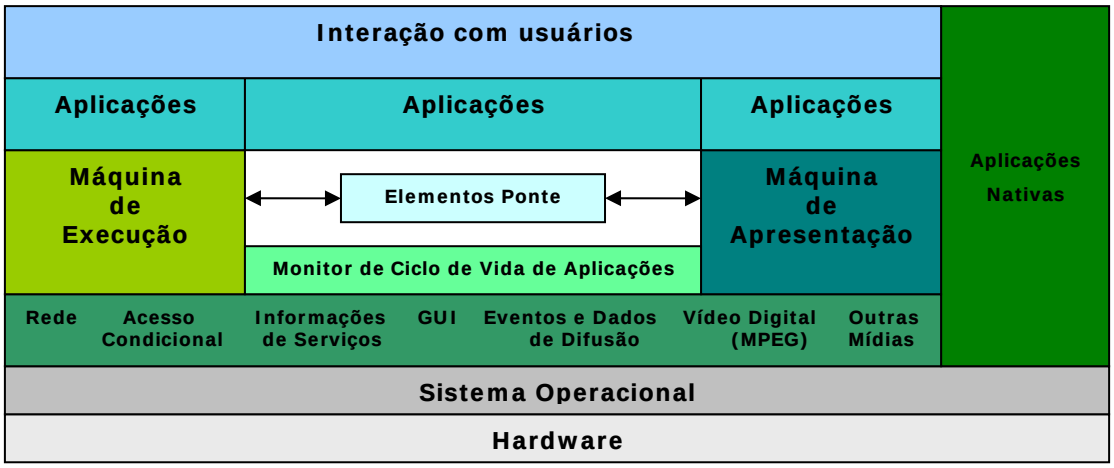


Figura 5.33 - Arquitetura de ambiente de execução de aplicações para TV Digital prevista pela recomendação ITU - J.200 [16]

A Figura 5.14 mostra a arquitetura proposta para o *middleware* do Sistema Brasileiro de Televisão Digital.

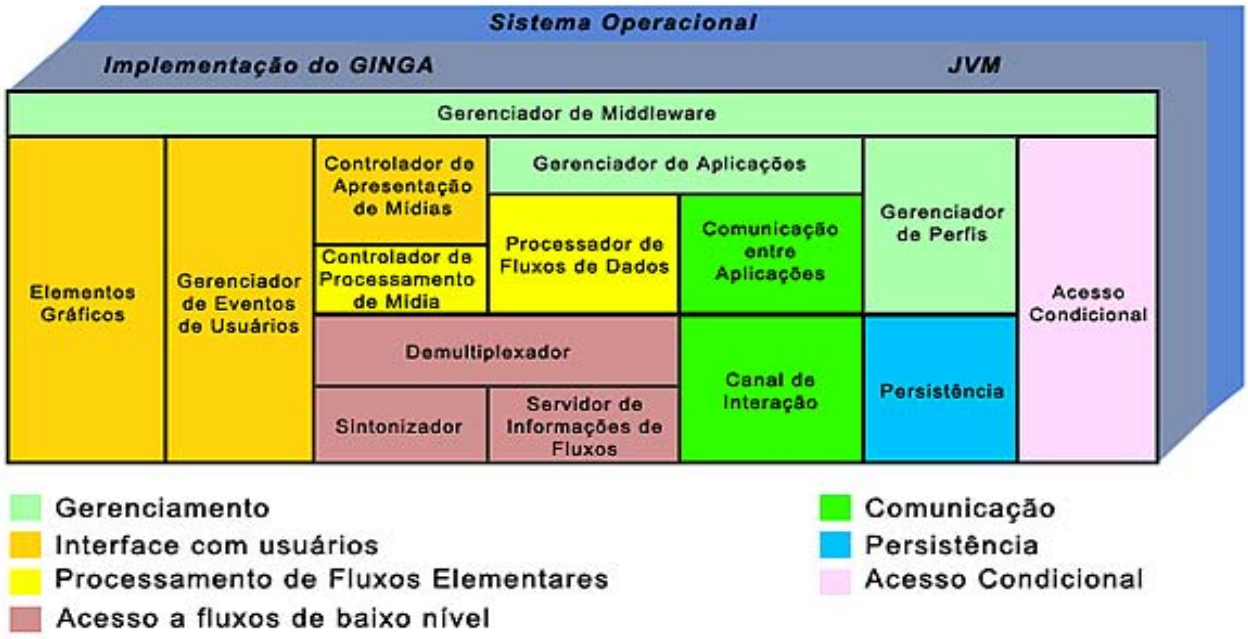


Figura 5.44 - Arquitetura de alto nível proposta para o *middleware* do sistema brasileiro de TV Digital [17]

6 – MECANISMOS DE PROTEÇÃO EM TV DIGITAL

6.1 - SEGURANÇA NA TRANSMISSÃO ELETRÔNICA DE CONTEÚDO DIGITAL RESTRITO

Devido à existência da restrição de acesso aos conteúdos digitais, são possíveis diferentes tipos de ataques realizados ao conteúdo digital protegido. A partir daí, podem ser identificados os seguintes requisitos básicos de segurança:

- Proteção de direitos autorais para distribuição eletrônica de conteúdo multimídia;
- Verificação de integridade do conteúdo multimídia, detectando quaisquer adulterações efetuadas e assegurando que o dado recebido é preciso, completo e consistente;
- Proteção do próprio conteúdo contra acessos não autorizados no processo de distribuição em meios heterogêneos;
- Criação e rastreamento de cópias não autorizadas determinando a origem das mesmas;
- Mecanismos de segurança relacionados à privacidade, identificação, autorização e transmissão do conteúdo.

Os mecanismos de proteção podem ser categorizados da seguinte forma [18]:

- **nível de aplicação**: diversos mecanismos de proteção atuam na transmissão, transações financeiras, fluxo de dados e serviços;
- **gerenciamento de mecanismo de proteção**: princípios, métodos e tecnologias utilizadas a fim de garantir direitos de propriedade intelectual, segurança e direitos do consumidor;
- **arquitetura do sistema de gerenciamento de proteção**: definição e criação de um *framework* abstrato para arquiteturas de gerenciamento de proteção, troca de mecanismos utilizados para o gerenciamento de proteção e formas de comunicação entre sistemas e as entidades pertencentes aos sistemas;
- **definições de metadados**: linguagem metadados cujo objetivo é descrever os parâmetros para os gerenciadores de proteção e seus componentes.

Neste contexto, a aplicação das técnicas de ocultação de dados e outras medidas de segurança que têm como objetivo reforçar as regras de gerenciamento de direitos autorais

cresce rapidamente com a expansão de comércio e transmissão de conteúdo digital por meio eletrônico.

Quando aplicados em sistemas de proteção de propriedade de conteúdo, um esquema de ocultação de dados utilizado deve ser suficientemente robusto de forma a resistir às manipulações comuns de processamento de dados. Em caso de disputas legais referentes à propriedade do conteúdo, a informação embutida pode ser usada como prova de identificação do proprietário verdadeiro.

6.1.1 - Inclusão de dados de forma oculta no conteúdo digital.

A ocultação eficiente de informações requer que a informação embutida (mensagem ou metadados) no sinal hospedeiro (imagem, vídeo, áudio, texto, etc) seja imperceptível e pode ser utilizada em aplicações diversas como proteção de conteúdo, proteção de propriedade, prevenção contra cópias ilegais, rastreamento de uso, preservação de conteúdo, etc.

Segundo Malik [19], as aplicações de ocultação de dados podem ser classificadas em três grupos abrangentes:

- **Esteganografia** a qual explora métodos de ocultar a existência de mensagens escondidas. Estes métodos incluem tinta invisível, microdot, assinatura digital e outros.
- **Marca d'Água (*watermarking*) digital** que compreende um sinal portador de informação embutido de forma imperceptível no dado digital podendo ser extraído posteriormente para realizar asserções sobre o dado hospedeiro. Em outras palavras, corresponde a um processo que encaixa em um determinado objeto (nesse caso, o dado hospedeiro a ser autenticado), um sinal cujo objetivo é levar informações sobre este objeto. Pode ser utilizada na proteção e/ou autenticação de conteúdo.
- ***Fingerprinting* digital** que corresponde a um método de inserção de rótulos ou identificação numérica em um conteúdo digital a ser distribuído. É um mecanismo bastante utilizado para rastrear cópias não autorizadas do conteúdo digital. O rastreamento se torna possível, pois o proprietário/distribuidor insere uma *fingerprint* que identifica o comprador em cada cópia distribuída. Caso seja localizada posteriormente uma cópia não autorizada do conteúdo protegido, sua origem poderá ser rastreada através da *fingerprint* única inserida no conteúdo [20]. O problema com o protocolo descrito acima é que não há como provar que de fato a cópia não autorizada foi gerada pelo comprador ou pelo próprio

distribuidor. Sendo assim, o revendedor pode distribuir várias cópias de um único comprador sem ter pago os valores referentes aos *royalties* do autor para cada cópia e ainda declarar que as cópias foram feitas ou distribuídas ilegalmente por tal comprador. Uma solução possível para este problema é a instituição de uma entidade de confiança como TTP (*Trusted Third Party*) a qual seria a responsável pela inserção e detecção da *fingerprint* no conteúdo protegido em caso de disputa, porém este processo nem sempre é viável, pois, além da sobrecarga de processos centralizados na TTP, existe ainda a possibilidade de acesso ao conteúdo (e adulteração do mesmo) na transmissão efetuada entre o revendedor e a TTP e entre a TTP e o consumidor.

No contexto de rastreamento de cópias não autorizadas, um esquema robusto de *fingerprinting* pode ser utilizado, desde que a identificação única seja embutida em cada cópia do conteúdo anteriormente à distribuição do mesmo.

Esquemas de ocultação de dados devem suportar manipulações de dados como adição de ruído, compressão, conversão analógico-digital, escalonamento, filtragem, conversão de formato, cifração, decifração, “embaralhamento”, etc. Porém a importância relativa de cada atributo depende da aplicação em questão.

Algumas características desejáveis para tais sistemas são [19]:

- **Robustez**: capacidade que a marca d’água tem de suportar ataques intencionais ou não intencionais os quais podem assumir a forma de processamento, como por exemplo, compressão de dados e efeitos de vídeo, ou tentativas deliberadas de remoção de uma ou mais partes do dado embutido. O nível de robustez desejado é determinado basicamente pelo tipo da aplicação da marca d’água.
- **Fidelidade**: percentual que demonstra a similaridade entre a mídia hospedeira e sua versão com dado embutido.
- **Capacidade**: se refere à quantidade de informação que um esquema de ocultação de dados pode embutir no sinal hospedeiro sem aumento relevante de distorção na mídia original.
- **Detecção pública ou privada**: se refere à disponibilidade do dado hospedeiro original no processo de detecção da informação. Caso o dado hospedeiro original esteja disponível no processo de detecção da marca d’água, o processo é conhecido como detecção com acesso à informação (*informed*) ou detecção privada, a qual é geralmente utilizada em processo de *fingerprinting*, autenticação de dados e detecção de adulteração de dados. Por outro lado, se o dado hospedeiro original não se encontra

disponível na aplicação de detecção, o processo é conhecido como detecção cega (*blind*) ou pública, a qual é o tipo geralmente utilizado para identificação de propriedade e *copyright*.

- **Taxa "Falso Positivo":** corresponde à freqüência de detecção de informação embutida em mídia não marcada.
- **Capacidade de comportar múltiplas marcas d'água**: refere-se a capacidade de embutir mais de uma marca na mesma mídia hospedeira.
- **Custo**: refere-se ao custo computacional da informação embutida e do processo de detecção, característica esta extremamente importante para aplicações em tempo real, como monitoração de transmissão e autenticação de conteúdo *on-line*.

6.2 - *DIGITAL RIGHTS MANAGEMENT*

O gerenciamento de direitos autorais (DRM – *Digital Rights Management*) corresponde a um conjunto de tecnologias, ferramentas e processos que visa proteger a propriedade intelectual de conteúdo digital durante seu ciclo de vida, sendo componente essencial e determinante no mercado de multimídia eletrônica, estando relacionado à proteção, distribuição, modificação e aplicação dos direitos e permissões associados ao uso de conteúdo digital. As responsabilidades primárias do sistema de gerenciamento de direitos autorais são: transmissão segura e confiável de conteúdo aos usuários, prevenção de acesso não autorizado, garantia de aplicação das regras de utilização e monitoração do uso de conteúdo [3]. Em outras palavras, a tecnologia de gerenciamento de direitos autorais (DRM) envolve o controle de acesso à informação, ou seja, os consumidores demandam acesso simplificado aos produtos adquiridos enquanto as companhias geradoras de conteúdo procuram proteger a propriedade intelectual do acesso ou duplicação não autorizados. Desta forma, o DRM situa-se entre estas duas partes na tentativa de apresentar um compromisso eficiente entre consumidores e produtores.

O gerenciamento de DRM se baseia em três passos distintos [21]. O primeiro passo compreende a obtenção por parte do sistema DRM das condições de acesso para o conteúdo protegido, identificando as restrições impostas pelo possuidor dos direitos autorais. Tais condições podem abranger critérios que definem acesso por tempo limitado, acesso por uma quantidade de vezes limitada, necessidade de pagamento para obtenção do acesso, etc. Para a especificação das condições de acesso alguns sistemas DRM utilizam linguagens de expressão de direitos (*rights expression languages* - REL) ou protocolos que

permitem regras de acesso flexíveis, enquanto outros sistemas especificam regras rígidas de acesso que são aplicadas a todo conteúdo protegido. Atualmente os dois padrões mais usados para as REL são o *Open Digital Rights Language* (ODRL) e o *eXtensible rights Markup Language* (XrML).

O ODRL é um padrão aberto criado especificamente para o tratamento de direitos autorais e é definido a partir de dois esquemas de declarações: uma para a declaração dos direitos de acesso e a outra para expressão dos termos e condições aplicáveis a qualquer tipo de conteúdo.

Já o padrão XrML é provavelmente a especificação mais utilizada para DRM. Além de utilizado nos produtos Microsoft da linha Windows Media Server 2003, também foi incorporado pelo grupo MPEG como *Rights Expression Language* para o padrão MPEG-21. Este padrão tem por objetivo definir um *framework* genérico aplicável ao processo de armazenamento, distribuição e uso de recursos multimídia, porém com possibilidade de ser utilizado em praticamente qualquer tipo de conteúdo.

Ambas, XrML e ODRL, definem conceitos bastante similares pois são baseadas na XML (*eXtensible Markup Language)*, porém a XrML é mais complexa e provê descritores que não existem na ODRL, ou seja, a principal diferença entre as duas especificações é o número de descritores no dicionário de dados de ambas para a declaração de direitos, permissões ou condições de acesso. Desta forma, uma declaração ODRL pode ser mapeada para a sintaxe XrML, porém o inverso nem sempre se aplica.

O segundo passo é, após a obtenção das condições de acesso, efetuar a vinculação de tais condições ao conteúdo de forma persistente. Isto é tipicamente realizado através de marcas d'água ou metadados.

Por último, o terceiro passo corresponde à segurança que previne o logro do sistema DRM através da modificação das condições de acesso.

O acréscimo de proteção persistente ao conteúdo é a forma mais efetiva de controlar e rastrear o acesso ao mesmo. Tal proteção é implementada através de tecnologia de proteção de arquivos por meios de cifração e permissão de acesso somente depois que a entidade que deseja obter acesso (usuário ou dispositivo) tem sua identidade autenticada e direitos de acesso verificados. A proteção nos sistemas DRM é dita persistente, pois é mantida com o conteúdo independente da utilização e transmissão do mesmo, em oposição aos arquivos que se encontram em um dado servidor que por sua vez perdem a proteção de

acesso uma vez que são transferidos do servidor, ou seja, que saem do alcance do mecanismo de controle de acesso.

As soluções de proteção persistente de conteúdo digital consistem basicamente de três itens [22]:

1. Empacotamento de conteúdo e metadados em arquivos com implementação de mecanismo de segurança, chamados pacotes, *containers*, envelopes, etc. O objetivo do empacotamento de conteúdo é fazer com que todos os acessos ao conteúdo protegido sejam administrados pelo sistema DRM. Caso o conteúdo esteja disponível sem empacotamento seguro, o mesmo pode ser acessado ou copiado diretamente. Por outro lado, o acesso direto ao conteúdo empacotado não provê acesso ao conteúdo a não ser que o modo de segurança aplicado seja derrotado. Desta forma, o empacotamento é normalmente acompanhado de cifração onde o conteúdo é embaralhado e se torna inteligível a não ser que a chave de decifração seja conhecida. Tal chave é fornecida pelo sistema DRM somente quando todas as condições de acesso especificadas pelo possuidor dos direitos autorais do conteúdo forem satisfeitas.
2. Controladores dos dispositivos de acesso do cliente os quais autenticam a identidade do dispositivo e/ou usuário que requer o acesso ao conteúdo, verificam o tipo de acesso requisitado, efetuam a decifração do conteúdo e providenciam o acesso. Os controladores podem também dar início a transações financeiras quando necessário.
3. Servidores de licenciamento que criam e distribuem licenças de acesso cifradas (muitas vezes denominadas "*tickets*", "*permits*" ou "*vouchers*") as quais descrevem para quem as permissões de acesso são garantidas e as condições sob as quais as permissões existem. Os sistemas DRM que não utilizam servidores de licenciamento inserem as descrições de direitos de acesso diretamente em cada arquivo de conteúdo no empacotamento de dados.

O sistema DRM usa cifração como base para as funções relacionadas à segurança, o que normalmente envolve processos de transmissão de conteúdo seguro, transmissão da chave de acesso ao conteúdo e dos direitos de acesso e autenticação do usuário bem como licenças de *software*, chaves de *hardware* e números seriais, dentre outros.

Referente ao processo de segurança de conteúdo restrito, os mecanismos de transporte devem prevenir o acesso não autorizado desde a origem até o dispositivo de acesso onde o conteúdo será consumido. Isto é eventualmente conhecido como segurança "*end-to-end*" e engloba o processo de segurança deste a etapa de radiodifusão, distribuição na rede (incluindo a Internet, redes privadas e dispositivos dentro do próprio ambiente do usuário) e armazenamento em mídia (como disco de vídeo digital, CD, disco rígido ou fita magnética). Uma forma de obter a segurança "fim-a-fim" é forçar a autenticação dos dispositivos de acesso antes mesmo que o conteúdo seja enviado e recebido. Este processo de autenticação ocorre quando ambos dispositivos, o que envia e o que recebe, são concordantes. Um dispositivo concordante é aquele que tem suporte para a forma de acesso e protocolos de segurança do sistema DRM.

Além disto, o sistema DRM deve permitir renovação das especificações de segurança estabelecidas para os dispositivos de forma que os modos de segurança definidos possam ser recuperados ou atualizados mesmo no caso de dispositivos cuja segurança tenha sido comprometida. Muitos sistemas de proteção de conteúdo efetivam o processo de renovação como revogação do direito de acesso do dispositivo. No caso das informações secretas contidas em um dispositivo concordante serem acessadas indevidamente, e a partir daí utilizadas em dispositivos não concordantes a fim de fazê-los acessar o conteúdo se passando por um dispositivo concordante, a identificação do dispositivo comprometido pode ser adicionada a uma lista de revogação a qual é, por sua vez, distribuída a todos os dispositivos concordantes. Desta forma, os dispositivos "pirateados" não conseguirão passar pelo processo de autenticação e consequentemente não conseguirão acessar o conteúdo protegido.

Atualmente, dentre as ferramentas mais empregadas no campo do DRM, podem ser citados os processos de Assinatura Digital, Marca D'água, Controle de Cópia, Acesso Condicional (*Conditional Access* - CA), ou mesmo combinação destes processos [23].

O Sistema de Assinatura Digital está focado na integridade do conteúdo transmitido, ou seja, na confirmação de que o conteúdo original transmitido não foi alterado entre o emissor e o receptor, examinando o conteúdo e gerando um valor de tamanho fixo o qual é similar a um *snapshot* do conteúdo naquele momento. Caso necessário, posteriormente poderão ser calculados novos valores e comparados ao valor inicial. Desta forma se o novo valor obtido não for igual ao primeiro valor, sabe-se que o conteúdo foi alterado.

A técnica de inserção de marcas d'água é utilizada tanto na identificação de propriedade e direitos autorais como na autenticação de conteúdo.

Especificamente em relação ao processo de identificação de propriedade e direitos autorais, é bastante comum o uso de marcas d'água juntamente com a cifração do conteúdo de acesso restrito. As técnicas de cifração são essenciais e o processo de inserção de marca d'água complementa a cifração do conteúdo restrito, oferecendo novas possibilidades, como por exemplo, identificação do proprietário dos direitos autorais, proteção contra cópia através da indicação e alteração do número de cópias realizadas, controle de acesso através da indicação dos direitos de acesso e uso do conteúdo e rastreamento de conteúdo através da indicação do usuário.

Quando aplicados no contexto de autenticação de conteúdo, em geral usam-se esquemas de proteção que podem detectar e provocar uma auto-invalidação ocasionada por modificações mínimas do conteúdo protegido. Para isto pode-se usar um sistema de marcas d'água frágeis ou semifrágeis de ocultação de dados. Neste processo, informações sobre o dado hospedeiro são embutidas no próprio dado hospedeiro de forma que possa ser posteriormente comprovada a autenticidade do dado, bem como adulterações realizadas no mesmo. O processo de assinaturas digitais se inclui nesta categoria de aplicação, ou seja, num contexto de verificação de integridade de conteúdo multimídia, pode-se embutir a assinatura diretamente no conteúdo utilizando-se a técnica de marca d'água.

O sistema de proteção contra cópias não autorizadas utiliza bits de sinalização ou outro tipo de informação embutida que são transmitidos juntamente com os dados enviados, e que podem ser interpretados pelo dispositivo digital gravador indicando se é possível realizar cópias do conteúdo recebido.

A proteção contra cópia pode ser efetuada tanto na conversão do sinal analógico para digital como no processo inverso. Sistemas de proteção de conteúdo analógico tipicamente modificam o sinal de vídeo a ser gravado ou transmitido, de forma que realizar cópias em dispositivos de vídeo-cassete comuns se torna bastante difícil ou impossível.

O sistema de proteção contra cópias de conteúdo digital é utilizado de forma a não permitir cópias não autorizadas do conteúdo emitido, ou seja, um sinal é enviado juntamente com o conteúdo e é detectado no sistema receptor indicando se não é autorizada a cópia do conteúdo, se é autorizada apenas uma cópia ou se são autorizadas múltiplas cópias.

No contexto da TV Digital, o STB inclui um codificador/decodificador digital de cores que contem circuito de proteção contra cópia do sinal protegido [5]. Caso o usuário

não tenha autorização de acesso para um determinado programa que se encontra protegido, as cores são modificadas de forma que o sinal enviado para a tela seja indistinguível, caso contrário, o “embaralhamento” das cores é revertido. Neste caso, quando o usuário grava o programa protegido utilizando dispositivo de vídeo-cassete sem a devida permissão de gravação, a cópia não autorizada é degradada utilizando as técnicas de proteção contra cópia de conteúdo analógico resultando em um sinal indistinguível.

Quando o sinal digital com proteção contra cópia é recebido, vídeo, áudio e informações de proteção de cópia são separados. O áudio e vídeo são passados para os decodificadores MPEG-2 e as informações de cópia para o componente CA do STB. Assim como nos sistemas de chave pública de cifração, o DRM se baseia em chaves secretas onde a chave, propriamente dita, é armazenada na memória *flash* do STB. Como a leitura da memória *flash* a cada vez em que estas chaves fossem requisitadas faria com que o processamento se tornasse muito lento, as chaves são copiadas para a memória RAM do STB no momento da inicialização do mesmo, fazendo com que o sistema CA se reporte a estas cópias toda vez que um sinal é decodificado.

Por fim, com relação à proteção do conteúdo contra acessos não autorizados, o conteúdo transmitido deverá ser cifrado ou parcialmente cifrado e posteriormente decifrado por mecanismos já citados anteriormente no dispositivo cliente. Para isto, pode-se utilizar o processo de acesso condicional que combina técnicas de “embaralhamento” e cifração de dados. O Sistema de Acesso Condicional será abordado em mais detalhes no item 6.3.

6.2.1 - Arquitetura de transações DRM

Em linhas gerais, a arquitetura de uma transação DRM [3] pode ser descrita como na Figura 6.1. A transação DRM, em seu nível mais elementar, tem início com a geração do conteúdo (1) que resulta na mídia propriamente dita (2) em forma de áudio, vídeo, texto ou outro formato. Uma vez convertida em sinal digital, o arquivo de mídia é cifrado ou sofre outro processamento a fim de protegê-lo contra uso não autorizado e armazenado em um servidor de conteúdo. O acesso a este arquivo é gerenciado pelo servidor de licenças possivelmente em conjunto com um controlador financeiro cujo objetivo é gerenciar pagamentos por acesso do conteúdo (3). A partir daí, a mídia decifrada ou revertida, conforme o processo sofrido no item (1), deve ser enviada diretamente para o navegador

cliente (4) ou pode ainda ser decodificada pelo aplicativo apropriado DRM que habilitará então seu acesso (5) e então o arquivo licenciado de mídia digital chega ao consumidor (6).

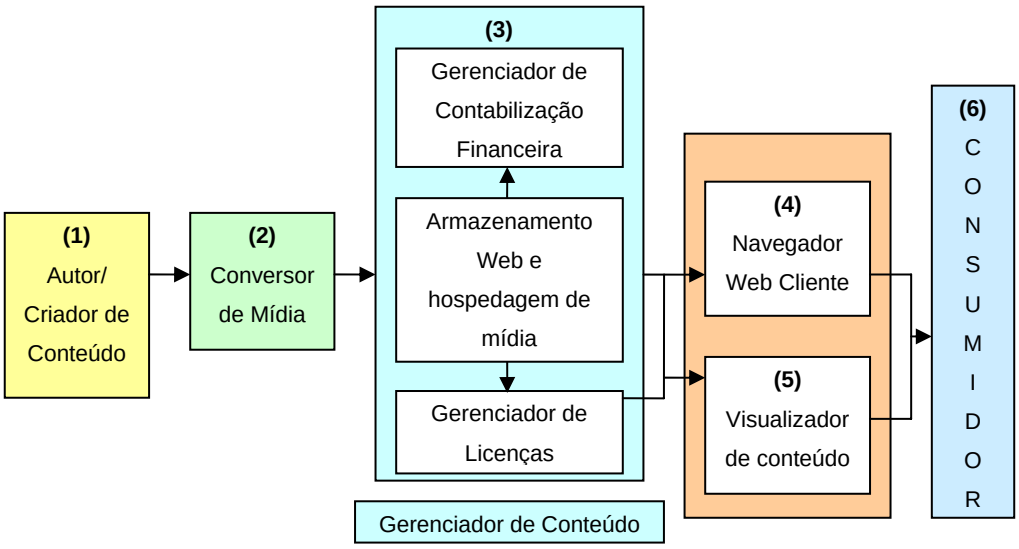


Figura 6.1 - Arquitetura simplificada de uma transação DRM [3]

Alguns aspectos essenciais de um sistema DRM efetivo geralmente incluem:

- Proteção de dados, de forma que os arquivos não sejam acessados sem obtenção dos privilégios apropriados (Proteção de Conteúdo);
- Identificação única de cada usuário de forma a assegurar que os direitos de acesso sejam aplicados apropriadamente (*Fingerprinting*);
- Gerenciamento centralizado de direitos permitindo distribuição gratuita, mecanismos contra fraudes e revogação de direitos (Autenticação de Conteúdo e ação legal);
- Flexibilidade permitindo que o sistema seja personalizado atendendo às características individuais de modelos de negócio, como por exemplo, aluguel, propriedade ou permissão de acesso *read-only* do conteúdo (Controle de Cópia).

As informações que definem o modelo de sistemas DRM correspondem às especificações dos tipos dos direitos que o sistema pode rastrear e medidas que o sistema pode adotar baseado nos atributos que definem, por exemplo, quantas vezes o conteúdo pode ser utilizado, por quanto tempo o usuário pode ter acesso ao conteúdo, quantas vezes o usuário pode efetuar cópias do conteúdo, dentre outros, ou seja, no contexto do DRM, segurança é uma medida da dificuldade em burlar o processo anti-cópia [5].

O modelo de sistemas DRM serve, então, para definir direitos ao conteúdo e garantir a efetivação de tais direitos. Existem três formas de garantir os direitos ao conteúdo:

- Legalmente através de formulários de registro, acordos de licenças e leis de *copyright***.**
- Legalmente através da análise de identificadores permanentemente embutidos no conteúdo como, por exemplo, marcas d'água**.**
- Tecnologicamente através do uso de cifração e autenticação de usuário a fim de proteger o conteúdo e torná-lo acessível somente sob condições específicas e restritas**.**

Existem vários modelos para arquiteturas de sistemas DRM disponíveis. Um dos mais empregados é o modelo de referência proposto por Rosenblatt, Trippe e Mooney [24] o qual pode ser visualizado na Figura 6.2. O fluxo do processo para este modelo pode ser descrito da seguinte forma:

1. O usuário obtém o conteúdo.
2. O usuário tenta acessar/utilizar o conteúdo o que dispara o controlador DRM. Uma vez ativado, o controlador DRM obtém a informação necessária para gerar uma licença de uso. Este processo inclui a obtenção das informações do usuário e do dispositivo cliente, bem como informações do pacote de conteúdo, incluindo o identificador de conteúdo.
3. O cliente DRM envia uma requisição de direitos de acesso/utilização.
4. O servidor de licenças verifica se a identificação do cliente consta no banco de dados de atributos de identidade.
5. O servidor de licenças busca as especificações de direitos de acesso para o conteúdo.
6. Uma transação financeira é efetivada, caso ainda não tenha sido realizada nenhuma referente a este processo e caso as regras de acesso assim determinem.
7. O gerador de licenças compila as informações de direitos de acesso, identidade do cliente e chaves de cifração e então gera uma licença, que por sua vez é cifrada ou sofre processo que evite adulteração.
8. A licença é enviada de volta ao cliente.
9. Após a geração da licença e do processo de autenticação, o controlador DRM pode decifrar o conteúdo e liberar o acesso por parte da aplicativo de exibição.

10. O conteúdo é exibido no dispositivo de saída.

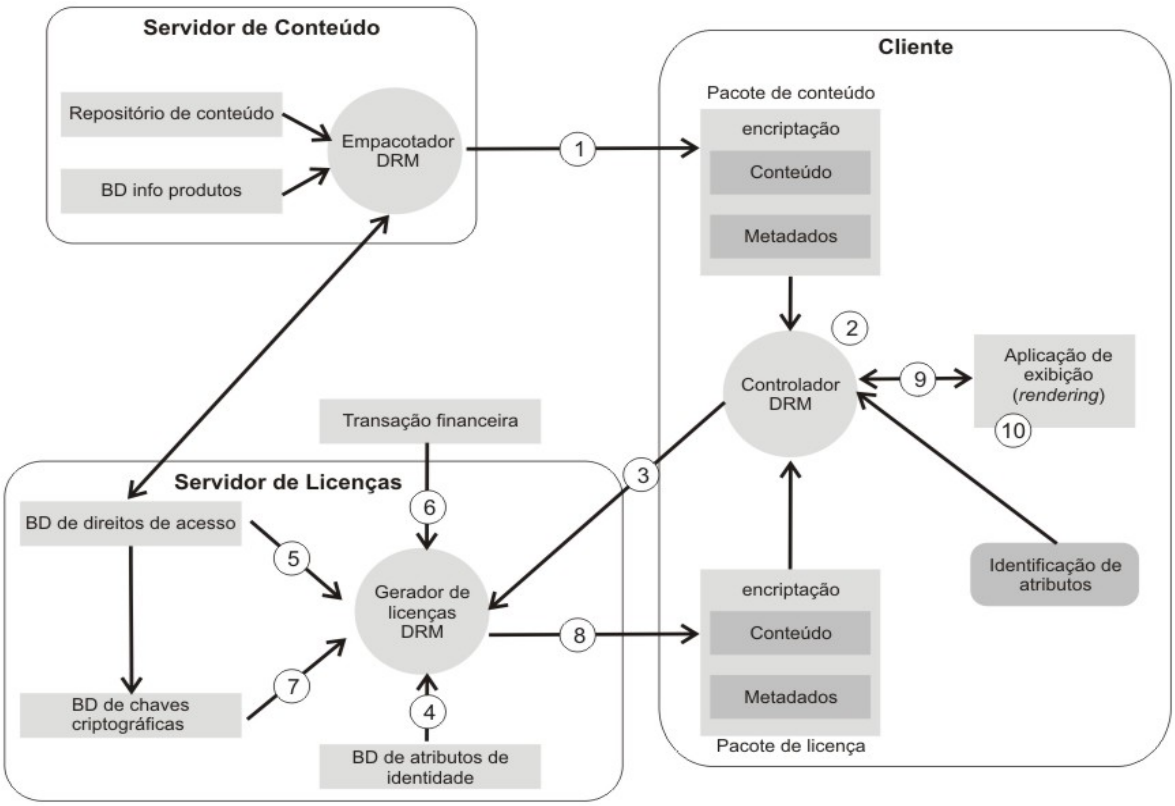


Figura 6.2 - Modelo de referência para plataformas DRM [24]

Desta forma, levando-se em conta esta arquitetura para tratamento de DRM acima, a cadeia de produção de conteúdo para TV Digital pode ser vista conforme a Figura 6.3 complementando a cadeia de valor da TV Digital Interativa apresentada na Figura 5.2. O tratamento de DRM pode ser realizado no processo de empacotamento do conteúdo digital no servidor de conteúdo, no processo de distribuição e entrega de conteúdo através de um gerador de licenças DRM e no próprio dispositivo de recepção através de um controlador DRM.

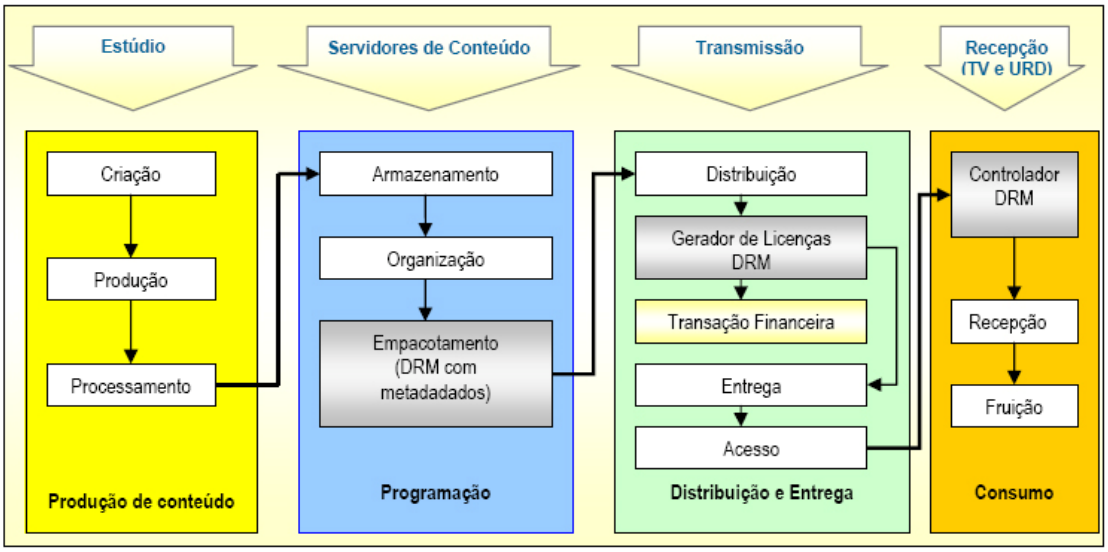


Figura 6.3 – DRM na cadeia de produção de conteúdo

A Tabela 6.1 exibe um resumo dos atuais sistemas de DRM em relação ao processo de transmissão, autenticação, licença e renovação de licença.

Tabela 6.1 - Sistemas atuais de DRM para distribuição e armazenamento [21]

	Mídia protegida	**Forma segura de transmissão**	**Dispositivo de autenticação**	**Associação de Direitos Autorais**	**Tecnologia Licenciada**	**Sistema de renovação**
Mídia Pré-Gravada	Vídeo em DVD-ROM	criptografia	Mútua entre drive DVD e PC	metadados	CSS	Revogação de dispositivo
	Áudio em DVD-Rom	criptografia	Mútua entre drive DVD e PC	metadados	CPPM	Revogação de dispositivo
		Marca d'água	n/a	Marca d'água	4C/Verance Watermark	n/a
	Vídeo ou áudio em DVD-R/RW/RAM	criptografia	Mútua entre drive DVD e PC	metadados	CPRM	Revogação de dispositivo
	Vídeo em fita digital	criptografia	n/a	metadados	Definição de proteção contra cópia	Revogação de dispositivo

	Mídia protegida	Forma segura de transmissão	Dispositivo de autenticação	Associação de Direitos Autorais	Tecnologia Licenciada	Sistema de renovação
Interface Digital	IEEE 1394	criptografia	Mútua entre origem e destino	metadados	DTCP	Revogação de dispositivo
	Interface Visual Digital (DVI)	criptografia	Mútua entre origem e destino	metadados	HDCP	Revogação de dispositivo
	Interface NRSS	criptografia	Mútua entre servidor e dispositivo de segurança removível	metadados	Padrões abertos	Revogação de Serviço
Broadcast	Satélite	criptografia	nenhum	metadados	Sistema de acesso condicional	Revogação de *smartcard*
	Terrestre	criptografia	nenhum	metadados	Sistema de acesso condicional	Revogação de *smartcard*
Transmissão a Cabo		criptografia	nenhum	metadados	Sistema de acesso condicional	Revogação de *smartcard*
Internet	*Unicast*	criptografia	Receptor	metadados	DRM	Atualização de *Software*
	Multicast	criptografia	Emissor e Receptor (dependendo do tipo de autenticação)	metadados	Gerenciamento de chave de grupo	TDB

6.3 - O SISTEMA DE ACESSO CONDICIONAL

O foco do Sistema de Acesso Condicional (CAS) é o “embaralhamento” (*scrambling*) do conteúdo enviado a fim de controlar quem tem acesso ao mesmo. Este embaralhamento faz com que som, imagem e dados se tornem inteligíveis. Desta forma, o CA permite acesso a determinados serviços na TVDI baseado no pagamento referente a este acesso ou em outras requisições como identificação, autorização, autenticação, registro ou mesmo a partir de uma combinação destes requisitos. As geradoras de serviço oferecem diferentes

tipos de conteúdo multimídia que vão desde o acesso gratuito a programas ou serviços do tipo *PayTV, Pay-Per-View* e Vídeo sob Demanda (VoD).

Os sistemas CA são desenvolvidos por empresas denominadas “Empresas Provedoras CA”, cujo enfoque vai desde a proteção de sinais de áudio e vídeo até o desenvolvimento do ambiente seguro para efetuar o devido processamento do sinal propriamente dito. Os sistemas CA mais comuns atualmente são o NDS e o Nagravision, porém outros sistemas estão disponíveis como o Conax, Irdeto Access, Philips (sistema CryptoWorks), France telecom (sistema Viaccess) e sistema Motorola.

Os algoritmos utilizados para este fim são de propriedade da Empresa Provedora CA, porém existem alguns algoritmos abertos, mas não publicamente conhecidos, como por exemplo, o *DVB Common Scrambling Algorithm*, que apesar de ser classificado como algoritmo aberto, exige dos fabricantes de *Set Top Box* que fazem uso deste sistema a assinatura de um acordo de não publicação do algoritmo em si.

A arquitetura típica de um CAS e seus macro-componentes pode ser vista na Figura 6.4.

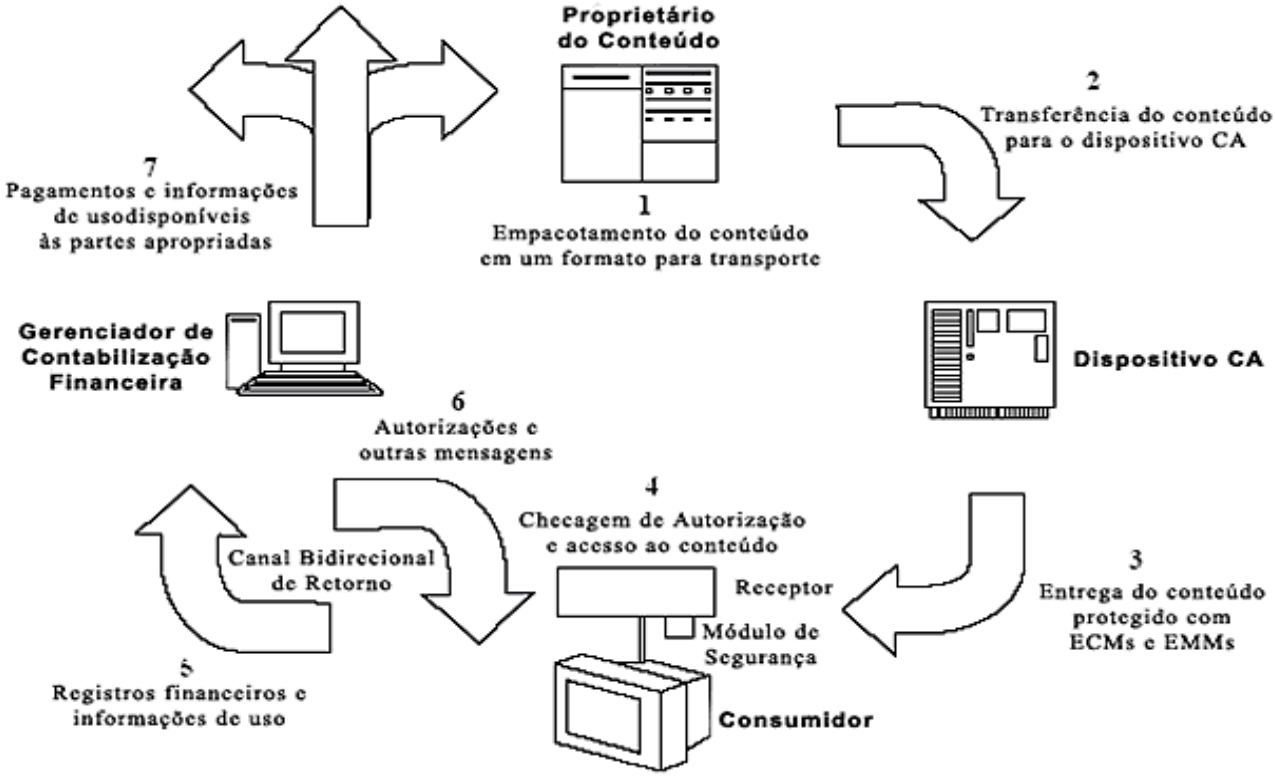


Figura 6.4 - Arquitetura do Sistema CA [3]

As atividades comuns representadas neste modelo genérico são:

1. O conteúdo digital (evento/programa) é comprimido a fim de minimizar a largura de banda necessária. O padrão de codificação MPEG2 para fluxos A/V é um dos mais utilizados, porém atualmente existem outras variações disponíveis como MPEG4, MPEG7 e MPEG21 os quais estão sendo estudados para outros tipos de aplicações.

2. O programa é enviado para o dispositivo CA a fim de que seja protegido e empacotado com inserção de mensagens que indicam as condições de acesso.

3. O fluxo A/V é cifrado e multiplexado juntamente com as mensagens adicionadas pelo sistema CA conhecidas como CAM (*CA messages*) que consistem nas mensagens de controle (ECM – *Entitlement Control Messages*) que detêm a chave de decriptografia (*control word*) além de uma breve descrição do programa (número, título, data, hora, preço, etc), e as mensagens de gerenciamento (EMM – *Entitlement Management Messages*) que especificam os níveis de autorização associados aos serviços. Juntas, as ECMs e EMMs podem controlar a capacidade de acesso de usuários individuais ou grupos de usuários.

Os identificadores de pacote (PIDs) dos pacotes utilizados para enviar as seções ECM e EMM são incluídos na PMT e CAT respectivamente. Além disso, conteúdos específicos podem ser determinados de acordo com o modelo de negócio, sistema de cobrança, dentre outros, permitindo assim a implementação de diferenciados tipos de sistema de acesso condicional.

O processo de cifração/decifração se baseia em três níveis de informação: a *control word (Kw)*, a *service key (Ks)* e *user key (Km)* [3]. A *control word* é cifrada utilizando a *service key*, providenciando o primeiro nível de cifração. Esta *service key* pode ser comum a um grupo de usuários e tipicamente cada serviço cifrado terá uma *service key*. A *control word* é enviada via *broadcast* em uma ECM aproximadamente a cada dois segundos, o que por sua vez é suficiente para o processo de decifração por parte do decodificador (Figura 6.5).

O próximo nível garante o acesso ao serviço somente por parte dos usuários autorizados, ou seja, somente os usuários que pagaram pelo serviço conseguem decifrar *control word*. Para que isto seja possível, a *service key* é cifrada fazendo uso da *user key*. Cada *user key* é única pertencente a um único usuário, desta forma a *service key* deve ser

cifrada com a *user key* para cada usuário que tem acesso autorizado para visualizar o conteúdo. Uma vez cifrada a *service key*, é enviada via *broadcast* como parte de uma EMM. Como há uma grande quantidade de informação a ser difundida, incluindo a própria *service key* que deve ser enviada para cada usuário, estas são enviadas com menos freqüência, ou seja, cada EMM é enviada aproximadamente a cada dez segundos [26].

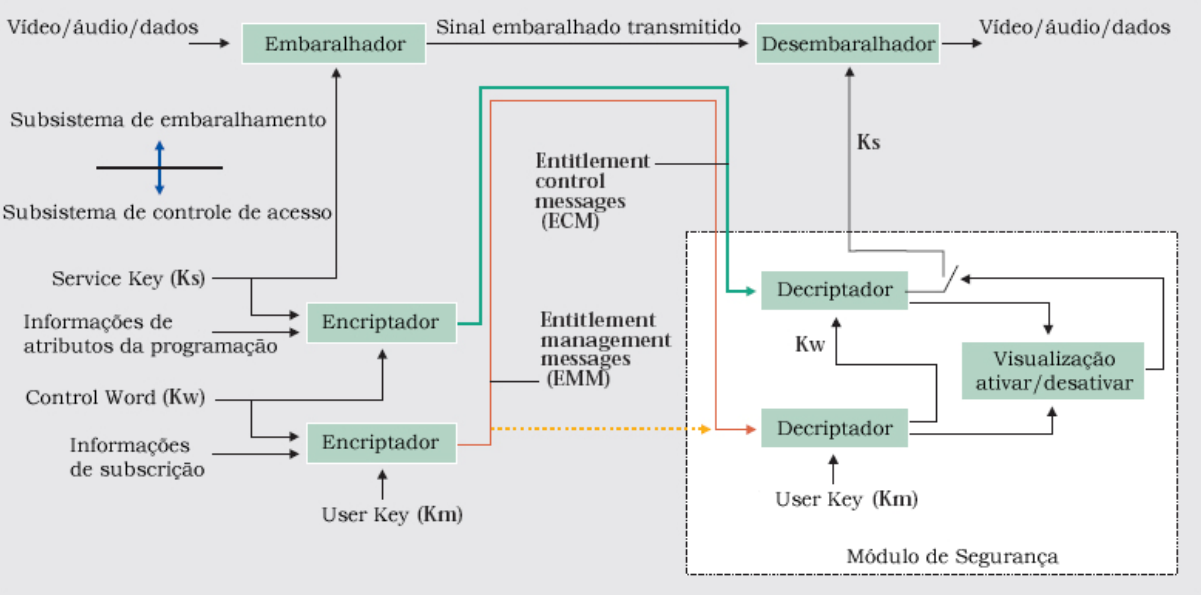


Figura 6.5 - Configuração de um sistema de acesso condicional [26]

Quando o receptor recebe uma CAM, é imediatamente passada para o sistema de CA. No caso de uma EMM, o receptor verifica se a EMM é de fato destinada àquele receptor e caso positivo, ele utilizará uma cópia da *user key* para decifrar a *service key*. A *service key*, por sua vez, será utilizada para decifrar quaisquer ECMs que são recebidas para o serviço em questão e recuperar a *control word*. Uma vez que o receptor possui a *control word* correta, ele pode utilizá-la para inicializar a decifração do conteúdo.

Os serviços são geralmente cifrados utilizando um sistema de cifra simétrica como, por exemplo, o *Data Encryption Standard* (DES) ou outro algoritmo, mas também podem ser utilizados algoritmos de cifração não simétricos o que torna o processo mais complexo. Por razões de segurança, as especificidades das ECMs é geralmente definida de forma privada pelas Empresas provedoras CA, o que não invalida a utilização de cifra baseada em chave pública (PKI) e funções *one-way*, as quais são ferramentas de grande valia para o processo seguro de envio de chaves.

4. Caso o usuário tenha autorização para acessar o programa protegido, o fluxo de áudio e vídeo é decifrado pelo receptor ou decodificador, e enviado à unidade de exibição. Adicionalmente pode ser utilizado um módulo de segurança removível, como por exemplo, um *smartcard* que provê um ambiente seguro para o processamento de ECMs, EMMs e outras funções pertinentes como autorização e armazenamento temporário de registros adquiridos.

5. A Entidade Controladora é componente essencial em cada sistema CA pois corresponde à instituição financeira por trás de todo o processo de cobrança/ pagamento, transmissão de EMMs e aplicações interativas de TV. Um *link* tipo *one-to-one* é estabelecido entre a entidade controladora e o decodificador (ou o módulo removível de segurança, se for o caso) com a presença de um canal de retorno, o qual pode ser basicamente uma conexão via modem através de linha telefônica. Da mesma forma que outros detalhes do sistema CA, a segurança neste canal de retorno deve ser definida de forma privada pela empresa provedora CA. De tempos em tempos, a entidade controladora coleta as informações do histórico de utilização de serviço e outras informações pertinentes para realizar o processamento e cobrança.

6. Autorizações, por exemplo, EMMs e outras mensagens (atualizações de sistema e segurança, etc) são enviadas para o receptor do usuário.

7. Por último, as informações de utilização, cobranças e pagamentos são enviados às partes apropriadas (provedores de conteúdo, operadoras de serviço, empresas provedoras CA, etc).

Nos sistemas CA o módulo de segurança está associado à complexa tarefa de recuperação das chaves de decifração. Estas chaves são então passadas ao receptor a fim de decodificar os fluxos de áudio e vídeo e a tarefa de decifração é efetuada tanto pelo módulo de segurança como também pelo dispositivo onde este módulo se encontra instalado.

Atualmente existem padrões que se empenham em retirar toda funcionalidade referente à segurança dos dispositivos de navegação. Nos Estados Unidos, o NRSS (*National Renewable Security Standard*) [27] define um elemento para segurança de perfil renovável e substituível para uso em dispositivos eletrônicos como STBs e TVs Digitais. Na Europa, o projeto DVB [9] especificou um padrão para uma interface comum (CI – *Common Interface*) localizada entre o dispositivo hospedeiro e o módulo de segurança.

Os sistemas CA atualmente em operação suportam diversas formas de aquisição/cobrança de serviços dentre os quais a assinatura regular e o modo *pay-per-view*. No entanto, outros modelos vêm sendo considerados a fim de prover outras facilidades de pagamento e conveniências. Um destes modelos usa “cartões pré-pagos” que permitem o armazenamento de créditos os quais podem ser obtidos a partir de revendedores autorizados ou até mesmo máquinas eletrônicas específicas para este fim. Outra alternativa para habilitar acesso ao conteúdo é o aluguel de equipamento apropriado da provedora de conteúdo o qual contém o *hardware* e *software* específicos para realizar a decifração do conteúdo [11].

O projeto DVB apresenta dois padrões de acesso chamados *Simulcrypt* e *Multicrypt*. No padrão *Simulcrypt* cada programa é transmitido com as mesmas mensagens de cabeçalho para acesso de sistemas CA múltiplos, habilitando assim decodificadores CA de tipos diferentes a fim de que possam receber e decifrar corretamente o programa. Já no padrão *Multicrypt*, cada decodificador é construído com uma interface comum para sistemas CA múltiplos. Os módulos de segurança das diversas provedoras de sistemas CA podem ser conectados em *slots* diferentes no mesmo decodificador permitindo assim a troca dentre os sistemas CA disponíveis. Estas arquiteturas podem ser adotadas para transmissão de TV digital a cabo, satélite e terrestre. O padrão ATSC [10] tem adotado o modo de acesso *Simulcrypt*.

6.4 - COMPARAÇÃO ENTRE SISTEMAS DRM E CA

Os termos Gerenciamento de Direitos Digitais (DRM) e Acesso Condicional (CA) têm sido usados de forma muitas vezes errônea como se ambos fossem sinônimos ou mesmo um fizesse parte do outro.

O Sistema de Acesso Condicional é a técnica que tem sido tradicionalmente utilizada para proteger os canais de TV através do controle de acesso ao conteúdo restrito, utilizando para isto a cifração do conteúdo. Apesar de prevenir o acesso indevido de conteúdo protegido, o CAS não define o que ocorre com o conteúdo uma vez entregue ao usuário. O CAS utiliza uma combinação de técnicas de cifração e embaralhamento e, como visto anteriormente, transmite juntamente com o sinal cifrado, as chaves de decifração através de mensagens também cifradas (ECM).

A principal diferença entre o CAS e o DRM é que o DRM é geralmente aplicado à proteção de um conteúdo específico definindo condições de uso do mesmo. Tipicamente, o DRM controla as ações possíveis de serem realizadas sob o conteúdo protegido, como por exemplo, definição de quando o conteúdo está disponível, em quais dispositivos o conteúdo pode ser acessado ou se pode ser transmitido de um dispositivo a outro, quantas vezes o conteúdo pode ser visualizado, por qual período o acesso ao conteúdo está disponível, etc.

De fato o sistema DRM utiliza a cifração do conteúdo, porém mesmo decifrado, as condições de acesso definidas permanecem vinculadas ao mesmo.

A tendência é que DRM e CA caminhem juntos e pode ser atualmente observado que o termo DRM vem sendo empregado como um conjunto de técnicas mais abrangentes referentes à proteção de conteúdo, o que inclui o acesso condicional, proteção do conteúdo e proteção de direitos sob o conteúdo.

6.5 - OS DESCRITORES DAS TABELAS SI RELACIONADOS AO TRATAMENTO DE DRM E CA

Como já visto antes, a constituição das tabelas SI é feita através de descritores padronizados, com uma sintaxe própria e que podem inclusive constar em mais de uma tabela SI. Neste caso, conforme as normas ARIB [7] e a ABNT/CEE-00:001.85 [28], existe precedência dos valores definidos para os descritores da tabela PMT em relação às tabelas EIT e STD, ou seja, a prioridade de informação é PMT>EI>STD.

Tais descritores também são utilizados como mecanismo de proteção contra cópias não autorizadas de conteúdo, tratamento de direitos autorais e especificação de acesso condicional. Os principais descritores referentes a estes processos estão especificados nas Tabelas 6.2 e 6.3 e nas Figuras 6.6, 6.7, 6.8, 6.9 e 6.10.

Tabela 6.2 - Nomes e funções dos principais descritores das tabelas SI relacionados ao processo de gerência de direitos autorais e acesso condicional [7]

Nome do Descritor	Função
Conditional Access Descriptor	Descreve o PID do portador das informações sobre método utilizado pelo acesso condicional bem como pelo ECM e EMM.
Copyright Descriptor	Identifica o *copyright*.
CA Indentifier Descriptor	Descreve o método de acesso condicional disponível.
Digital Copy Control Descriptor	Descreve a informação que controla a geração de cópias em equipamentos de gravação digital além da taxa máxima de transmissão.
Content Availability Descriptor	Descreve a informação que controla a gravação e saída de programas.

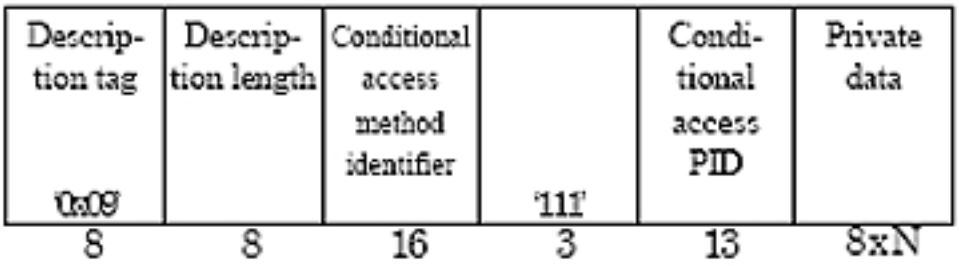


Figura 6.6 - Estrutura de dados do *Conditional Access method descriptor* [7]

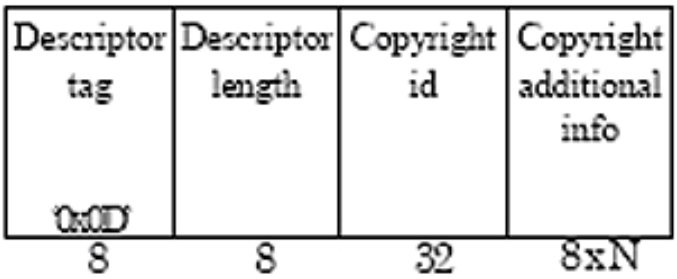


Figura 6.7 - Estrutura de dados do *Copyright descriptor* [7]

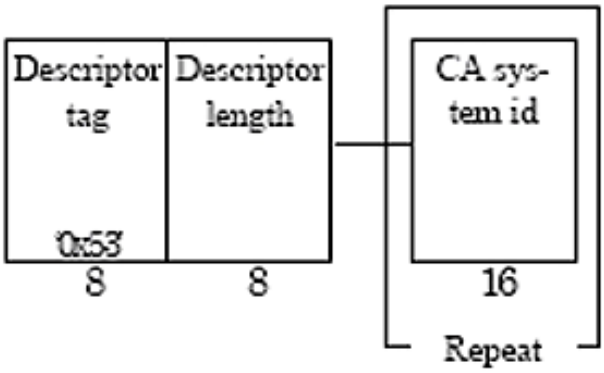


Figura 6.8 - Estrutura de dados do *CA identifier descriptor* [7]

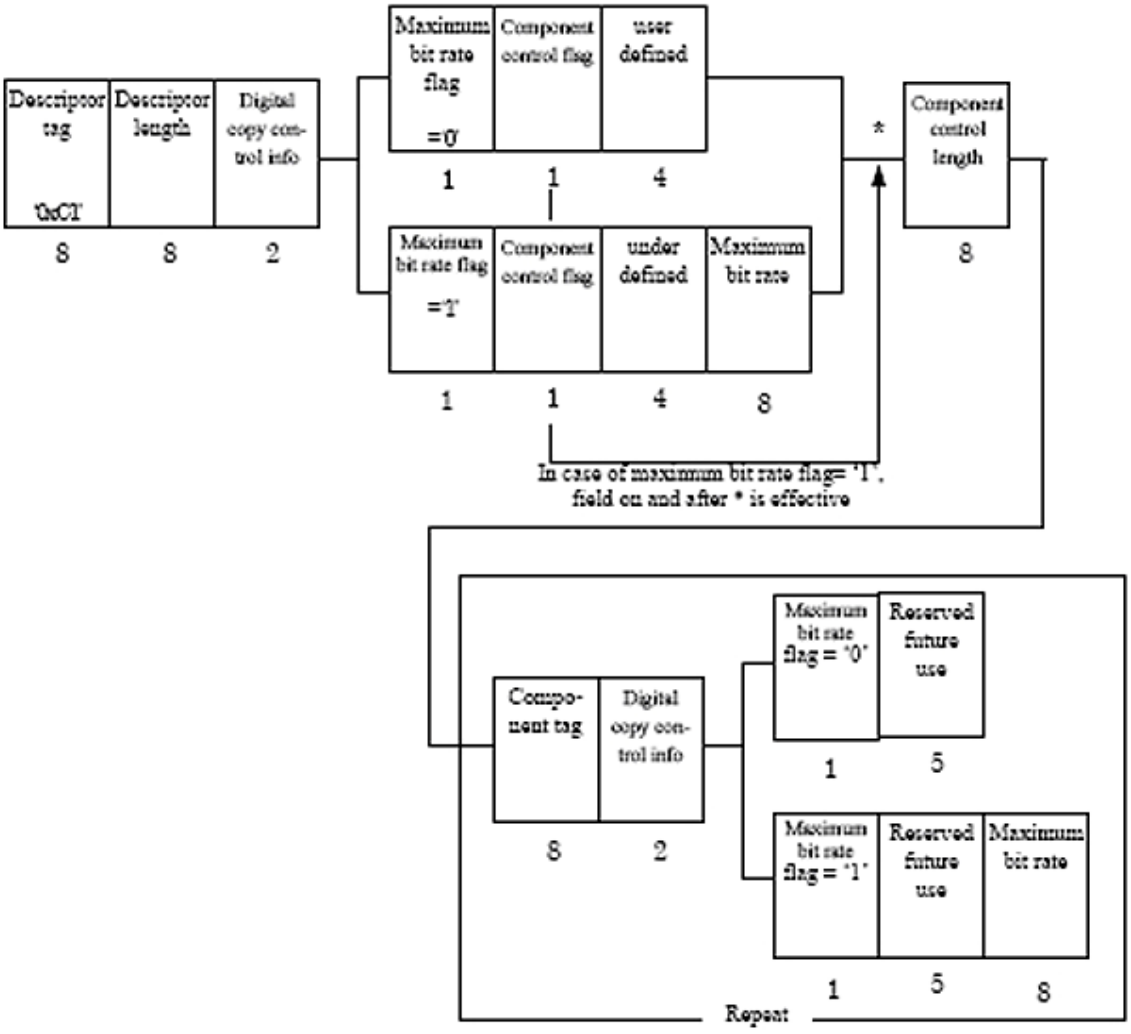


Figura 6.9 - Estrutura de dados do *Digital copy control descriptor* [7]

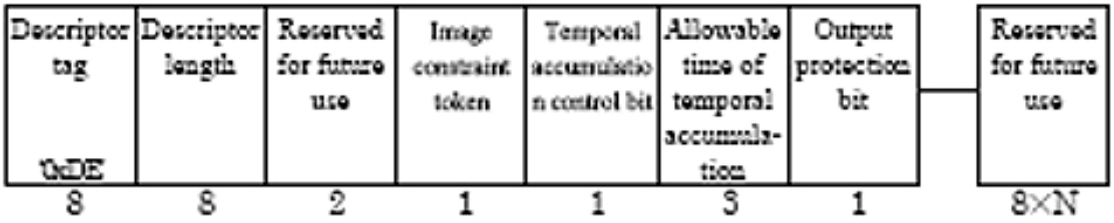


Figura 6.10 - Estrutura de dados do *Content availability descriptor* [7]

Tabela 6.3 - Nomes e funções dos principais descritores utilizados no sistema de transmissão digital (excluindo *Service Information*) [7]

Nome do Descritor	Função
CA EMM TS Descriptor (Descritor especificado na ARIB STD-B25)	Indica o canal específico quando a transmissão EMM é realizada por método de canal específico.
CA Contract Information Descriptor (Descritor especificado na ARIB STD-B25)	Descreve o tipo do serviço do acesso condicional do programa especificado e permissão de recepção e gravação.
CA Service Descriptor (Descritor especificado na ARIB STD-B25)	Descreve o provedor de serviço transmitido para apresentação de indicação de mensagem automática.

A Tabela 6.4 traz os descritores listados na Tabela 6.2 acima e suas possíveis localizações dentro das tabelas SI. Isto, porém, não restringe o uso dos mesmos em outras tabelas.

Tabela 6.4 - Localização e requisições dos descritores SI [7]

Descritor	Nível de Transmisssão	CAT	PMT	BAT	SDT	EIT
conditional_acess_descriptor	Obrigatório para acesso condicional	O	O			
copyright_descriptor	A ser definido		O			
CA_identifier_descriptor	Opcional			O	O	O
digital_copy_control_descriptor	Opcional		O		O	O
content availability descriptor	Opcional		O		O	O

O controle de cópia de conteúdo deve ser baseado no descritor de controle de cópia digital (*digital copy control descriptor*) e no descritor de disponibilidade de conteúdo (*content availability descriptor*) [28].

Através do descritor de disponibilidade de conteúdo é possível especificar a situação atual da criptografia dos sinais de saída. Um exemplo de descritor de disponibilidade de conteúdo pode ser observado na Figura 6.11.

Já o descritor de controle de cópia digital contém a informação que define o controle da geração de cópias em equipamentos de gravação digital. No caso de gravação digital permitida, o provedor de serviço que detém os direitos autorais do conteúdo transmitido usa este descritor para informar sobre o evento de gravação, as informações de direitos autorais para o equipamento de cópia digital em interfaces digitais de alta velocidade compatíveis com *Digital Transmission Content Protection* (DTCP) e a especificação da máxima taxa de bits usada para verificar a disponibilidade da gravação além de selecionar um modo de gravação. Um exemplo de descritor de controle de cópia digital pode ser observado na Figura 6.12.

A especificação do DTCP define um protocolo criptográfico para proteção de conteúdo de entretenimento de áudio e vídeo contra cópia não autorizada, interceptação e alteração do conteúdo nos meios de transmissão digitais [29]. Somente conteúdo multimídia enviado para um dispositivo a partir de outro dispositivo com sistema com proteção de cópia (como por exemplo, o CSS – *Content Scrambling System*, utilizado nos dispositivos de DVD) poderá ser protegido por este sistema de proteção contra cópias.

O uso desta especificação juntamente com o acesso à propriedade intelectual e métodos de cifração a serem implementados são escopo de uma licença gerenciada pelo *Digital Transmission Licensing Administrator* (*DTLA*), o responsável pelo estabelecimento e administração do sistema de proteção de conteúdo do DTCP.

Syntax	No. of bits	Identifier
content_availability_descriptor(){		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
reserved_future_use	2	bslbf
image_constraint_token	1	bslbf
retention_mode	1	bslbf
retention_state	3	bslbf
encryption_mode	1	bslbf
for(i=0;i<N;i++){		
reserved_future_use	8	uimsbf
}		
}		

Figura 6.11 - *Content availability descriptor* [7]

Segundo a definição semântica encontrada na norma ARIB STD-B10:2006 [7], o *encryption_mode* do descritor de disponibilidade de conteúdo é um campo de tamanho 1 bit que indica quando a saída de alta velocidade da interface digital está protegida. Quando o valor deste campo está definido como “1” significa que nenhuma proteção é requerida para o conteúdo.

Syntax	No. of bits	Identifier
digital_copy_control_descripton(){		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
digital_recording_control_data	2	bslbf
maximum_bitrate_flag	1	bslbf
component_control_flag	1	bslbf
copy_control_type	2	bslbf
if(copy_control_type == 01){		
APS_control_data	2	bslbf
}		
else{		
reserved_future_use	2	bslbf
}		
if(maximum_bitrate_flag == 1){		
maximum_bitrate	8	uimsbf
}		
if(component_control_flag == 1){		
component_control_length	8	uimsbf
for(j=0;j<N;j++){		
component_tag	8	uimsbf
digital_recording_control_data	2	bslbf
maximum_bitrate_flag	1	bslbf
reserved_future_use	1	bslbf
copy_control_type	2	bslbf
if(copy_control_type == 01){		
APS_control_data	2	bslbf
}		
else{		
reserved_future_use	2	bslbf
}		
if(maximum_bitrate_flag == 1){		
maximum_bitrate	8	uimsbf
}		
}		
}		
}		

Figura 6.12 - *Digital copy control descriptor* [7]

Ainda segundo a norma ARIB STD-B10:2006 [7], a semântica para o descritor de controle de cópia digital é definida da seguinte forma:

- *copy_control_type*: campo de tamanho 2 bits que indica o tipo de informação para controlar a geração de cópia conforme os valores exibidos na Tabela 6.5.

Tabela 6.5 - Codificação para *copy_control_type* [7]

Copy control type	**Descrição**
00	Não definido
01	Saída através de codificação especificada pelo provedor de serviço para interface serial
10	Não definido
11	Saída sem codificação para interface serial

- *digital_recording_control_data*: campo de tamanho 2 bits que contém informação para controlar a geração de cópia conforme os valores exibidos na Tabela 6.6.

Tabela 6.6 - Codificação para *digital recording control data* [7]

Digital recording control data	**Descrição**	
	Para copy_control_type =11	***Para copy_control_type =01***
00	Cópia livre	Cópia livre
01	Não utilizado	Cópia proibida
10	Pode ser copiado uma única vez	Pode ser copiado uma única vez
11	Cópia proibida	Cópia proibida

- *APS_control_data*: campo de tamanho 2 bits que contém informação para controlar a cópia analógica quando *copy_control_type* é definido como 01.

Em radiodifusão de televisão digital terrestre, quaisquer saídas de fluxo de transporte, exceto interfaces digitais de alta velocidade compatíveis com DTCP, não são permitidas no momento. Em outras palavras, a proteção de conteúdo sob DTCP é utilizada quando a emissora define "*copy_control_type*" em um descritor de controle de cópia com o valor "01" a fim de proteger o conteúdo. Valores diferentes de "01" para "*copy_control_type*" indicam que não somente a saída de dados digital, mas também a saída de vídeo analógico é proibida.

As Tabelas 6.7 e 6.8, extraídas da norma brasileira ABNT/CEE-00:001.85 [28], trazem um resumo das combinações de codificações possíveis para os descritores de controle de cópia digital.

Tabela 6.7 - Operação de descritores para o serviço de televisão digital e serviço especial de vídeo [28]

<table>
<tr><th rowspan="2">Controle de cópia digital</th><th rowspan="2">Controle de cópia analógico</th><th colspan="3">Operação do descritor de controle de cópia digital</th><th>Operação do descritor de disponibilidade de conteúdo</th></tr>
<tr><th>Copy_ control_type</th><th>Digital_recording_ control_data</th><th>APS_control_data</th><th>Encryption_ mode</th></tr>
<tr><td>Cópia livre</td><td rowspan="2">Cópia livre</td><td rowspan="7">01</td><td rowspan="2">00</td><td rowspan="2">00</td><td>0</td></tr>
<tr><td>Cópia livre</td><td>1</td></tr>
<tr><td rowspan="2">Nunca copiar</td><td>Nunca copiar sem proteção de saída</td><td rowspan="2">11</td><td>00</td><td>1</td></tr>
<tr><td>Nunca copiar com proteção de saída ou resolução reduzida para 480p (350 000 pixels)</td><td>Diferente de 00</td><td>1</td></tr>
<tr><td rowspan="2">Copiar uma geração</td><td>Copiar uma geração sem proteção de saída</td><td rowspan="2">10</td><td>00</td><td>1</td></tr>
<tr><td>Copiar uma geração com proteção de saída ou resolução reduzida para 480p (350 000 pixels)</td><td>Diferente de 00</td><td>1</td></tr>
</table>

Tabela 6.8 - Operação dos descritores para serviço de dados, serviço especial de dados e serviço de dados da lista de indicadores [28]

Controle de cópia digital	**Controle de cópia analógico**	**Operação do descritor de controle de cópia digital**			**Operação do descritor de disponibilidade de conteúdo**
		Copy_control_type	**digital_recording_control_data**	**APS_control_data**	**encryption_ model**
Cópia livre	Cópia livre	01	00	00	0
Cópia livre					1
		11	00	00	1
Nunca copiar	Nunca copiar sem proteção de saída	01	11	00	1
	Nunca copiar com proteção de saída ou resolução reduzida para 480p (350 000 pixels)			Diferente de 00	
Nunca copiar e a saída de MPEG_TS está desativada	Nunca copiar sem proteção de saída	11		00	1
	Nunca copiar com proteção de saída ou resolução reduzida para 480p (350 000 pixels)			Diferente de 00	
Copiar uma geração	Copiar uma geração sem proteção de saída	01	10	00	1
	Copiar uma geração com proteção de saída ou resolução reduzida para 480p (350 000 pixels)			Diferente de 00	
Copiar uma geração mas a saída de MPEG_TS está desativada	Copiar uma geração sem proteção de saída	11		00	1
	Copiar uma geração com proteção de saída ou resolução reduzida para 480p (350 000 pixels)			Diferente de 00	

6.6 - ARQUITETURA E MECANISMOS DE SEGURANÇA NO MHP

O *framework* de segurança do MHP permite a autenticação da fonte do código da aplicação ou outros arquivos. Todas as mensagens de autenticação são armazenadas como arquivos em diretórios específicos e transmitidas para o dispositivo receptor juntamente com a informação via *broadcast*. O sistema usa três mensagens de segurança diferentes armazenadas em arquivos [13]:

- Código *Hash* de cifra – provê um sumário da quantidade de dados.
- Assinatura – provê um código *hash* mestre (utilizado para a computação em todo o dado especificado) que por sua vez detém uma assinatura digital de uma entidade certificadora. O processo da assinatura digital associa o código *hash* mestre ao signatário. Sendo assim, o processamento do código

hash autentica os dados assinados de forma que seja possível detectar qualquer tipo de adulteração sobre os dados originalmente assinados.

- Certificado – provê uma “cadeia de credibilidade” a partir da entidade certificadora até uma TTP (autoridade certificadora principal) a qual é de conhecimento do receptor.

As mensagens são entregues dento de arquivos do conjunto dos arquivos de sistema de forma que o esquema de autenticação seja aplicado a qualquer arquivo de sistema hierárquico dentre os canais da transmissora.

Arquivos de diretórios utilizam aplicação de código *hash* que é computado levando-se em conta o conteúdo e atributos dos objetos ao invés de informações específicas de transporte. Desta forma, a autenticação é independente do protocolo utilizado para transporte de dados.

A assinatura faz referência a um certificado que contém a chave pública a ser utilizada na decodificação da assinatura, além de identificar o algoritmo utilizado para gerar o código *hash* e o valor da assinatura propriamente dito.

O certificado provê a chave pública que pode ser utilizada para decodificar o código *hash* contido na assinatura e então habilitar a seqüência de verificação de certificados. O certificado é assinado por uma entidade certificadora superior.

Como os objetos são organizados hierarquicamente, a autenticação se baseia em estruturas hierárquicas. Os códigos hash são computados sistematicamente e de forma acumulativa em alguns ou todos os objetos na hierarquia. O algoritmo utilizado na computação do código *hash* é o MD5 ou SHA.

A assinatura no topo da hierarquia identifica a origem dos objetos. Este processo permite a autenticação de um arquivo de sistema com uma simples assinatura e somente os objetos carregados na memória é que necessitam checagem do código *hash* em tempo real.

7 – UTILIZAÇÃO DE METADADOS NA TV DIGITAL

Levando-se em conta a possibilidade de interatividade no ambiente da TV Digital, o usuário/expectador passa a ter um papel decisivo de modificação no fluxo de programação linear clássica a partir dos serviços oferecidos. Porém, na medida em que os serviços e tipos de conteúdos multimídia são diversificados, a complexidade que envolve a manipulação de informações para TV aumenta da mesma forma como observada em outros tipos de mídia digital.

É neste contexto que surge o tratamento de informações com metadados. O uso de metadados permite o tratamento de conteúdo digital e serviços no ambiente de TV digital de forma eficiente e otimizada. De forma sucinta, metadados são dados que explicam dados [18]. Esta definição pode ser estendida de forma que a descrição dos dados por metadados deve ser suficiente para que estes possam ser utilizados como dicionários na tomada de decisões referente ao uso dos dados [30]. Outra definição válida é aquela que diz que metadados são uma máquina para entendimento das informações sobre os recursos Web e outros [31].

Desta forma, os metadados podem prover informações de grande valia, tanto no entendimento da sintática como também da semântica de dados complexos através do desmembramento da essência da informação em um conjunto simplificado de descritores. A partir daí, pode-se inferir que através do uso de metadados é possível estruturar, manipular e representar dados sobre recursos, contextos e serviços.

7.1 - TIPOS DE METADADOS

Os metadados podem ser classificados, dentre outros padrões de classificação, em três tipos: descritivos, administrativos e estruturais [32].

Metadados descritivos são aqueles que descrevem o conteúdo de um documento sendo utilizados em identificação, organização e pesquisa.

Metadados administrativos correspondem às informações necessárias que permitem que o dispositivo de repositório gerencie o objeto. Tais informações podem incluir metadados técnicos (formato de armazenamento, forma de escaneamento, etc), informações de direitos autorais e licenciamento, e informações necessárias para preservação do objeto por longo tempo (metadados de preservação).

Metadados estruturais correspondem às informações que criam vínculos lógicos entre os objetos individuais compondo uma unidade funcional a fim de descrever o processo para uso e navegação, como por exemplo, imagens individuais e outros componentes que constituem um livro digital.

Em geral só metadados descritivos são visíveis aos usuários de um sistema onde são utilizados para localização e acesso a itens de uma coleção. Metadados administrativos são normalmente utilizados por aqueles que fazem a manutenção das coleções e metadados estruturais são normalmente utilizados por interfaces de aplicativos que compilam objetos digitais individuais em unidades funcionais para os usuários.

7.2 - FORMATOS DE METADADOS

O padrão *eXtensible Markup Language* (XML), atualmente bastante difundido em aplicações Internet, é um formato simples e aberto e, apesar de ter sido inicialmente desenvolvido para manipulação de texto eletrônico, vem sendo largamente utilizado para muitos tipos de aplicações de metadados.

O XML não corresponde, ao contrário do formato HTML, a um conjunto de *tags*, e sim a um conjunto de regras que permitem a definição de outras *tags*. Um dos seus benefícios é permitir a separação do conteúdo da apresentação.

Dentre as vantagens da utilização do XML como codificação de metadados podem ser citados: robustez, independência do *software* utilizado e a possibilidade de troca e leitura de informações entre sistemas até mesmo de plataformas diversas.

O XML pode ser expresso de duas formas: a primeira que corresponde ao *Document Type Definition* (DTD), a qual lista quais *tags* podem ser utilizadas dentro de um documento XML além de especificar os conteúdos e relacionamentos entre elas.

A segunda forma corresponde ao *XML Schema* o qual define um conjunto de regras que devem ser seguidas, visando à estruturação e organização dos metadados nos documentos, de acordo com a sintaxe no formato XML. Esta última modalidade tem muito mais recursos que a DTD porém, por ser mais recente, fica limitada à *software* que tenha capacidade de manipulá-la.

7.3 - METADADOS E A TV DIGITAL

A cultura da interatividade vem sido assimilada pelos usuários principalmente devido à Internet. A navegação na Web é feita através de metadados e HTML, os quais definem a estrutura e *links* dos conteúdos da Internet.

Atualmente, a transmissão de informações no ambiente da TVD é baseada nas especificações de metadados das tabelas de informações de serviços (SI – *Service Information*). As tabelas SI utilizam as tabelas PSI (*Program Specific Information*) do padrão MPEG-2 que, por sua vez, definem um conjunto de estruturas que descrevem os serviços da TVD. Estas tabelas facilitam a criação, tratamento e acesso otimizado às informações, porém, tabelas SI são consideradas metadados rígidos. Metadados rígidos possuem um propósito específico e não estão sujeitos a uma padronização personalizada de metadados.

Apesar disso, muitos serviços necessitam de informações adicionais além daquelas disponíveis na tabela SI, ou seja, surgiu a necessidade de possibilitar a criação de metadados de estrutura personalizada a fim de atender os novos serviços em cenários cada vez mais complexos. São os chamados metadados flexíveis definidos a partir de outros formatos que não causam sobrecarga na rede, permitindo complementar as informações disponíveis nas tabelas SI.

A utilização de metadados no ambiente da TVD traz grandes possibilidades e pode levar ao que Tom Worthington [33] denominou de *"killer application"*. Segundo ele, o atual sistema de transmissão digital tem um modelo de negócio que tem falhado à medida que ignora o que os usuários mais têm interesse: controle. Desta forma, metadados provêm, de forma transparente, simplificação das aplicações na Internet e podem ser utilizados para transformar a transmissão digital em um serviço viável.

Segundo Lugmayr [18], as principais razões para a viabilização da transmissão digital são:

- A interoperabilidade das plataformas distribuídas ao longo da cadeia de valores da TVDI**;**
- Interfaces abertas e padronizadas para compartilhamento semi-automatizado de multimídia;
- Troca de dados de forma padronizada ao longo da cadeia de valores**;**
- Metadados estruturados de forma rígida garantem alta performance**;**

- Maior granularidade e nível de detalhamento devido à maior complexidade dos metadados utilizados**;**
- Resolução de metadados escalonáveis no tempo e no espaço para representação de conteúdo**;**
- Acesso simplificado às informações de contexto a partir da representação do conteúdo devido aos modelos unificados de metadados**;**
- Existência de modelos de apresentação para uma interatividade facilitada**;**
- Fáceis e rápidas adaptação, transcodificação, transformação e encapsulamento de metadados e conteúdo**;**
- Metadados servem como vínculo virtual entre a criação, transmissão e troca de conteúdo multimídia através do espaço de serviço virtual**.**

7.3.1 - Ciclo de vida dos metadados na TV Digital

Conforme pode ser observado na Figura 7.1, existem padrões específicos de metadados relacionados às diversas etapas na geração/consumo de conteúdo para TV Digital, envolvendo desde os produtores de conteúdo, provedores de serviços e usuários finais.

A fase de Pré-produção tem o foco direcionado para o planejamento, conceituação e refinamento contínuo das idéias projetadas. Os resultados obtidos nesta fase estão mais relacionados a conceitos, tomada de decisão e definição dos requisitos do serviço a ser elaborado, além da própria captura do conteúdo multimídia.

Durante a fase de Produção, as partes de conteúdo multimídia, em qualquer forma, são concretizadas e finalizadas a partir da combinação dos diferentes conteúdos. Pode ser, por exemplo, uma filmagem, implementação de serviços, dentre outros.

A fase Pós-produção compila a programação combinando-a em apenas um produto final para distribuição (entrega), e inclui as etapas relacionadas ao armazenamento (*Ingest*) e compressão.

A fase de Entrega se encarrega da agregação do conteúdo multimídia editado juntamente aos serviços acoplados e a entrega propriamente dita através da transmissão *broadcast*.

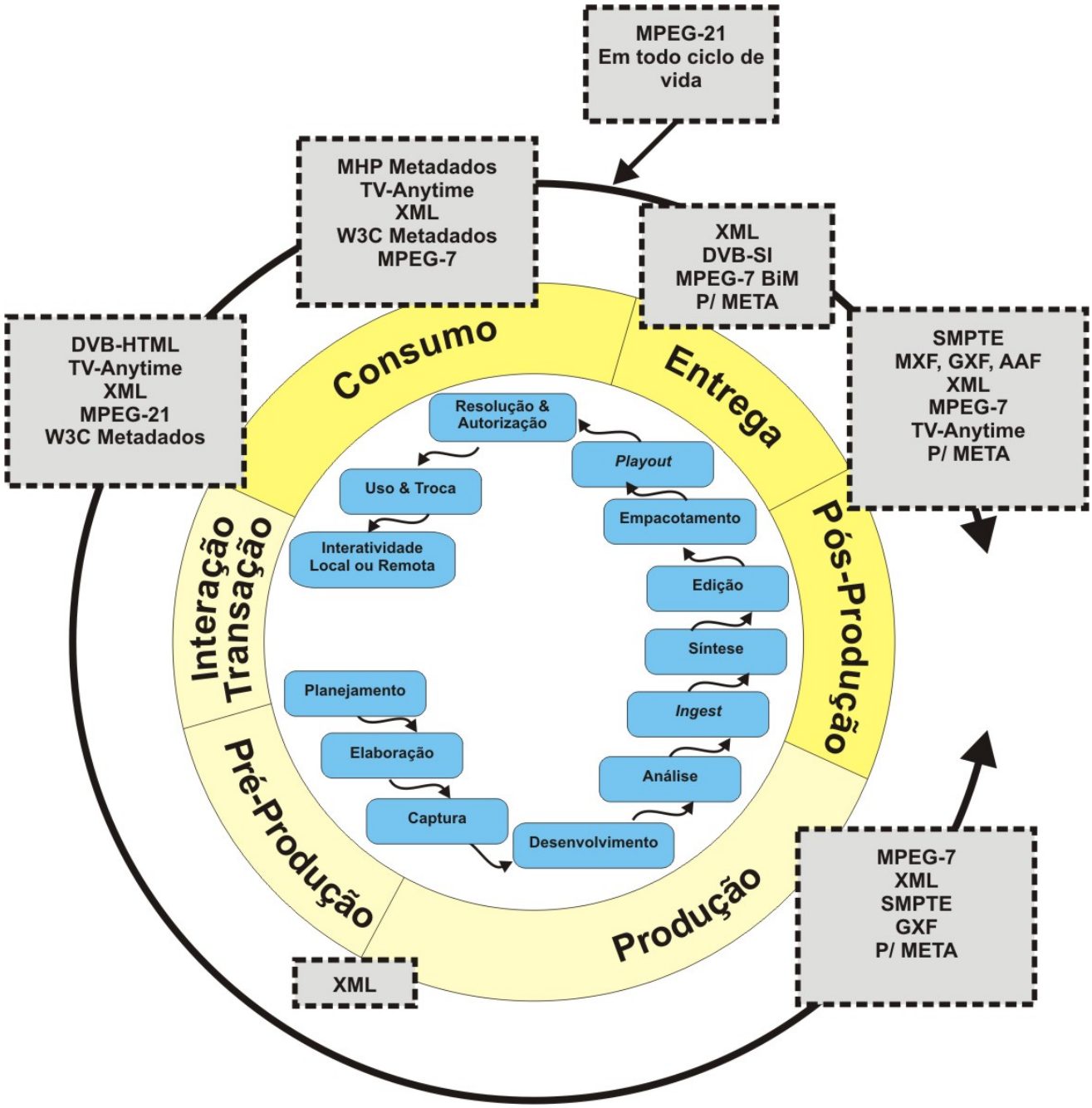


Figura 7.1 - Ciclo de vida dos metadados na TV Digital [18]

A fase de Consumo corresponde à apresentação e utilização dos serviços e conteúdos por parte do usuário. Uma estação de TV pode ainda adicionar seus serviços de informação além de definir como tal conteúdo poderá ser utilizado pelos usuários. Sendo assim, baseado nos direitos de acesso e opções de conteúdo restrito, o consumidor pode gravar a programação com o uso de um dispositivo como um vídeo cassete ou ter acesso aos serviços de informação.

Finalmente a fase de Interação corresponde ao processo de resposta por parte do usuário através da interação local realizada no próprio terminal de acesso ou através de interação remota via canal de retorno, se disponível.

Ainda na Figura 7.1 pode ser observado que cada etapa na cadeia de produção de conteúdo para TV Digital tem padrões específicos de metadados utilizados, por exemplo, nas etapas de produção, troca de mídia e empacotamento, os padrões mais utilizados são *Advanced Authoring Format* (AAF), *General Exchange Format* (GFX), *Material eXchage Format* (MXF), p/ META da EBU. Tais padrões estão focados nos produtores de conteúdos e provedores de serviços.

O SMPTE (*Society of Motion Picture and Television Engineers*) define um conjunto de padrões de *broadcast* e contém todas as definições dos metadados registrados dentre os quais o AAF, o GXF, o MXF e o P/META da *European Broadcast Union* (EBU).

O padrão AAF tem como principal característica seguir um modelo de fluxo de trabalho focalizando principalmente a troca, captura, edição e pré-visualização de conteúdo digital durante as etapas de pós-produção, fornecendo um modelo de integração com outros padrões pré-definidos como o MXF, SMPTE e o XML [18].

Já o padrão GXF foi definido pela SMPTE e descreve o conteúdo que possui ou não compressão de dados transportado em um *byte* do fluxo, além de descrever a própria estrutura do *byte* do fluxo multiplexado. É designado principalmente para troca de dados entre arquivos, edição, fontes de captura e execução (*playout*) [18].

O padrão MXF surgiu de um esforço cooperativo do *Professional MPEG Fórum*, EBU e AAF *Society*. Representa um formato de arquivo *stand-alone* que pode ser utilizado desde a fase de pré-produção até a pós-produção e pode ser substituído por outros formatos específicos de uma fase, como por exemplo, o formato AAF na fase de pós-produção [18].

Por fim, o esquema P/META da EBU define um conjunto de descritores comuns para possibilitar a troca de definições de metadados em âmbito de produção, entrega e repositório de conteúdo multimídia, dentro da cadeia de produção de conteúdo [18].

Segundo Lugmayr [18], três padrões estão em expansão no cenário mundial para descrição de multimídia e serviço interativo na TV Digital. São eles MPEG-7 [34], MPEG-21 [35] e TV-Anytime [36].

Em 1988 o *Moving Picture Experts Group* (MPEG) foi fundado e deu início a um processo de definição de uma série de padrões referentes aos recursos de multimídia.

Inicialmente foram definidos padrões referentes à compressão de áudio e vídeo como MPEG-1, MPEG-2 e MPEG-4. Em seguida, surgiram o MPEG-7, padrão de descrição para conteúdo áudio-visual, e o MPEG-21, padrão de especificação de empacotamento e proteção de conteúdo multimídia.

7.3.2 - MPEG–7

A crescente disponibilidade de conteúdo multimídia requer uma linguagem descritiva que seja eficiente, abrangente e de formato independente, a fim de permitir a localização e consumo de um conteúdo específico de forma rápida e precisa.

O padrão MPEG-7, também formalmente conhecido como “interface de descrição de conteúdo multimídia”, oferece um conjunto mínimo de ferramentas e de formato independente, o que permite a flexibilidade e interoperabilidade necessárias no processamento de conteúdo multimídia [37].

Este padrão está organizado em 8 partes, sendo estas:

- Parte 1 (Sistemas) – padroniza a transmissão binária, sincronização e formas de armazenamento;
- Parte 2 (DDL) – define a linguagem de metadados (Description Definition Language);
- Partes 3 e 4 (Áudio/Vídeo) – definem os esquemas de descrição de vídeo e áudio respectivamente;
- Parte 5 (Entidades Genéricas) – definem os esquemas de descrição de conteúdo genérico que não seja áudio ou vídeo;
- Parte 6 (*Software* de Referência) – define o *software* genérico que dá suporte às diferentes partes padronizadas;
- Parte 7 (Adaptação de Teste) – tem como foco principal os processos para teste do padrão MPEG-7 em *hardware* compatível ou implementações de software;
- Parte 8 (Extração e uso das descrições MPEG-7) – define a interface de descrição de conteúdo e procedimentos para o uso das ferramentas MPEG-7 e implementação em *software* de referência.

A descrição do conteúdo multimídia disponibilizada através deste padrão possibilita a especificação de informações que vão desde características de baixo nível, como por

exemplo, cor, textura, forma, e movimento, até informações de alto nível, como por exemplo, o nome de um personagem em uma cena.

A aceitação e utilização deste padrão no mercado multimídia são facilitadas a partir de uma definição mínima de padrões de especificação, ou seja, no caso, somente o formato da descrição de conteúdo está definido. A parte referente ao desenvolvimento de técnicas de extração, codificação e uso são realizados pela indústria. Já que o padrão MPEG-7 não só está focado na descrição do conteúdo, mas também visualiza de forma separada descrições e conteúdo – ainda que mantenha mecanismos de vinculação entre a descrição e o conteúdo - o conteúdo pode ser especificado de formas diferentes, de acordo com o contexto da aplicação. As etapas de criação da descrição e consumo da descrição não são contempladas no padrão.

Níveis relevantes de abstração podem ser obtidos na descrição do conteúdo devido ao formato utilizado. Assim, o uso do MPEG-7 permite que uma base de dados de conteúdo multimídia seja pesquisada manual ou automaticamente, como já ocorre em buscas textuais nos sistemas atuais. Isto traz grandes benefícios para as aplicações multimídia, como catálogos e bibliotecas virtuais.

Os tipos de ferramentas descritivas especificadas pelo padrão MPEG-7 são [38]:

- Descritores (D) – representam uma funcionalidade e definem a sintaxe e semântica na representação da funcionalidade**;**
- Esquemas de Descrição (*Description Schemes* – DS) – especifica a estrutura e a semântica dos relacionamentos entre os componentes que podem ser Descritores ou Esquemas de Descrição**;**
- Linguagem de definição de descrição – permite a criação de novos Esquemas de Descrição, bem como a extensão de esquemas já existentes**;**
- Ferramentas de Sistema – permite a junção de descrições, sincronização de descrições com o conteúdo associado, representação binária para armazenamento eficiente e transmissão, gerenciamento e proteção de propriedade intelectual, etc.

7.3.3 - MPEG-21

O MPEG-21 propõe uma padronização aberta, através da definição de um *framework*, para transmissão de mídia digital através da cadeia de valor de forma transparente, enfatizando

aspectos de proteção de direitos autorais, interoperabilidade, gerenciamento de conteúdo, proteção contra acesso e modificação não-autorizada, etc.

O *framework* proposto se baseia no conceito de item digital (*Digital Item* - DI) e na interação dos usuários com os itens digitais. Um item digital é a versão digital dos objetos "reais", como por exemplo, livros. Os elementos básicos de um DI são os recursos associados a descritores, podendo ser um recurso qualquer de multimídia, como vídeo, áudio ou mesmo metadados. Os descritores são normalmente definidos a partir de outros padrões de metadados e detém informações sobre os recursos, como por exemplo, variações de recurso, conteúdo, largura de banda requerida para permitir o acesso ao recurso, dentre outros. Resumindo, um DI é um objeto estruturado que possui conteúdo multimídia, metadados associados e estruturas que representam a relação entre os recursos e os metadados.

O padrão MPEG-21 apresenta as seguintes características:

- Empacotamento e vinculação de conteúdos multimídia aos descritores associados, independente de sua localização, em um DI que é tido como uma unidade atômica para processamento;
- Maior disponibilidade de informações sobre o conteúdo digital por parte dos usuários;
- Maior flexibilidade no acesso e consumo de conteúdo, possibilitados através de adaptação, transcodificação e transformação dos itens digitais de acordo com as requisições da rede e dos terminais de acesso;
- Interoperabilidade no gerenciamento de direitos autorais;
- Gerenciamento de conteúdo unificado baseado em uma estrutura de dados abstrata utilizada para armazenamento, processamento e adaptação de recursos multimídia;
- Definição de metadados para pacotes digitais lógicos, direitos autorais, formato de arquivo, etc. o que permite soluções heterogêneas e interoperáveis para manipulação de itens digitais direcionados por metadados.

Atualmente o padrão MPEG-21 está definido em 17 partes, sendo estas [39] [40]:

- Parte 1 (Visão, tecnologias e estratégia) – descreve o framework MPEG-21 em linhas gerais, apresentando cenários de uso, exemplos de aplicações e linhas gerais de compatibilidade;
- Parte 2 (*Digital Item Declaration* – DID)- define um conjunto de termos abstratos e conceitos que definem o modelo de um Item Digital. Neste modelo, a definição

do Item Digital abrange tanto a representação do conteúdo digital como também das possíveis ações disponíveis sob este conteúdo;

- Parte 3 (*Digital Item Identification* - DII) – o escopo desta parte inclui a especificação unívoca dos Itens Digitais e suas partes, especificação unívoca dos IPs relacionados aos Itens Digitais, especificação unívoca de Esquemas de Descrição, uso de identificadores para vincular Itens Digitais às informações relacionadas, como metadados descritivos, identificação de tipos diferentes de Itens Digitais;

- Parte 4 (*Intellectual Property Managemant and Protection Components – IPMP Components*) – define um framework genérico para proteção contra uso não autorizado de Itens Digitais;

- Parte 5 (*Rights Expression Language* – REL) – define uma linguagem de declaração de direitos e permissões utilizando os termos definidos no *Rights Data Dictionary*. A REL tem por finalidade prover mecanismos flexíveis e interoperáveis que possibilitam o uso de recursos digitais de forma transparente e escalonável na publicação, distribuição e consumo de filmes digitais, músicas digitais, livros eletrônicos, *broadcasting*, jogos interativos, *softwares* de computador e outros recursos digitais de criação, sempre permitindo a proteção do conteúdo digital e validação das permissões, condições e taxas associadas ao acesso do mesmo.

- Parte 6 (*Rights Data Dictionary* – RDD) – compreende um conjunto de termos claros, consistentes, estruturados, integrados e univocamente identificados que dão suporte à Linguagem de Expressão de Direitos (REL) do padrão MPEG-21.

- Parte 7 (*Digital Item Adaptation* – DIA) – Uma característica extremamente relevante no que se refere à utilização de redes e terminais de acesso para transmissão de conteúdo multimídia é o acesso transparente do conteúdo por parte do usuário, independente da plataforma utilizada. Sendo assim, a adaptação dos Itens Digitais é imprescindível, apesar de no caso do MPEG-21, não ser normativa;

- Parte 8 (*Reference Software*) – O *software* de referência do ISO/IEC 21000 como objetivos principais: validação das partes do MPEG-21, esclarecimento da especificação escrita das partes do MPEG-21 e adaptação de teste para checar a interoperabilidade das aplicações que primam pela compatibilidade com MPEG-21;

- Parte 9 (*File Format*) – Um Item Digital padrão MPEG-21 pode ser uma coleção complexa de informações. Além de mídia estática (imagens) e dinâmica (filmes), a especificação pode incluir informações pertinentes ao Item Digital, metadados, informação

de layout, etc, ou seja, tanto pode incluir dados textuais (XML) como dados em formato binário (por exemplo, uma apresentação MPEG-4 ou imagem estática);

- Parte 10 (*Digital Item Processing* – DIP) – especifica ferramentas que permitem que os usuários possam interagir com Itens Digitais através da inclusão de aspectos dinâmicos às declarações estáticas dos Itens Digitais;
- Parte 11 (*Evaluation Tools for Persistent Association Technologies* – PAT) – O termo "associação persistente" é usado para classificar todas as técnicas para o gerenciamento da identificação e descrição do conteúdo. Isto inclui a existência de identificadores dentro do contexto de diferentes tipos de conteúdo e formatos de transporte, incluindo cabeçalhos de arquivos e conteúdo agregado, como marcas d'água. Tal característica permite que os identificadores associados a conteúdo sejam protegidos contra alteração ou remoção não autorizados;
- Parte 12 (*Test Bed for MPEG-21 Resource Delivery*) – O *test bed* é composto basicamente por um *streaming player*, um servidor de mídia e um emulador de rede IP. A parte 12 descreve as APIs de cada componente do teste bed a fim de facilitar o processo de desenvolvimento de compontentes para conteúdos MPEG sob redes IP;
- Parte 13 (*Scalable Video Coding* - SVC) – Define uma nova tecnologia de codificação de vídeo com performance de alta compressão. Tal característica permite o vislumbre de grande otimização em Internet vídeo, Vídeo em redes *wireless*, vídeo para redes *wireless* móveis, VOD, transmissão *broadcast* em tempo real, produção e distribuição de conteúdo para múltiplos canais, aplicações do tipo vigilância que necessitam de armazenamento, etc;
- Parte 14 (*Conformance Testing*) – Especificações para adaptação e compatibilidade de teste para as várias partes do MPEG-21;
- Parte 15 (*Event Reporting*) – Especifica as formas para expressar eventos e requisições de eventos ocorridas;
- Parte 16 (*Binary Format*) – Especifica o formato binário para descrições baseadas na linguagem XML baseadas nas outras partes do MPEG-21. Isto possibilita a troca eficiente ou armazenamento das descrições MPEG-21;
- Parte 17 (*Fragment Identification for MPEG Media Types*) – Especifica uma sintaxe normativa para fragmentos de identificadores de URI a ser utilizado para endereçamento de partes de qualquer recurso do tipo áudio/mpeg ou vídeo/mpeg.

Originalmente, o padrão MPEG-21 foi criado como uma definição de metadados para o gerenciamento de direitos autorais, porém seu desenvolvimento atual se encontra além dos propósitos originais.

7.3.4 - TV-Anytime

O TV-Anytime (TVA) é um conjunto de especificações abertas para sistemas integrados e interoperáveis de forma que provedores de conteúdo, provedores de serviço e usuários possam manipular e armazenar conteúdo multimídia digital, principalmente nos dispositivos tipo gravadores de vídeo pessoais. Conforme o Fórum TV – Anytime [41], a expectativa é que uma aplicação executada em equipamentos de TV Digital deve, a princípio, ter acesso a armazenamento de dados (persistência), possibilitar a entrega de dados em redes independentes, interoperáveis e integradas através de sistemas existentes e especificar estruturas de segurança necessárias.

O padrão TV-Anytime tem como principais objetivos [42]:

- Possibilitar acesso por parte dos usuários a conteúdos personalizados, de acordo com interesses específicos e provenientes de vários provedores de conteúdo;
- Permitir o acesso e uso de conteúdo personalizado por parte dos usuários onde e quando desejarem, sem restrições de regras de acesso e uso.

O padrão TV-Anytime adota como formato de representação de metadados a DDL do padrão MPEG-7, que por sua vez é baseada na linguagem XML. Além de ser largamente utilizada, o XML traz diversas vantagens dentre elas a extensibilidade e a facilidade para separar dados e aplicação.

A especificação do padrão de metadados do TV-Anytime contém duas partes principais: Parte A e Parte B.

A Parte A trata dos chamados *Schemas* que descrevem a estrutura única de documentos de forma a agregar descrições de programas, usuários e atributos de classificação.

A Parte B contém o formato binário recomendado MPEG-7 BiM, um modelo de fragmentação, um modo de encapsulamento destes fragmentos e um método de indexação. Em outras palavras, define um conjunto de mecanismos que permite e otimiza o processo de entrega de conteúdo com metadados formatados de acordo com o padrão TVA. Os principais requisitos são a eficiência da largura de banda, capacidade para que os dados sejam transmitidos de forma assíncrona através do *carroussel* de dados, modularização da

informação enviada de forma a permitir atualizações parciais e priorização na forma como a informação é ciclicamente transmitida, melhorar o processo de navegação dentro da informação transmitida a fim de prover, quando necessário, uma forma eficiente de recuperar partes com acesso prioritário.

7.3.5 - Análise comparativa entre os padrões de formatação de metadados

Segundo Lugmayr [18], os metadados podem ser classificados em metadados orientados a *broadcast*, metadados orientados a multimídia e genéricos (Figura 7.2). Os padrões orientados a *broadcast* são aqueles que foram desenvolvidos especificamente para o uso em ambiente de *broadcast*. Já a maioria dos padrões de metadados orientados a multimídia emergiram dos tipos de serviços disponíveis na Internet.

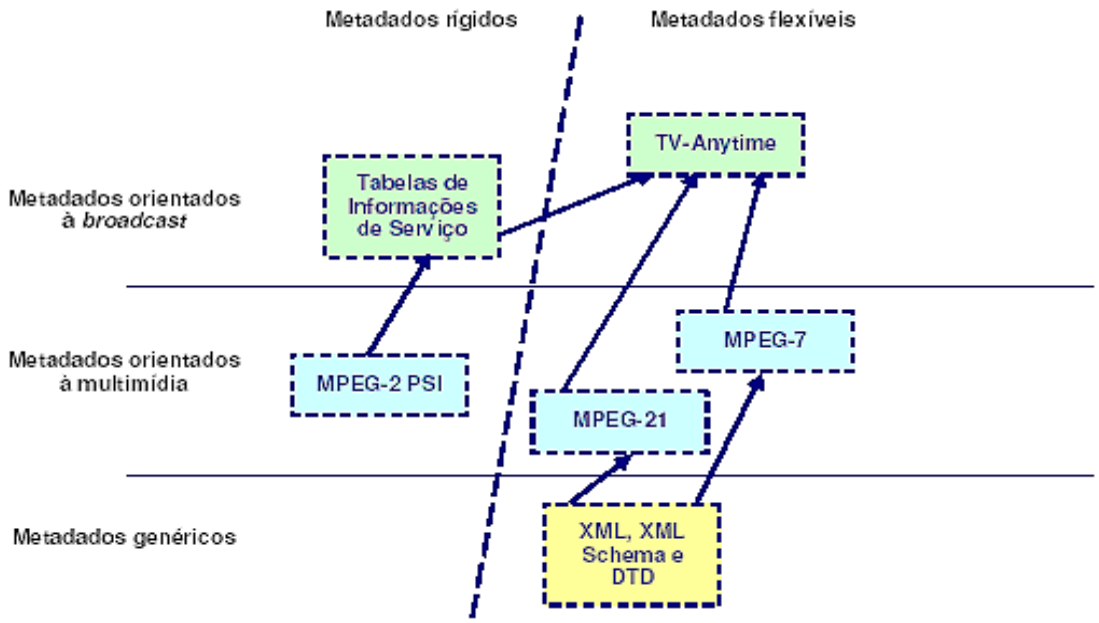


Figura 7.2 - Classificação dos Padrões de Metadados [18]

O padrão MPEG-7 trata em essência da descrição do conteúdo multimídia. O padrão MPEG-21 provê, dentre outros, ferramentas estruturadas de itens digitais e descritores para rede e capacidade de dispositivos. Em outras palavras, o padrão MPEG-21 possui uma abordagem onde os itens digitais são descritos numa visão mais abrangente e

encapsulam, de forma abstrata, os serviços disponíveis. Apesar de um item digital ser tido como um elemento genérico, a especificação DID (MPEG-21 Parte 2) tem como objetivo oferecer um conjunto de termos e conceitos que compõem um modelo para a representação padronizada dos itens digitais. Já o padrão TVA oferece uma estrutura completa para descrição semântica de serviços de TV entregues e consumidos no receptor do usuário. A ênfase maior do padrão TVA se dá no contexto da seleção de conteúdo e consumo posterior ao da transmissão.

Os três padrões descritos (MPEG-7, MPEG-21 e TVA) são baseados em XML, o que os caracteriza como padrões com facilidade de extensão e adaptação. Da mesma forma, os três padrões utilizam o MPEG-7 na codificação para transporte e MPEG-7 BiM como modelo de fragmentação e modo de encapsulamento dos fragmentos.

O padrão MPEG-21 trata de forma enfática do Gerenciamento de Direitos Digitais (DRM) apresentando três partes da especificação que tratam integralmente deste assunto, sendo elas, partes 4 (IPMP), 5 (RDD) e 6 (REL). A parte 4 define a forma de proteção para os itens digitais de uso não autorizado enquanto as partes 5 e 6 se referem ao gerenciamento dos direitos do usuário. O padrão TVA também possui aspectos relacionados ao DRM através do grupo *Rights Management and Protection* (RMP) que discute a proteção do conteúdo transmitido em *broadcast*. O padrão MPEG-7, por sua vez, aborda apenas alguns aspectos como autoria e controle de acesso.

Com relação à interação com o usuário, o padrão MPEG-7 associa as informações de interação do usuário com o conteúdo por meio das preferências do usuário e históricos de consumo de conteúdo multimídia. Desta forma, é possível personalizar o acesso, apresentação e consumo de conteúdo a partir do cruzamento de informações entre as preferências do usuário e descrição dos conteúdos. Neste sentido, o padrão MPEG-21 é mais abrangente, pois traz informações de todo o ciclo de vida do conteúdo digital ao longo da cadeia de distribuição (produção, distribuição e consumo). O *Digital Item Adaptation* (MPEG-21 – Parte 7) utiliza os esquemas do padrão MPEG-7 além de outros descritores, como por exemplo, descritor de preferências de apresentação, características de acessibilidade (ajuste de conteúdo para facilitar o acesso por portadores de deficiências auditivas e/ou visuais) e localização (informações de mobilidade e destino). Já no padrão TVA, a interface com o usuário é provida através dos componentes que efetuam a busca e aquisição de conteúdo, gerenciamento de armazenamento local e resolução de localização. Esta última tem por objetivo oferecer ao usuário um mecanismo de referência de conteúdo independente da localização do mesmo.

A Tabela 7.1 traz um resumo comparativo dos três padrões de metadados: MPEG-7, MPEG-21 e TV-Anytime segundo os requisitos apresentados.

Tabela 7.1- Comparação de requisitos apresentados pelos padrões MPEG-7, MPEG-21 e TV-Anytime [43]

Requisitos	**Padrão de Metadados**		
	MPEG-7	**MPEG-21**	**TV-Anytime**
Padronização e capacidade de extensão	Suporta	Suporta	Suporta
Descrição de serviços interativos para TV	Não suporta	Suporta parcialmente	Suporta
Define formato de codificação para transporte (fragmentação, encapsulamento)	Suporta	Suporta	Suporta
Provisão de serviços orientados ao ambiente de *broadcast*	Não suporta	Suporta parcialmente	Suporta
Descrição de conteúdo digital de multimídia	Suporta	Suporta parcialmente	Suporta parcialmente
Aspectos relacionados à DRM	Suporta parcialmente	Suporta	Suporta
Interação com usuário final	Suporta	Suporta	Suporta

8 – ESTUDO DE CASO

O estudo de caso tratado a seguir compreende as principais funções de um sistema que disponibiliza conteúdos de acesso restrito a usuários pré-cadastrados em uma base de dados. Desta forma, após a efetivação do *login*, os conteúdos disponíveis podem ser acessados, gerando quando aplicável cobrança através de um sistema de contabilização financeira.

A modelagem do sistema será baseada na sistemática adotada pelo *Rational Unified Process* (RUP). O RUP é um processo de engenharia de *software* que utiliza a abordagem da orientação a objetos em sua concepção fazendo uso da notação da *Unified Modeling Language* (UML) para ilustrar os processos em ação.

8.1 – ARQUITETURA DO SISTEMA

Cada camada apresentada na arquitetura de segurança é gerenciada por um componente específico o qual está disponível a partir de uma interface de comunicação *web*, por exemplo, uma interface *web service* a ser implementada por um provedor de serviço Internet.

Cada requisição de serviço solicitada a este provedor passa pelo Gerenciador de Segurança, de forma que este tenha o controle sobre quais serviços poderão ter o acesso efetivado ou não.

A checagem de acesso executada pelo Gerenciador de Segurança envolve interação com o Gerenciador de Usuários, Gerenciador de Contabilização Financeira, Gerenciador DRM e indiretamente Gerenciador de Licenças (Figura 8.1).

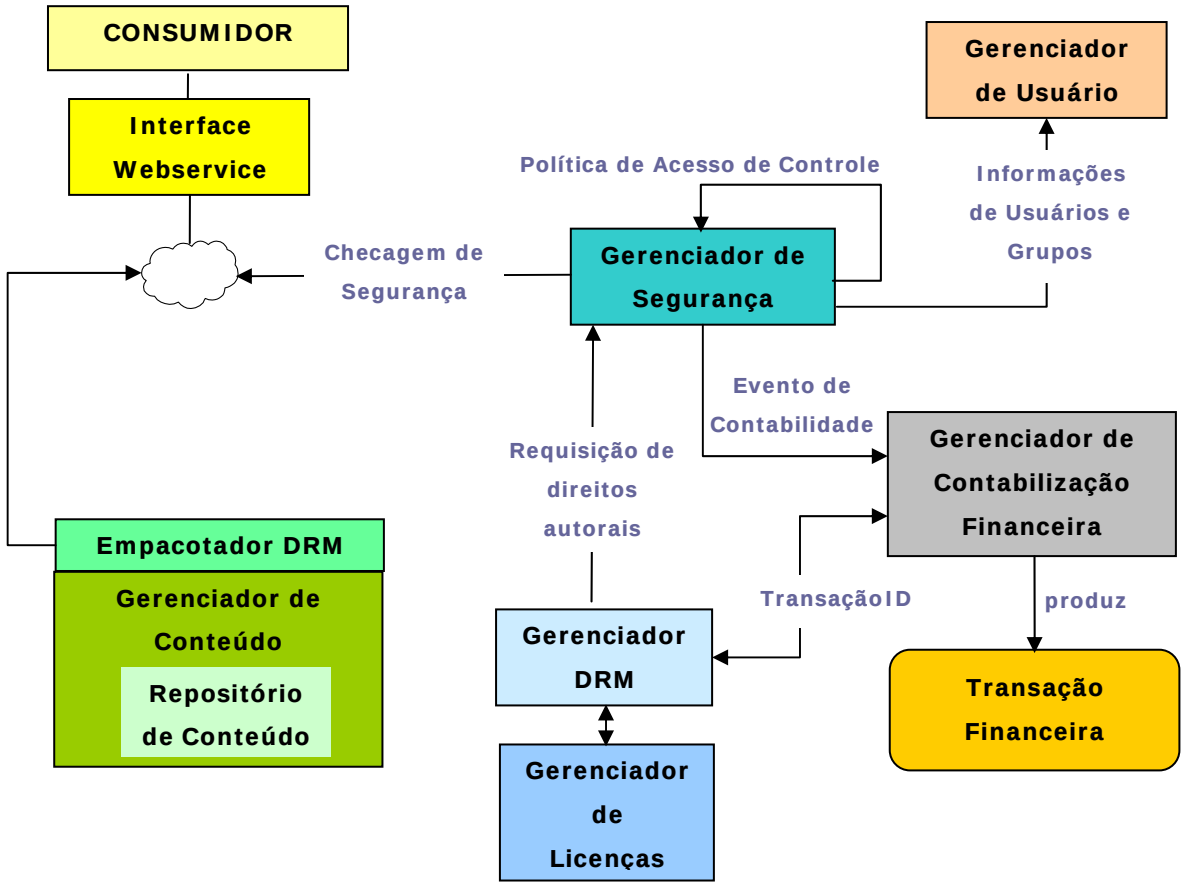


Figura 8.1 - Arquitetura do sistema

8.2 – PROCESSOS RELACIONADOS AO ACESSO DE CONTEÚDO RESTRITO

Os principais subsistemas referentes ao consumo de conteúdo restrito por parte de usuários são: autenticação, gerenciamento de usuários, tratamento de direitos autorais, contabilização financeira e autorização.

8.2.1 - Autenticação de usuário

A primeira etapa para que um usuário tenha acesso ao conteúdo restrito corresponde à etapa de autenticação. Autenticação é o processo pelo qual o usuário comprova que é quem diz ser através da apresentação de credenciais a fim de comprovar sua identidade. Uma vez realizada, o usuário passa para o status de usuário autenticado.

O processo de autenticação consiste dos seguintes casos de uso (Figura 8.2):

- Registrar em Novo Serviço – Todo usuário deve ser previamente registrado como usuário de um serviço específico para poder fazer uso do mesmo, porém, antes de se registrar, o usuário deve ser autenticado através do caso de uso Efetuar *Login*.
- Eliminar Registro de Serviço – O usuário, ao desistir do acesso a um determinado serviço, pode eliminar seu registro naquele serviço.
- Efetuar *Login* – O usuário provê informações a fim de comprovar sua identidade. Uma vez autenticado, não necessita mais de efetuar o login, mesmo que faça uso de diversos serviços. Uma nova sessão se inicia com o login do usuário.
- Efetuar *Logout* – O usuário finaliza a sessão de trabalho e a partir daí é considerado usuário anônimo.

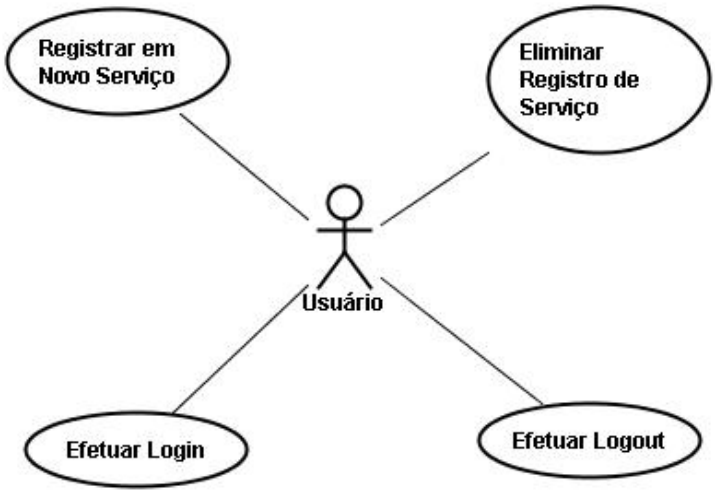


Figura 8.2 - Casos de uso do processo de autenticação do usuário

8.2.2 - Gerenciamento de usuários.

O gerenciamento de usuários é utilizado para identificar a identidade do usuário. É a partir dele que os usuários propriamente ditos são criados e organizados em grupos a partir de funções atribuídas a eles, bem como são definidas as permissões de acesso ao conteúdo por parte dos usuários.

Os principais casos de uso referentes ao gerenciamento de usuários são (Figura 8.3):

- Manter Conta de Usuário – A conta do usuário detém toda informação sobre a identidade do mesmo. O usuário deverá ter um identificador único e uma senha de acesso individual do usuário para que ele mesmo possa acessar seus dados e alterar parte desses dados. Outras informações relevantes podem ser armazenadas no banco de dados como, por exemplo, *email*, nome completo, endereço, etc.
- Gerenciar Funções de Usuários – Os grupos de usuários representam um conjunto de usuários que compartilham as mesmas permissões de acesso dentro de um mesmo contexto. As funções agregadoras que são quem determinam a formação dos grupos são definidas a partir de um nome único, descrição e uma lista de permissões associadas.
- Associar Permissões de Grupos de Usuários aos Recursos – Corresponde à definição da política de segurança para os recursos/conteúdos disponíveis onde são vinculados os grupos de usuários, a partir das permissões previamente definidas, aos recursos/conteúdos disponíveis.
- Associar Funções aos Usuários – Provê meios que define o mapeamento para vinculação das funções agregadoras aos usuários e grupos de usuários.
- Gerenciar Grupos de Usuários – Um usuário pode pertencer a um ou mais grupos.

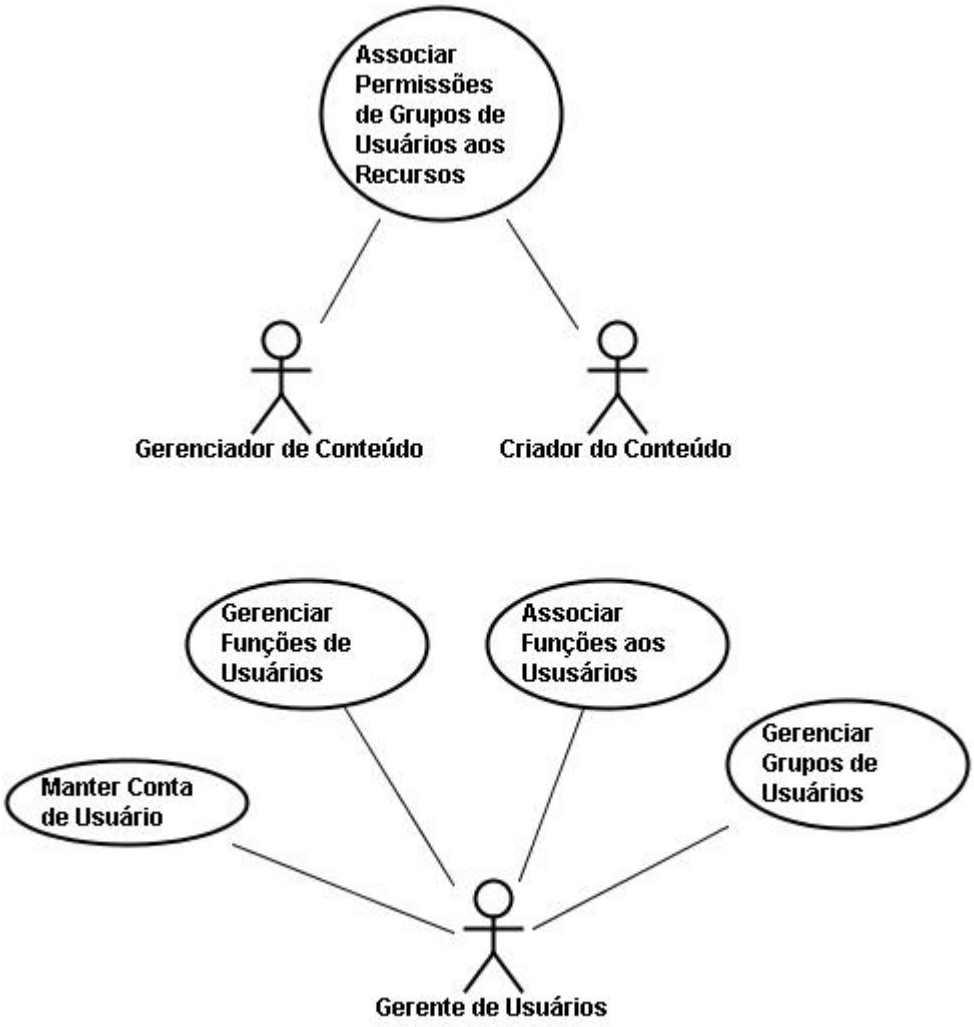


Figura 8.3 - Casos de uso do gerenciamento de usuários

8.2.3 - Gerenciamento de segurança

Cada acesso aos serviços ou conteúdos restritos deve conter informações sobre o usuário que invoca o serviço, as credenciais de identificação providas, o contexto de segurança e o nome da operação a ser executada.

Em outras palavras, o Gerenciador de Segurança deve verificar se um determinado usuário que requisita uma operação específica sobre um determinado conteúdo ou serviço tem permissão para tanto. No sistema proposto, isto é feito através da definição e avaliação das políticas de acesso de controle para recursos e operações sobre os mesmos, usando como base o modelo de controle que por sua vez é baseado em funções pré-definidas.

Para cada recurso que por sua vez é identificado por uma URN (*Uniform Resource Name*), uma política de controle pode ser declarada dentro do Gerenciador de Segurança, vinculando outras funções às permissões (direitos de executar operações).

Desta forma, toda vez que o Gerenciador de Segurança identifica um pedido de acesso a serviço ou conteúdo, ele busca as informações das funções disponíveis para o usuário em questão e toma uma decisão referente à autorização requisitada a partir do mapeamento entre o recurso URN cadastrado e o método invocado.

O processo de segurança abrange também os direitos autorais dos conteúdos disponíveis. Os principais casos de uso referentes ao gerenciamento de direitos autorais são:

- Definir Direitos Digitais para o Conteúdo – Através da especificação de um identificador único de conteúdo, os Direitos Digitais vinculados ao mesmo devem ser criados e editados sujeitando a publicação deste a certas condições (*royalties*, não comercial, uso científico do recurso, etc), permitindo assim a transferência da licença de uso a partir do proprietário dos direitos autorais ao provedor do conteúdo.
- Exibir Direitos de Proteção Intelectual (IPR) – A partir do identificador único de conteúdo, os direitos de proteção intelectual do conteúdo podem ser exibidos.
- Liberação dos Direitos Digitais – Caso um usuário tenha intenção de acessar determinado conteúdo protegido, o acesso à descrição dos direitos digitais vinculados a tal conteúdo permite a verificação se é possível obter a licença a partir do proprietário dos direitos digitais bem como a forma de obter esta licença. Desta forma, o usuário deverá seguir todos os passos definidos na licença a fim de finalizar a transação e obter a liberação dos direitos digitais para o conteúdo. Caso seja necessário, o pedido de liberação pode ser enviado ao proprietário dos direitos para efetivação manual da liberação.
- Criar Marca D'água – Uma vez efetivada a transação que permite o acesso a um conteúdo específico, o usuário pode obter uma cópia do mesmo. Desta forma, o conteúdo deve ter uma marca d'água implantada antes de chegar ao usuário que permita, dentre outros, a referência do identificador da transação a fim de identificá-la posteriormente.
- Detectar a Marca D'água – Permite a checagem e extração das informações contidas na marca d'água embutida no conteúdo.
- Gravar Informações de Direitos Digitais nos Conteúdos – Cada provedor de conteúdo deve ser apto a associar informações de direitos digitais a um ou mais objetos de

conteúdo. Apenas após esta etapa que o conteúdo se torna disponível no sistema de armazenamento do provedor de conteúdo para distribuição.

- Modificar Informações de Direitos Digitais nos Conteúdos - O provedor de conteúdo deve ser apto a alterar ou ampliar os métodos de publicação e/ou permissões de uso para os itens do conteúdo digital.

8.2.4 - Contabilização financeira

O processo de contabilização ou transações financeiras é gerado uma vez que o conteúdo protegido é disponibilizado após a obtenção da licença de uso do mesmo.

Os principais casos de uso referentes ao processo de contabilização são:

- Criar Políticas de Cobrança – Cada organização tem autonomia para definir como os usuários sofrerão cobranças pelos serviços nos quais estão registrados.
- Atualizar Políticas de Cobrança - Cada organização tem autonomia para alterar as políticas de cobrança já estabelecidas.
- Visualizar Políticas de Cobrança - Cada organização tem acesso às informações das políticas de cobrança definidas para os usuários.
- Associar Política de Cobrança à Operação – Uma política de cobrança pode ser associada à cada operação.
- Pesquisar Eventos de Cobrança – Para cada usuário é possível obter uma lista de operações relevantes de cobrança bem como os identificadores únicos de transação.
- Efetuar Pagamento – Pode ser requerido que o usuário pague uma taxa pelo registro em um serviço específico ou para acessar um conteúdo restrito. Uma vez que a identidade do usuário é estabelecida, ele é redirecionado para um sistema de pagamento. Tal sistema resulta em uma transação de pagamento onde a quantia paga é registrada. Esta informação se torna disponível no processo de contabilização e a atual sessão do usuário é atualizada de forma que o mesmo tenha acesso ao conteúdo ou serviço pelo qual pagou.

8.2.5 - Autorização

O processo de autorização define se um usuário específico tem permissão para efetuar uma ação requisitada de tal forma que tal permissão deve ser verificada anteriormente da ação ser executada.

As informações de autorização podem ser construídas baseadas em políticas de acesso que vinculam um recurso a um conjunto de permissões requeridas de forma a habilitar a execução de ações específicas sobre o recurso em questão.

A autorização deve existir em dois níveis: estática, que define políticas de acesso a serviços e conteúdo restrito, e dinâmica que pode sobrescrever a autorização estática caso condições específicas sejam encontradas, como por exemplo, a taxa de acesso é paga.

Quando o usuário tenta acessar um serviço ou conteúdo restrito, o primeiro passo é checar as políticas de segurança, ou seja, as permissões mapeadas entre conteúdo e usuário associadas aos mesmos. Caso o usuário já possua o direito de executar a operação requerida de acordo com as permissões estáticas, nada mais é necessário para acessar o conteúdo. Por outro lado, caso o usuário não possua as permissões necessárias para acessar o conteúdo, é verificado se a transação necessária para tal já foi realizada junto ao sistema de cobrança. Se a transação já tiver sido efetivada, o usuário ganha dinamicamente a autorização de acesso requisitada. A transação que gera autorização de acesso dinâmica é realizada pelo subsistema de contabilização financeira, mais especificamente como resultado do caso de uso Efetuar Pagamento apresentado anteriormente.

8.3 – CONTROLE DE ACESSO

O controle de acesso define a forma que o desenvolvedor da aplicação pode restringir quais operações podem ser executadas em um sistema. Existem vários modelos de controle empregados no desenvolvimento de aplicações. Para o estudo de caso em questão, o modelo utilizado se baseia em funções que definem grupos de usuários que compartilham os mesmos direitos de acesso, ou seja, um grupo corresponde a um conjunto de usuários que compartilham as mesmas funções. A cada função é associado um conjunto de permissões em um dado contexto de segurança. Desta forma, o usuário pode acessar serviços e conteúdos de acordo com as permissões associadas às funções as quais ele se encontra vinculado. Um conjunto básico de operações é vinculado com a função especial “usuário anônimo” que é associado a cada usuário por padrão.

A grande vantagem deste modelo baseado em funções é a escalabilidade. Como as permissões indicam o tipo de acesso aos recursos disponíveis, a segurança no sistema cresce e a cada vez que uma nova funcionalidade ou novo tipo de conteúdo é agregado. Sendo assim, o administrador que gerencia as políticas de controle de acesso terá somente o trabalho de especificar que os usuários agregados a funções específicas são quem podem acessar o conteúdo novo. Em outras palavras, o administrador é quem define o conjunto de funções e o associa aos usuários. Tal modelo de acesso de controle é conhecido como RBAC (*Role Based Access Control*).

8.3.1 - Diagrama de classes

O diagrama de classes da Figura 8.4 ilustra a interface de segurança para o controle de acesso. As principais classes do subsistema de Controle de Acesso são:

- GerenciadorUsuário - Esta interface agrupa todas as operações referente somente à busca de informações no grupo de usuários disponível sem disponibilizar qualquer tipo de operação de modificação nos dados;
- GerenciadorFuncao – Permite a manutenção das informações e operações vinculadas às funções. Provê operações que permitem criar e apagar funções, associar tais funções a um ou mais usuários e listar as funções existentes;
- GerenciadorRegistro – Responsável pela criação, alteração e exclusão dos perfis de usuário;
- GerenciadorPermissoes – Permite verificar o tipo de autorização concedida ao usuário para o acesso de um determinado conteúdo ou serviço;
- Usuario – Esta classe provê todos os métodos necessários para manipular as informações relacionadas a um determinado usuário. Adicionalmente, permite a vinculação de novos atributos, como nome, endereço, etc., a serem definidos na classe Atributo;
- Atributo – Permite a especificação de um novo atributo genérico a ser vinculado à classe Usuario;
- Funcao – Classe que contém informações relacionadas às funções vinculadas aos grupos de usuários;
- Grupo – Classe utilizada pela classe Funcao para vincular dinamicamente um conjunto de usuários a uma função específica;

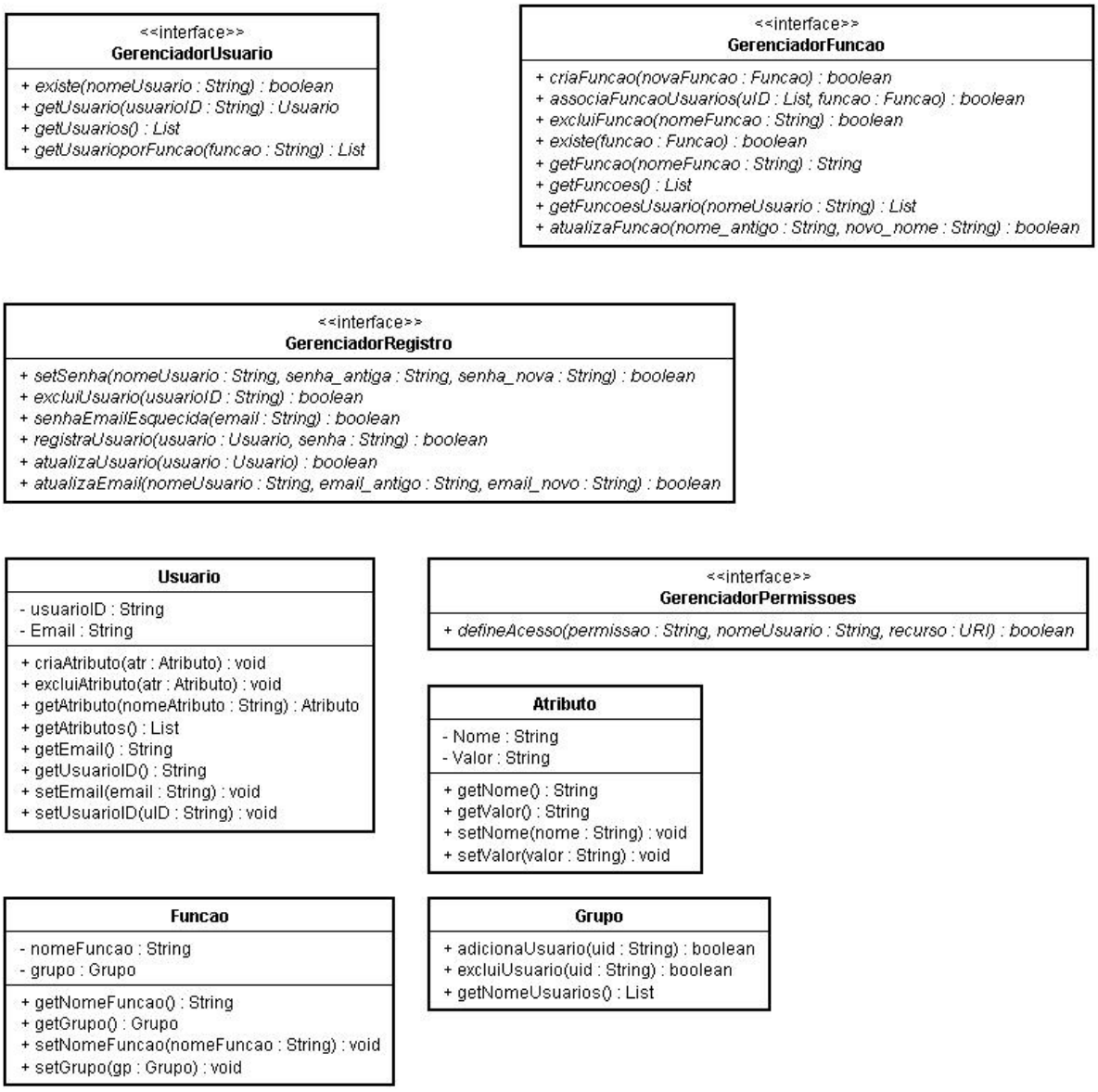


Figura 8.4 - Diagrama de classes da gerência de segurança referente ao controle de acesso

8.4 – CONTABILIZAÇÃO FINANCEIRA

O subsistema de contabilização financeira é usado para checar e manipular eventos de contabilidade vinculados à operação a ser executada dentro de um dado contexto de segurança. Tal operação gera os eventos de contabilidade para, a partir daí, habilitar o acesso a conteúdos restritos e/ou gerar cobrança.

Este subsistema possui forte relação com o subsistema de tratamento de direitos autorais o qual é a principal fonte de eventos de contabilização financeira. O processo de

tratamento de direitos autorais utiliza a efetivação das transações financeiras como condição primordial para liberação dos direitos digitais de uso do conteúdo restrito.

8.4.1 – Diagrama de classes

O diagrama de classes da Figura 8.5 ilustra a interface para tratar o processo de contabilização financeira, gerando eventos de contabilidade, criando políticas de contabilização dentre outros.

As principais classes do subsistema de Controle de Acesso são:

- GerenciadorContabilidade – Esta interface representa o ponto de partida para todas as operações relacionadas ao sistema de contabilidade financeira;
- PoliticaContabilidade – Interface que provê as funcionalidades relacionadas à modificação das políticas de contabilidade financeira. Basicamente a política de contabilidade define quais ações, instâncias da classe AcaoContabilidade devem ser disparadas. Uma política pode conter uma ou mais ações relacionadas. Somente o administrador do sistema de contabilidade pode modificar as políticas estabelecidas;
- ContabilidadeAdapter – Define métodos a serem estendidos por outras interfaces;
- AcaoContabilidade – Relaciona eventos de contabilidade a uma dada ação;
- EventoContabilidade – Define a funcionalidade genérica de um evento de contabilidade. Toda ação é vinculada aos usuários e a um ou mais eventos derivados desta classe;
- EventoCobranca – Interface que define as funcionalidades sobre a geração de cobrança propriamente dita;
- EventoLogging – Interface que detém as funcionalidades relacionadas ao esquema de armazenamento de informações de uso (log) para rastreamento posterior das atividades realizadas;
- Transação – Detém as informações associadas aos eventos de cobrança, objetos derivados da classe EventoCobranca;

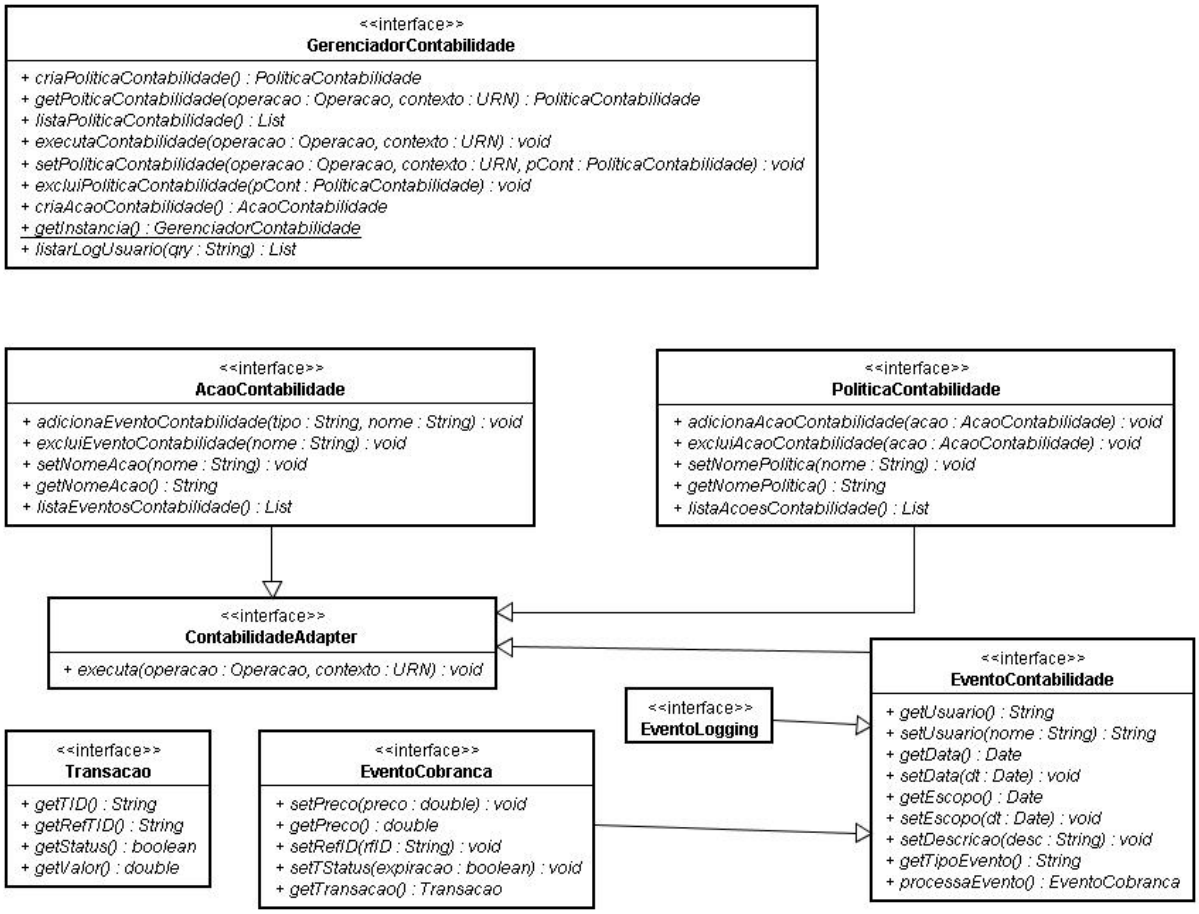


Figura 8.5 – Diagrama de classes do gerenciador de contabilização financeira

8.4.2 – Diagrama de seqüência

O diagrama representado na Figura 8.6 traz a seqüência de passos relacionados à criação de uma nova política de contabilidade. O administrador do subsistema de contabilidade é quem dá início a este processo. Inicialmente é preciso identificar uma ação derivada da classe AcaoContabilidade ou criar uma nova ação. Uma vez identificada a ação para a qual a nova política de contabilidade será criada, a nova política poderá ser criada e por fim vinculada à ação especificada. Uma política de contabilidade pode possuir diversas ações vinculadas.

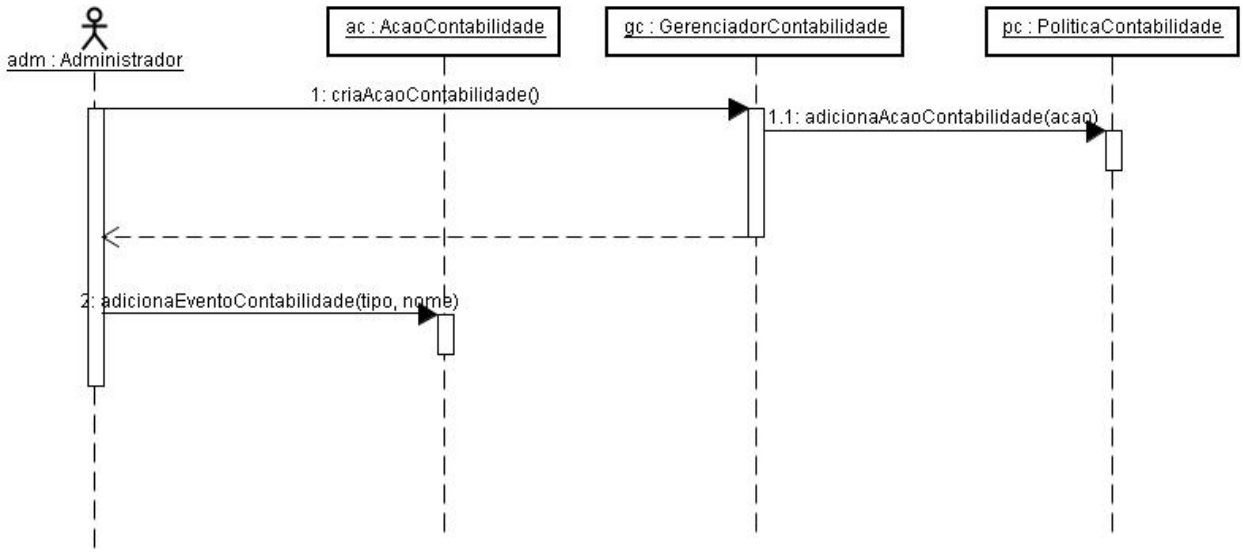


Figura 8.6 - Diagrama de seqüência da criação de política de contabilidade

Cada operação possível é vinculada a uma única política de cobrança, porém o mapeamento entre uma operação e uma política não é feito diretamente. Em outras palavras, o contexto, ou URN, sobre o qual a operação é executada é quem torna possível tal mapeamento. Uma vez identificada a política a partir da operação solicitada, as ações associadas àquela política de cobrança são buscadas e por conseqüência, os eventos relacionados às ações são disparados. Por fim, os eventos de cobrança, derivados da classe EventoCobranca, buscam as informações contábeis dos valores relacionados à operação solicitada a partir do GerenciadorDRM (Figura 8.7). A vinculação da operação à política de cobrança pode ser observada no diagrama de seqüência da Figura 8.8.

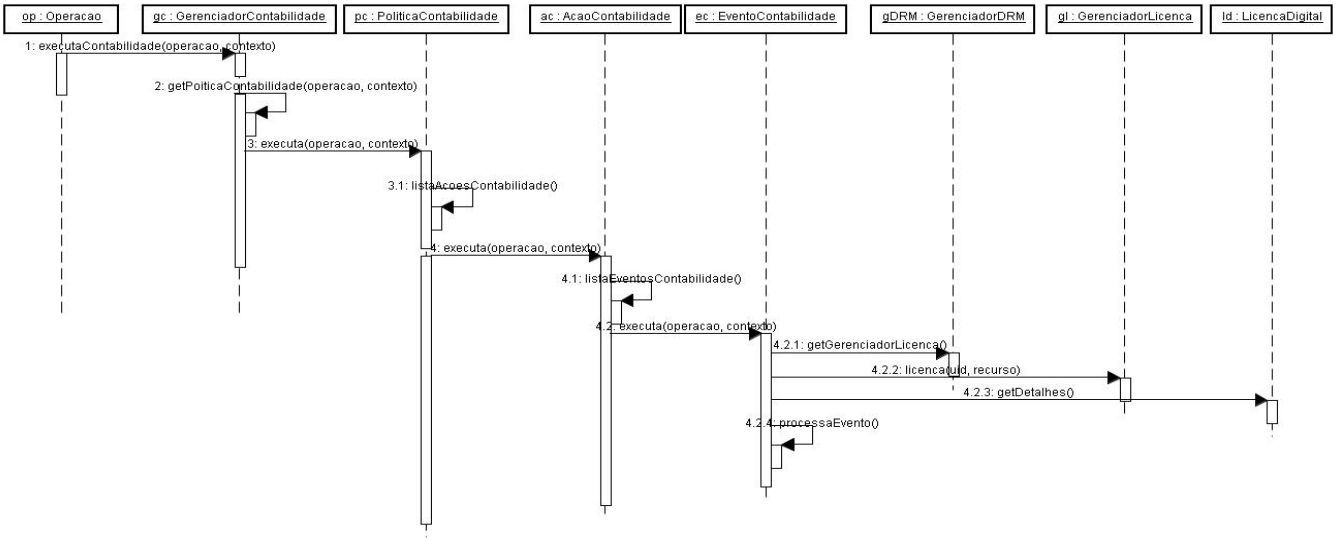


Figura 8.7 - Diagrama de seqüência da execução de cobrança

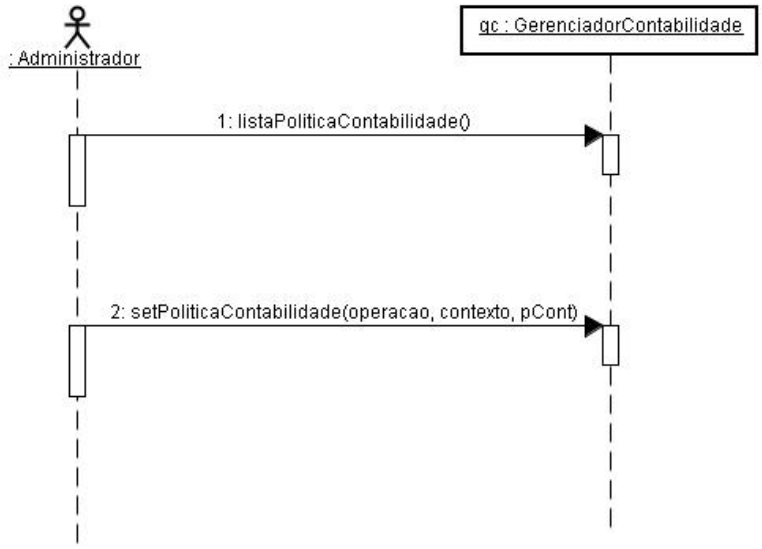


Figura 8.8 - Diagrama de seqüência da vinculação da política de cobrança às operações

É possível ainda listar os eventos de contabilidade gerados por usuário a fim de emitir relatórios ou para simples conferência, caso necessário (Figura 8.9).

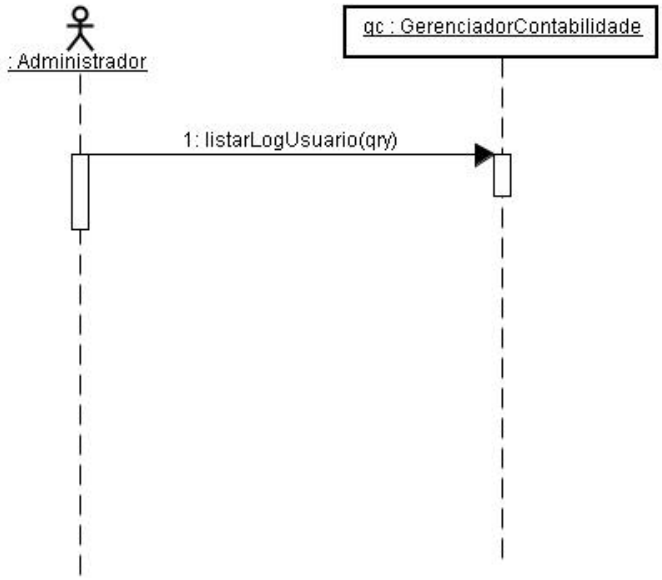


Figura 8.9 - Diagrama de seqüência da pesquisa de eventos de contabilidade

8.5 – PROTEÇÃO DOS DIREITOS DE PROPRIEDADE INTELECTUAL

O subsistema de Gerenciamento de Direitos Digitais tem como finalidade a verificação dos direitos autorais do conteúdo ou serviço requisitado e quais são as etapas a serem cumpridas a fim de obter a liberação de acesso ou utilização dos mesmos. A partir das informações e condições obtidas, o módulo DRM pode negar o acesso ao conteúdo ou gerar dinamicamente a autorização de acesso a partir da criação de uma licença segundo um modelo pré-definido baseado na XrML. A geração de tal autorização dispara eventos de contabilidade a serem manipulados pelo Gerenciador de Contabilidade.

A inserção de marcas d'água digitais é considerada das técnicas mais eficientes para vincular os direitos digitais a um conteúdo multimídia como áudio, vídeo e imagens. Diversos algoritmos têm sido desenvolvidos neste sentido de forma a satisfazer as condições necessárias, tanto do ponto de vista do conteúdo a ser protegido como também dos metadados a serem embutidos dentro do conteúdo propriamente dito. É possível, por exemplo, ocultar metadados no conteúdo por motivos de segurança e confidencialidade. Desta forma, somente aqueles que têm conhecimento da existência dos metadados inseridos no conteúdo podem acessá-los desde que tenham autorização para isto.

A licença de acesso a ser gerada deverá ser baseada em um padrão DRM REL. Os metadados contidos na licença devem fornecer no mínimo as informações sobre a concessão de uso do conteúdo restrito, o código identificador único da licença, condições de uso e o emissor da licença. A sugestão de padrão de metadados utilizado para criação da

licença é o padrão MPEG-21 REL, pois como foi visto anteriormente, este padrão provê um modelo completo para declaração de direitos digitais além de permitir a interoperabilidade em casos de importação e exportação de arquivos de licença com sistemas externos.

As condições de uso definem quantas vezes o conteúdo pode ser acessado, o período disponível para o acesso (data de expiração dos direitos adquiridos), dentre outros.

As funcionalidades básicas disponíveis no Gerenciador de DRM são:

- Verificar se o usuário possui licença para acesso a conteúdo restrito;
- Criação, alteração e exclusão de licenças;
- Importar e exportar licenças para possibilitar interoperabilidade entre sistemas que utilizam o mesmo padrão de metadados;
- Validação de licenças importadas de outros sistemas, o que envolve a verificação da assinatura digital da licença obtida de forma a atestar que a mesma não foi adulterada;
- Criação e detecção de marca d'água.

8.5.1 - Diagrama de classes

O diagrama de classes da Figura 8.10 ilustra a interface para proteção de direitos autorais através da geração de licenças de acesso, inserção de marcas d'água no conteúdo protegido, validação de licenças importadas de outros sistemas, dentre outros.

As principais classes do subsistema Gerenciador de DRM são:

- GerenciadorDRM – trata as requisições para acesso ao Gerenciador de Licenças e Validação de Direitos autorais;
- GerenciadorLicenca – Detém todas as operações relacionadas às licenças digitais;
- ValidadorLicenca – Responsável pelo processo de validação de licenças obtidas externamente;
- RELAcao – Efetiva o mapeamento entre as operações e ações;
- DRMResposta – Interface que auxilia na extração de informações retornadas pelo GerenciadorDRM quando um processo de validação de licença é efetuado;
- LicencaDigital – Interface que busca a Licença armazenada no sistema DRM e traz as informações armazenadas na Licença;

- CriptografiaAdapter – Interface que provê os métodos genéricos para cifração.
- DadosAdapter – Interface criada a partir da CriptografiaAdapter pelo processo de especialização que provê formas de cifração e decifração de informações resultantes dos processos da classe GerenciadorDRM;
- MarcaDaguaAdapter – Interface que detém o processo de inserção e recuperação de marcas d'água em conteúdos restritos.

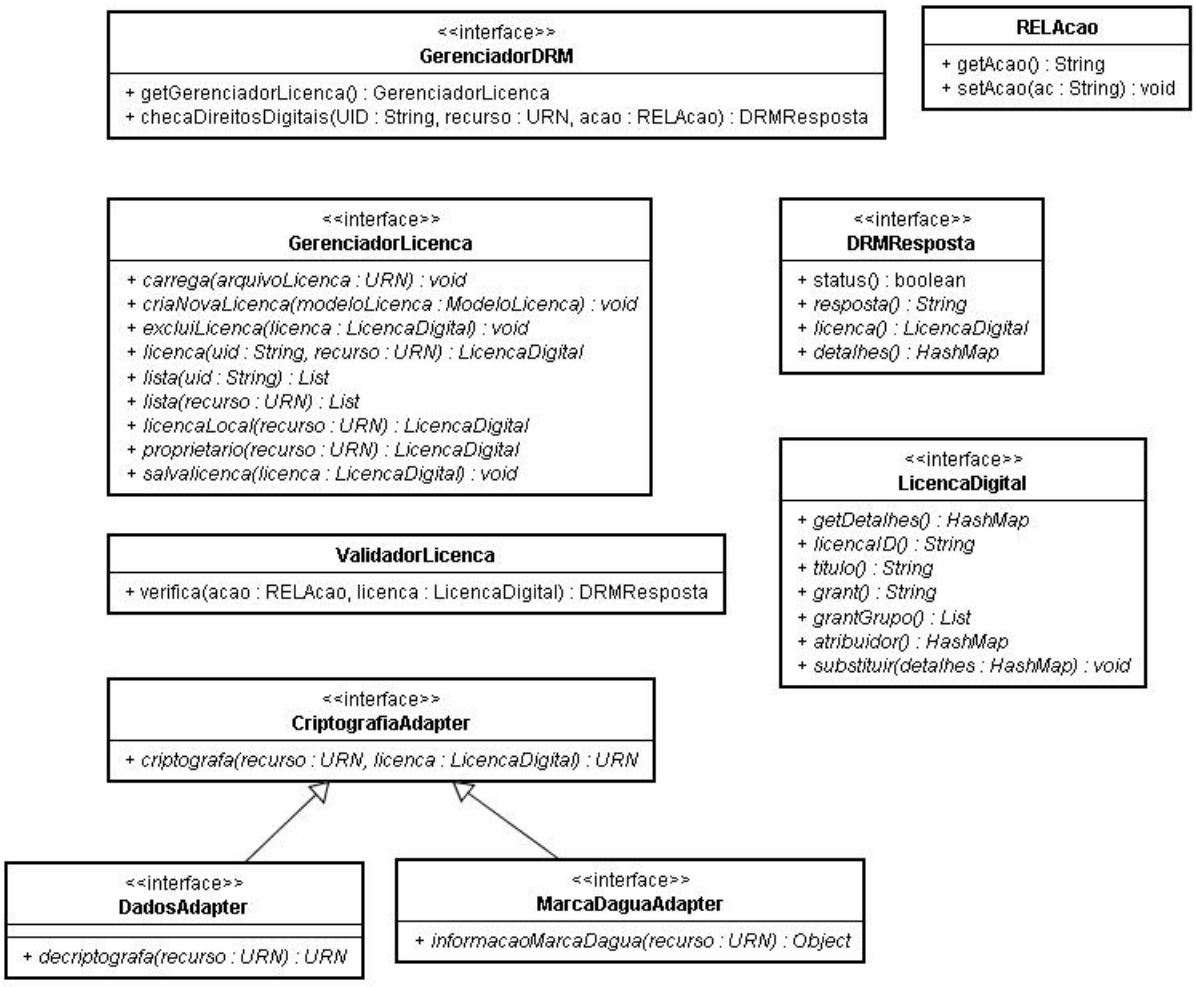


Figura 8.10 - Diagrama de classes do gerenciamento de direitos autorais

Uma das funcionalidades do subsistema de tratamento de DRM é criar dinamicamente a licença a partir de uma requisição de usuário, ou seja, é possível um usuário adquirir nova licença caso queira acessar um conteúdo restrito para o qual não possui licença de acesso ou a que possui já esteja com o prazo de utilização expirado.

Adicionalmente, é possível realizar alteração nos parâmetros da licença caso o usuário requisite uma modificação das permissões vinculadas à que possui de forma a possibilitar a utilização dos recursos disponíveis.

A requisição para criar, modificar ou excluir é tratada pela classe GerenciadorLicenca.

A Figura 8.11 mostra o processo de criação de uma nova licença de acesso. A licença é um objeto criado a partir da classe LicencaDigital. A licença é preenchida com as informações requisitadas e então armazenada. O licenciador do recurso (proprietário dos direitos autorais) é identificado e o processo para a geração da licença é iniciado a partir da análise da licença primária do licenciador. Em seguida, as credenciais do licenciador são validadas bem como é checado se o mesmo possui permissão para outorgar nova licença de uso. Por fim, a nova licença é assinada digitalmente pelo licenciador.

A licença gerada é então armazenada no próprio DRM, porém sem estar ativada. A ativação é efetivada após a execução do evento de contabilidade associado às políticas de contabilidade definidas pelas condições de acesso.

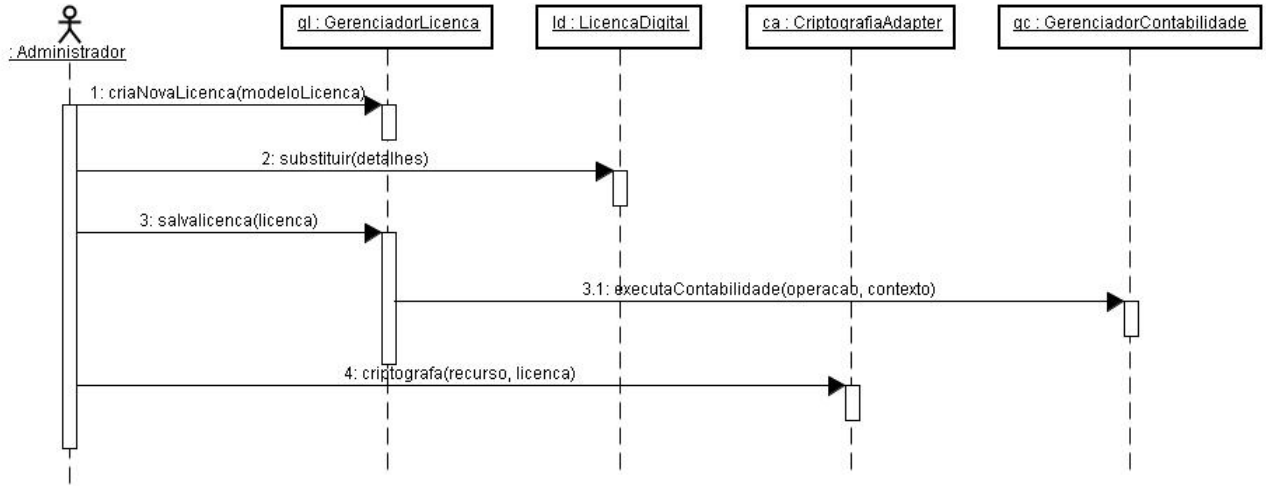


Figura 8.11 - Diagrama de seqüência para criação de licença de acesso

O processo de modificação da licença de acesso pode ser observado na Figura 8.12. Caso o usuário faça uma requisição de alteração de ação, o DRM efetua a modificação da licença existente. Os dados do usuário são validados e o processamento da nova informação é iniciado. As credenciais do licenciador são validadas de forma a conferir se o mesmo possui permissão para permitir a inclusão de uma nova ação na licença de uso. Por fim, a nova licença é assinada digitalmente pelo licenciador e armazenada no DRM. A

nova permissão conferida só se torna ativada após o evento de contabilidade associado a esta alteração ser finalizado com sucesso. Licenças com prazo expirado ou inativas não podem ser modificadas.

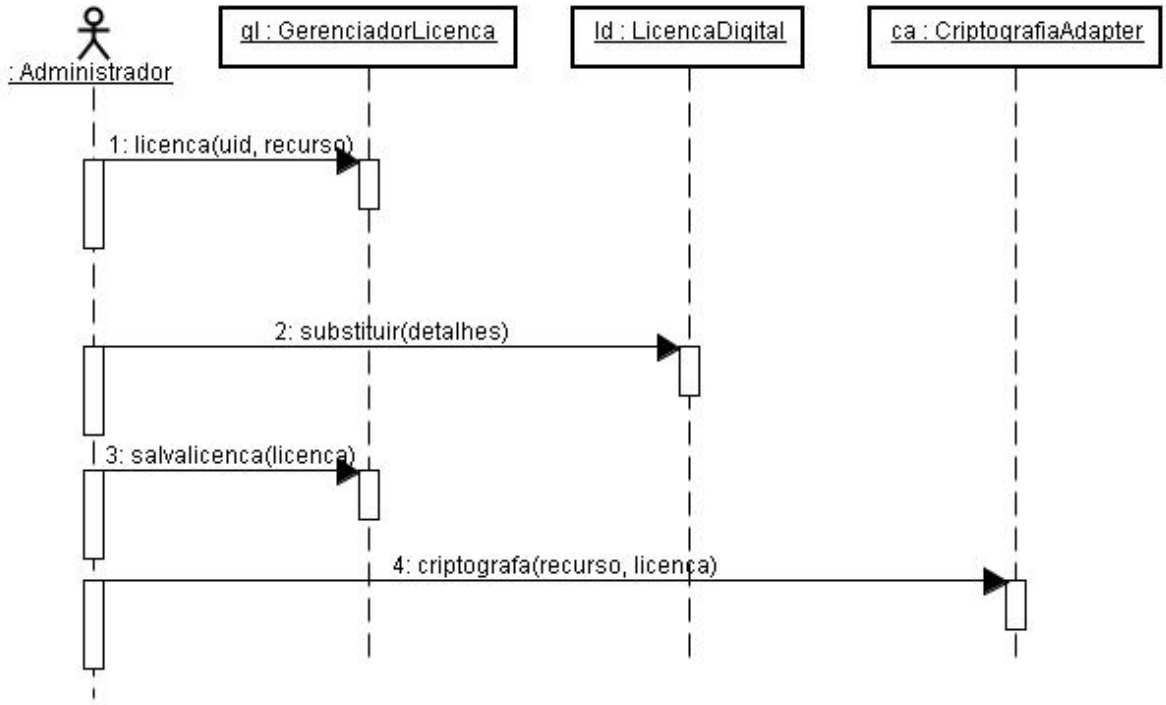


Figura 8.12 - Diagrama de seqüência para alteração de licença de acesso

A Figura 8.13 ilustra o processo de exclusão da licença de acesso. Esta funcionalidade atribui o status inativo à licença especificada.

O processo de checagem dos direitos autorais pode ser observado no diagrama da Figura 8.14. O usuário inicialmente requisita uma determinada atividade que envolve um dado recurso. Por exemplo, Paulo deseja executar um arquivo de música chamado musica.wav. Neste processo estão identificados o usuário Paulo, a ação executar e o recurso arquivo musica.wav. O manipulador de requisições passa esta requisição para o GerenciadorSeguranca que por sua vez a passa ao GerenciadorDRM. Internamente na aplicação, todas as operações associadas ao DRM estão vinculadas a uma ação definida na especificação REL utilizada.

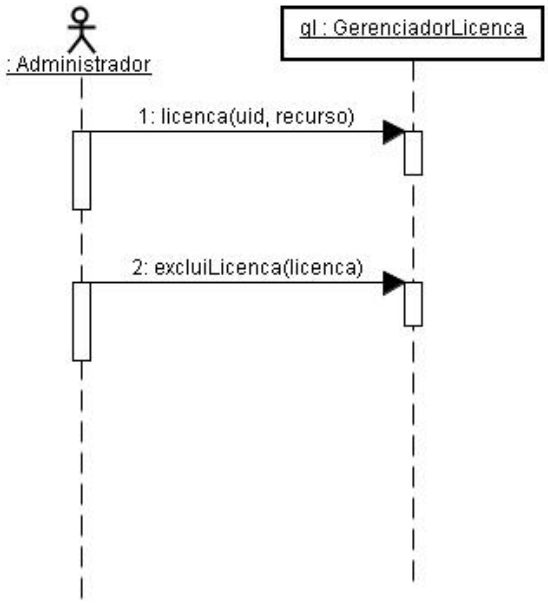


Figura 8.13 - Diagrama de seqüência para exclusão de licença de acesso

A licença requerida pelo usuário juntamente com o recurso a ser acessado são identificados resultando na validação da licença e na autorização de uso por parte do usuário. Caso não seja localizada a permissão para execução da ação requerida, uma exceção é levantada trazendo todos os detalhes referentes à tentativa mal sucedida de acesso.

O processo de inserção e o processo de detecção de marca d'água no conteúdo podem ser observados nos diagramas das Figuras 8.15 e 8.16 respectivamente.

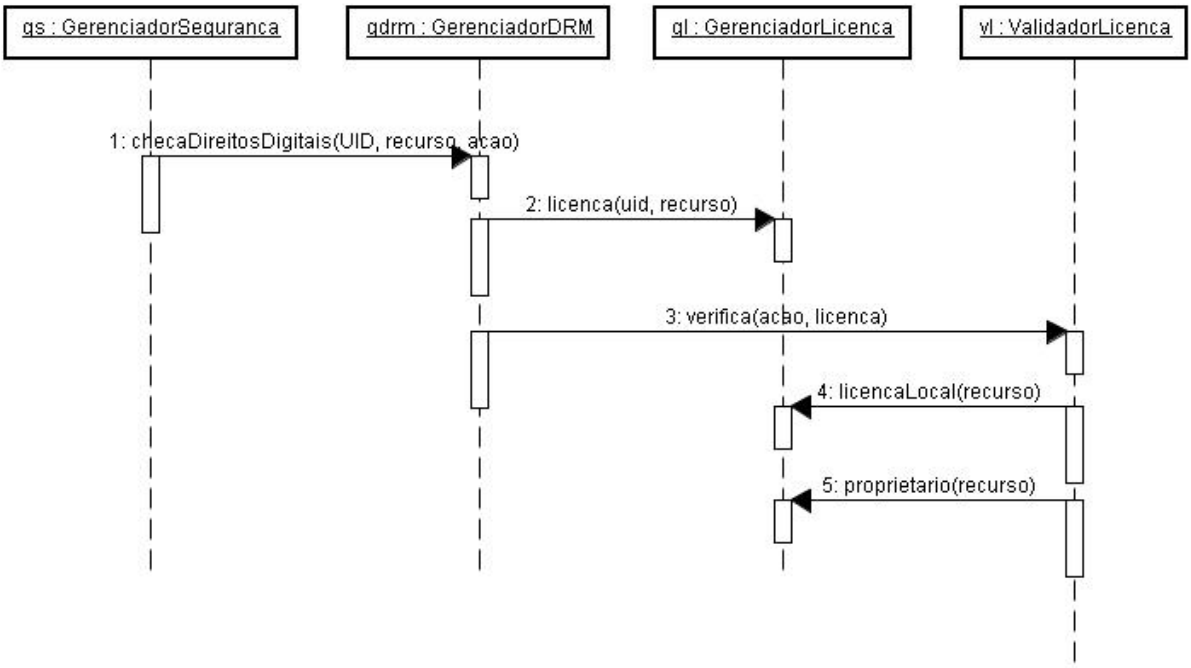


Figura 8.14 - Diagrama de seqüência para checagem dos direitos autorais de conteúdo digital

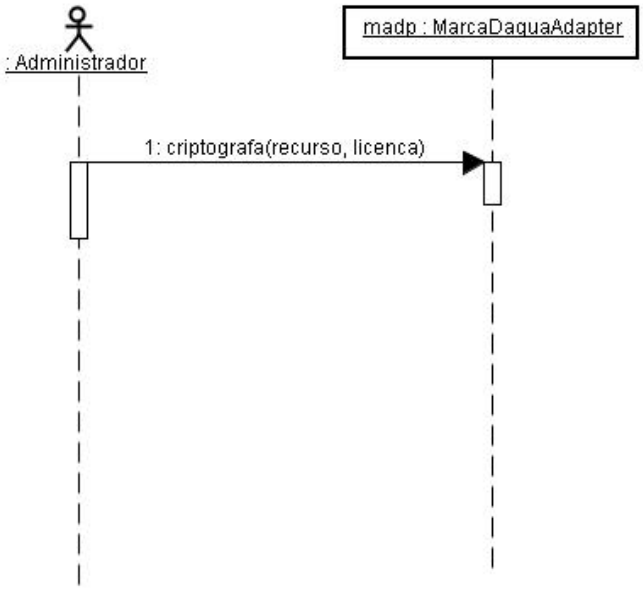


Figura 8.15 - Diagrama de seqüência da aplicação de marca d'água em conteúdo restrito

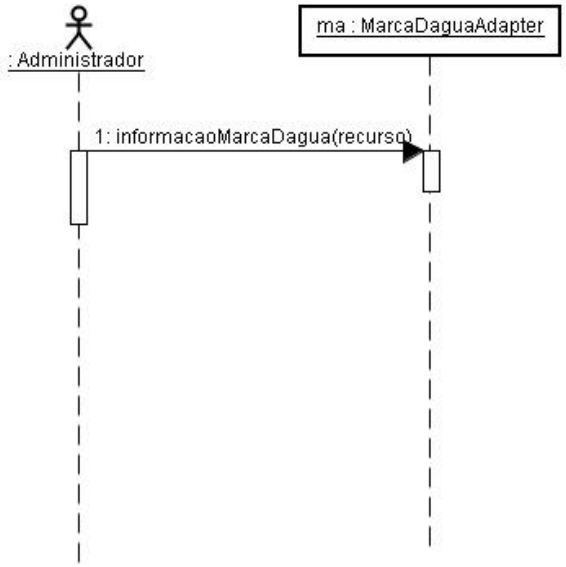


Figura 8.16 - Diagrama de seqüência da detecção de marca d'água em conteúdo restrito

9 - CONCLUSÃO

Na presente dissertação, buscou-se, inicialmente, caracterizar a arquitetura e os padrões de um sistema de TV Digital. Foi descrita a cadeia de valor da TV Digital, porém com ênfase na etapa de transmissão e nas tabelas SI onde constam descritores utilizados no processo de proteção contra acesso e cópia de conteúdos restritos.

A seguir foram descritos mecanismos de proteção de conteúdo, dentre os quais cabe destacar: Assinatura Digital, Marca D'água, Controle de Cópia, e Acesso Condicional. Dentro deste contexto, focalizou-se as principais técnicas relacionadas ao Gerenciamento de Direitos Digitais que são a inserção de marca d'água no conteúdo protegido a fim de anexar informações pertinentes às condições de acesso e a cifração do conteúdo, normalmente processada pelo sistema de acesso condicional, de forma a não permitir o acesso indevido sem que tais condições anteriormente citadas sejam satisfeitas.

O trabalho prossegue com discussão sobre diferentes padrões de metadados úteis não só no processo descritivo de condições de acesso de conteúdo restrito, mas também na descrição das informações do proprietário do conteúdo, dentre outros aspectos. Pôde-se observar que os metadados não se aplicam somente à área de *broadcast*, mas também no trato de conteúdo multimídia em geral e, devido ao fato de terem como base a linguagem XML, são extremamente escalonáveis e flexíveis, fato este devido à possibilidade de definição de novos descritores que abarquem necessidades que possam surgir no mercado de conteúdo digital.

Por fim, é apresentado sob o foco de engenharia de *software*, um modelamento de sistema de DRM em TV Digital, com base na metodologia do RUP. O sistema apresentado aborda os processos de autenticação, gerenciamento de usuários, tratamento de direitos autorais com geração dinâmica de licença de uso, contabilização financeira em tempo real e aquisição de autorização de acesso, uma vez satisfeitas as condições estabelecidas na licença de uso.

O trabalho realizado permitiu caracterizar a utilização de aspectos de segurança da informação necessários à proteção de conteúdo em diferentes etapas ao longo da cadeia de valor específica do sistema considerado.

Adicionalmente é possível sugerir novas técnicas a serem utilizadas em conjunto com aquilo que já vem sendo atualmente empregado, por exemplo, em relação à inserção de marcas d'água no conteúdo digital. Tais marcas d'água podem incluir outras

informações relevantes além das atualmente empregadas, como identificação unívoca do usuário que adquiriu direito de acesso de forma a permitir um rastreamento em caso de identificação de cópias suspeitas. Outra opção seria incluir na marca d'água a informação sobre o número de vezes que o conteúdo pode ser copiado de forma que a cada nova cópia, tal informação na marca d'água seja atualizada.

Apesar de todas as técnicas existentes no ramo de segurança de conteúdo digital restrito, existem áreas que demandam estudos aprofundados a fim de obter melhores soluções a serem empregadas neste contexto.

Trabalhos futuros podem ser sugeridos a partir das dificuldades existentes no processo de proteção de conteúdo. Alguns exemplos são citados a seguir: estudo de técnica de cifração de conteúdo de vídeo de forma escalonável, estudo de técnicas de criação de marcas d'água mais robustas a fim de intensificar a segurança das informações armazenadas na marca d'água em si, forma de tratar direitos digitais quando, numa rede heterogênea, estão envolvidos dispositivos não compatíveis com o sistema DRM proposto.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Sivaraman, Ganesh; Cesar, P.; Vuorimaa, P., *System Softwares for Digital Television Applications, Proceedings of the IEEE International Conference on Multimedia and Expo; Japan; 2001*.

[2] Instituto Brasileiro de Geografia e Estatística – IBGE. Disponível em http://www.ibge.gov.br. Acesso em: dezembro de 2007.

[3] Eskicioglu, A. M.; Town, J.; Delp, E. J., *Security of digital entertainment content from creation to consumption*, 2003.

[4] Fernandes, J.; Lemos, G; Elias, G. - Introdução à Televisão Digital Interativa: Arquitetura, Protocolos, Padrões e Práticas, 2004.

[5] Schwalb, Edward M., *iTV Handbook. Technologies and Standards*. Ed. Prentice Hall, 2004.

[6] Silva, J. Q.; Monografia; Universidade do Vale do Rio dos Sinos; 2003.

[7] ARIB STD-B10:2006 – *Service Information for ARIB TR-B14:2007, Operational guidelines for digital terrestrial television broadcasting*

[8] ISO/IEC 13818-1 "*Information technology – Generyc coding of moving pictures and associated audio information:Systems*", 2000.

[9] Projeto DIGITAL VIDEO BROADCASTING (DVB). Disponível em http://www.dvb.org. Acesso em: novembro de 2006.

[10] ADVANCED TELEVISION SYSTEMS COMMITEE (ATSC). Disponível em http://www.atsc.org, acessado última vez em novembro de 2006.

[11] INTEGRATED SERVICES DIGITAL BROADCASTING (ISDB). Disponível em http://www.arib.org.jp/english, acessado última vez em novembro de 2006.

[12] Morris, S.; Smith-Chaigneau, A., *Interactive TV Standards, A guide to MHP, OCAP, and Java TV*. EUA: Elsevier, 2005.

[13] Luo, J., *Home Network Application Security (MHP),* 2002.

[14] Disponível em http://www.mhp.org/html_index.html, acessado última vez em dezembro de 2006.

[15] GEM – Globally Executable MHP, *A Guide to Platform Harmonization*. Disponível em: http://www.mhp.org/mhp_technology/gem/wp05.platform%20harmonisation.final.pdf. Acesso em: maio de 2006.

[16] Revista Mundo Java, número 17, ano III, 2006.

[17] Leite, L. E. C., et al. FlexTV – Uma Proposta de Arquitetura de Middleware para o Sistema Brasileiro de TV Digital. In: Revista de Engenharia de Computação e Sistemas Digitais, v. 2, pp 29-50, 2005.

[18] Lugmayr, A.; Niiranen; S., Kalli, S., *Digital Interactive TV and Metadata.* Ed. Springer, 2004.

[19] Malik, Hafiz M. A., *Data Hiding Techniques for Digital Rights Management of Multimedia Archives*, Tese Doutorado – Departamento de Engenharia Elétrica e Computação, Universidade de Illinois - Chicago, 2006.

[20] Barni, M.; Bartolini, F., *Watermarking Systems Engineering*. Marcel Dekker, 2004.

[21] Lin, T. E.; Eskicioglu, A. M.; Lagendijk, R. L; Delp, E. J. – "*Advances in Digital Video Content Protection*", 2004.

[22] Wiley J., *Digital Rights Management: Business and Technology*, 2001.

[23] Wood, D., EUROPEAN BROADCAST UNION: *EBU TECHNICAL REVIEW No. 282*, Março 2000.

[24] Rosenblatt, B.; Trippe, W.; Mooney, S., *Digital Rights Management: Business and Technology*. Ed. M&T Books, 2001.

[25] Ishikawa, K., *DRM for digital broadcasting in Japan*, extraído de http://www.indicare.org/tiki-print_article.php?articleId=166 em outubro de 2006.

[26] ITU-R Rec. BT810: *Conditional-access broadcasting systems* (1992.9)

[27] ELECTRONICS INDUSTRIES ASSOCIATION. EIA-679-B, *National Renewable Security Standard*, parte B. Março 2000.

[28] ABNT/CEE-00:001.85, Projeto 00:001.85-005/1 – Televisão digital terrestre – Gerenciamento digital de direitos – Parte 1: Ferramentas de proteção da interface de saída, 2007.

[29] *Digital Transmission Content Protection Specification*, Volume 1, 2005.

[30] Équille, L. B., *Metadata definition and specification*, ENTHRONE Project, 2004.

[31] Berners-Lee, T. – *Metadata Architecture*, disponível em http://www.w3.org/DesignIssues/Metadata.html, acessado última vez em dezembro de 2007.

[32] *Oxford Digital Library*, disponível em http://www.odl.ox.ac.uk/metadata.htm, acessado última vez em dezembro de 2007.

[33] Worthington, T. – *Metadata: The killer application for digital broadcasting*, disponível em http://www.tomw.net.au/2002/mka.html, acessado última vez em dezembro de 2007.

[34] ISO MPEG-7, Part 5 - *Multimedia Description Schemes*, ISO/IEC JTC1/SC29/ WG11/N4242, 2001.

[35] ISO MPEG-21, Part 7 - *Digital Item Adaptation*, ISO/IEC JTC1/SC29/WG11/ N5231, 2002.

[36] TVA (1999) TV-Anytime Forum, disponível em http://www.tv-anytime.org, acessado última vez em dezembro de 2007.

[37] Manjunath, B. S.; Salembier, P.; Sikora, T – *Introduction to MPEG-7, Multimedia Content Description Interface*, Ed. Wiley, 2002.

[38] Magalhães, J. M. C. – *Universal Access to Multimedia Content Based on the MPEG-7 Standard*. Dissertação (Tese de Mestrado). Universidade Técnica de Lisboa, 2002.

[39] *MPEG-21 Multimedia Framework*, disponível em http://mpeg-21.itec.uni-klu.ac.at/cocoon/mpeg21/_mpeg21Parts.html, acessado última vez em dezembro de 2007.

[40] *MPEG-21 Overview* v.5 – disponível em http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm, acessado última vez em dezembro de 2007.

[41] TV–Anytime Fórum, disponível em http://www.tv-anytime.org, acessado última vez em dezembro de 2007.

[42] Evain, J. P.; Murret-Labarthe, H. – TV-Anytime Phase 1 – *A decisive milestone in open standards for Personal Video Recorders*, 2003.

[43] Alves, L. G. P.; Kulesza, R.; Silva, F. S. da; Jucá, P.; Bressan, G. – Análise Comparativa de Metadados em TV Digital, 2006.

[44] Relatório “Cadeia de Valor” – FUNTTEL - Projeto Brasileiro de Televisão Digital, OS40539, CPQD. Outubro de 2004.

[45] OpenTV, disponível em http://www.opentv.com, acessado última vez em dezembro de 2007.

[46] NDS, disponível em http://www.nds.com/solutions/mediahighway.html, acessado última vez em dezembro de 2007.

[47] Microsoft TV, disponível em http://www.microsoft.com/tv, acessado última vez em dezembro de 2007.

[48] ITU. “ITU-T Recommendation J.200: Worldwide common core – Application environment for digital interactive television services”, 2001.

[49] ITU. “ITU-T *Recommendation J.201: Harmonization of declarative content format for interactive television applications*”, 2004.

[50] ITU. “ITU-T *Recommendation J.202: Harmonization of procedural content formats for interactive TV applications*”, 2003.