

LAISA CAROLINE DE PAULA COSTA

**SEGURANÇA PARA O SISTEMA BRASILEIRO DE
TELEVISÃO DIGITAL: CONTRIBUIÇÕES À
PROTEÇÃO DE DIREITOS AUTORAIS E À
AUTENTICAÇÃO DE APLICATIVOS**

São Paulo

2009

LAISA CAROLINE DE PAULA COSTA

**SEGURANÇA PARA O SISTEMA BRASILEIRO DE
TELEVISÃO DIGITAL: CONTRIBUIÇÕES À
PROTEÇÃO DE DIREITOS AUTORAIS E À
AUTENTICAÇÃO DE APLICATIVOS**

Dissertação Apresentada à Escola
Politécnica da Universidade de São Paulo
para Obtenção do Título de Mestra em
Engenharia Elétrica

Área de concentração

Sistemas Eletrônicos

Orientador

Prof. Dr. Marcelo Knörich Zuffo

São Paulo

2009

Dedicatória

Dedico este trabalho aos meus pais:

Marina e Claudio

Agradecimentos

À minha família, especialmente aos meus pais que prestaram todo tipo de apoio e incentivo para garantir a conclusão deste trabalho.

Ao meu amigo e companheiro Luiz Fernando De Biase, que sempre me ouviu nos momentos mais difíceis.

Aos participantes do Fórum SBTVD, pelas inúmeras discussões e ensinamentos. Especialmente ao Prof. Volnys Bernal, Rodrigo Nascimento, Klaus Shenk, Rubert Kukla, e Maarten Muijen.

Aos meus amigos Gil Barros e Adilson Hira, pelas discussões e orientações na execução deste trabalho.

Ao Sr. Hilel Becher, gerente do Núcleo de Engenharia de Mídias do Laboratório de Sistemas Integráveis, por todo o apoio prestado a esta dissertação.

A todos os colegas com quem tive a oportunidade de trabalhar, que direta ou indiretamente me ajudaram na realização deste trabalho.

A todos os meus professores que contribuíram com a minha formação acadêmica.

Finalmente agradeço ao meu orientador Prof. Dr. Marcelo Zuffo, pelos seus ensinamentos, pelas frutíferas discussões, pelas oportunidades de interação com profissionais da área e pelas longas horas de revisão deste trabalho.

Financiamento

Este trabalho contou com o financiamento da Associação do Laboratório de Sistemas Integráveis Tecnológico (LSI-TEC) e da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) por meio da *Rede de Cooperação Universitária para Ensino Superior e Pesquisa Avançada em TV Digital e seus Cenários Interdisciplinares de Evolução*.

Resumo

O sistema de televisão é considerado o principal meio de comunicação e entretenimento no Brasil. Com o início das transmissões do sistema de televisão digital brasileiro no final de 2007, os principais impactos da digitalização do sistema de TV são: a alta definição de imagens e som, a mobilidade e a portabilidade. Com o tempo, outras funcionalidades serão incorporadas: a multiprogramação (mais de um programa no mesmo canal) e a interatividade. E é a partir da TV interativa que passa a ser possível o oferecimento de serviços para a população. Este trabalho tem como objetivo sistematizar as questões relacionadas com segurança no âmbito da televisão digital terrestre, além de propor e avaliar contribuições para uma arquitetura de segurança considerando o cenário expandido da televisão digital brasileira; especialmente no que tange a proteção de direitos autorais em TV aberta e a autenticação de aplicativos e serviços para TV interativa. A pesquisa realizada considera a realidade brasileira, suas necessidades específicas e as tecnologias disponíveis mais adequadas a elas, viabilizando o uso de serviços com alto valor agregado. Para atingir estes objetivos, foi realizado um amplo levantamento de tecnologias e sistemas existentes relacionados com o tema de segurança em TV digital. Com base neste levantamento, o trabalho apresenta uma sistematização da segurança para a televisão digital terrestre e aberta no Brasil na qual são identificados casos de uso e requisitos. É proposto o SPDA-BR, um sistema de proteção de direitos autorais adequado ao parque de televisores nacional e com menor impacto no custo de receptores; é proposto também o AUTV, um mecanismo de autenticação de aplicativos flexível (que possa ser utilizada para atualização de *software*, instalação de *drivers*, aplicativos interativos), compatível com padrões abertos e com a ICP Brasil. Esta dissertação forneceu subsídios para a escrita da norma de segurança para o Sistema Brasileiro de Televisão Digital, gerou publicações de artigos científicos e técnicos, e a comprovação de viabilidade, tanto do SPDA-BR como do AUTV, através de simulações e prova de conceito, respectivamente.

Palavras-chave: Televisão (Engenharia elétrica), Televisão digital, Televisão interativa, Segurança de redes, Segurança de software, Criptologia.

Abstract

In Brazil, the television system is considered an important source of communication and entertainment. The Brazilian digital transmissions started on December 2007 and first offered functionalities were the high definition, mobility and portability. In a later moment other functionalities will be added: multiprogramming (more than one service per channel) and interactivity. With the interactivity it is possible to offer digital services to the public. This work goals are to present a systematic DTV security issues overview, to propose and analyze DTV security issues contributions; specifically to the digital rights protection, considering free to air DTV, and the services and applications to interactive TV. This research considers the Brazillian requirements and identifies the most suitable technologies to these requirements, allowing high value services integration to the television system. In order to achieve these goals, it was done a wide state of the art research and the DTV security use cases identification and its requirements specification. The SPDA-BR and AUTV were proposed. The SPDA-BR is a digital rights protection system suitable to the Brazilian scenario with the minimum cost impact. The AUTV is a flexible authentication mechanism (that can be applied to software update, driver installation and interactive DTV applications), compatible to the open standards and to the Brazilian Public Key Cryptographic Infrastructure. This text contributed to the DTV Brazilian system, generated scientific and technical publications, and specified as well as proved the feasibility of both SPDA-BR and AUTV, through simulation and proof of concept, respectively.

Key-words: Television (Electrical Engineering), Digital television, Interactive television, Network security, Software security, Criptology.

Lista de Figuras

Figura 1. Exemplo simplificado de uma rede doméstica.....	19
Figura 2. Diagrama de blocos para um sistema de transmissão de TVD terrestre.....	38
Figura 3. Produção de conteúdo e a inserção do DRM. Fonte: Fernando ET AL (2008)	39
Figura 4. Arquitetura de software de receptores de televisão digital interativos.	43
Figura 5. Arquitetura do Receptor de Televisão Digital.....	45
Figura 6. Receptor não interativo.	47
Figura 7. Receptor interativo-local.	48
Figura 8. Receptor interativo-pleno.	48
Figura 9. Escopo do Soquete de Segurança	52
Figura 10. Estrutura de Feistel.....	58
Figura 11. Função F da Estrutura de Feistel	58
Figura 12. Rede de permutação e substituição.	59
Figura 13. Configurações do módulo de acesso condicional em receptores.....	61
Figura 14. Diagrama da CI.....	62
Figura 15. Exemplo de hierarquia lógica de chaves	64
Figura 16. Configuração de um sistema de acesso condicional.	70
Figura 17. Algoritmo Multi-2. Fonte: Ougi ET AL. (2006)	71
Figura 18. Geração de chaves expendida do Multi-2. Fonte: Ougi ET AL. (2006).....	72
Figura 19. Arquitetura do DReaM. Fonte: Fernando, Jacobs e Swaminathan (2008).....	74
Figura 20. Processo de atualização do FlexiCert. Fonte: Lakshminarayanan e Zhou (2003)..	80
Figura 21. Componentes no modelo de operação geral da IGP. Fonte: ITU-T X.509 (2005).	82
Figura 22. Modelo de delegação de privilégios. Fonte: ITU-T X.509 (2005)	82
Figura 23. Liberação de recurso. Fonte: Adaptado de ITU-T X.509 (2005)	83
Figura 24. Estrutura de certificação digital no Brasil. Fonte: Ribeiro (2008).....	87
Figura 25. Cálculo do valor de hash de diretórios.	92
Figura 26. Modelo centralizado de geração de EMMs.	112
Figura 27. Modelo descentralizado de geração de EMMs.....	113
Figura 28. Arquitetura do sistema embarcado.....	117
Figura 29. Decisão de processamento pelo módulo embarcado ou cartão criptográfico.....	120
Figura 30. Integração entre processamento embarcado ou no cartão criptográfico.	121
Figura 31. Estudo de caso: atualização do software residente de um receptor.	147

Figura 32. Estudo de caso: atualização do software residente de um receptor.	148
Figura 33. Estudo de caso: instalação de dispositivo externo.	150
Figura 34. Estudo de caso: execução local de aplicativo interativo.	153
Figura 35. Estudo de caso: execução local de aplicativo interativo com Terceiro.....	154
Figura 36. Organização de hierarquia lógica de chaves segundo modelo e fabricante.	162
Figura 37. Organização de hierarquia de chaves segundo modelo e fabricante – pior caso..	163
Figura 38 Organização de hierarquia de chaves segundo modelo e fabricante – melhor caso	164
Figura 39. Organização de hierarquia lógica de chaves segundo localidade.	165
Figura 40. Organização de hierarquia lógica de chaves segundo ordem de requisição.....	167
Figura 41. Funcionamento JCA/JCE.	172
Figura 42. Entradas e saídas do aplicativo Autenticador.	173
Figura 43. Interface gráfica do Aplicativo Autenticador.	174
Figura 44. Blocos internos do aplicativo Autenticador.....	175
Figura 45. Entradas e saídas do Verificador de Autenticação.	176
Figura 46. Interface gráfica do Verificador de Autenticação.....	177
Figura 47. Diagrama IDEF0 do Verificador de Autenticação.....	178
Figura 48. Cadeia de certificação para o caso de autenticação de driver.....	181
Figura 49. Cadeia de certificação para o caso de aplicativo interativo avançado.	181

Lista de Tabelas

Tabela 1. Quadro comparativo entre sistemas de TV Digital (recepção fixa)	40
Tabela 2. Classificação dos Requisitos de Segurança	50
Tabela 3. Padrões da ICP-Brasil. Fonte: ITI (2006).....	88
Tabela 4. Tabela comparativa entre tipos de certificados ICP-Brasil.....	90
Tabela 5. Sintaxe do arquivo de hash. Fonte: GEM (2008).....	93
Tabela 6. Interpretação do campo digest_type	93
Tabela 7. Diretivas para cálculo do hash	94
Tabela 8. Sintaxe dos arquivos de certificados de identidade no GEM. Fonte:GEM.	96
Tabela 9. Quadro comparativo: MULTI-2 x AES.....	115
Tabela 10. Interpretação do campo digest_type	128
Tabela 11. Medida de taxa disponível para as emissoras de TV no SBTVD.	160
Tabela 12. Custo de distribuição de mensagens EMM sem uso de hierarquia de chaves.	168
Tabela 13. Consumo de banda para diferentes estratégias de gerenciamento de receptores.	169
Tabela 14. Características técnicas de processadores para cartões criptográficos. Fonte: Yang (2001)	170
Tabela 15. Comparação de processamento do AES para modelos de cartões criptográficos. Fonte: Yang (2001)	171

Lista de Abreviaturas e Siglas

AA	Autoridade de Atributos
AAC	<i>Advanced Audio Coding</i>
AC3	<i>Arc Consistency algorithm #3</i>
AR	Autoridade de Registro
ASN.1	<i>Abstract Syntax Notation One</i>
AES	<i>Advanced Encryption Standard</i>
ABNT	Associação Brasileira de Normas Técnicas
AC	Autoridade de Certificação
API	<i>Application Programming Interface</i>
ATSC	<i>Advanced Television System Committee</i>
AUTV	Sistema de AUtenticação de aplicativos para TV digital
AVC	<i>Advanced Video Coding</i>
BML	<i>Broadcast Markup Language</i>
BST-COFDM	<i>Band Segmented Transmission – COFDM</i>
CAT	<i>Conditional Access Table</i>
CGMS-A	<i>Copy Generation Management System – Analog</i>
CMS	<i>Cryptographic Message Syntax</i>
CODEC	CODificador e DECodificador
COFDM	<i>Coded Orthogonal Frequency Division Multiplex</i>
DASE	<i>DTV Application Software Enviornment</i>
DES	<i>Data Encryption Standard</i>
3DES	<i>Triple DES</i>
CAS	<i>Conditional Access System</i>
Drivers	<i>device drivers, adaptadores de dispositivos</i>

DVD	<i>Digital Video Disc</i>
DMP	<i>Digital Media Project</i>
DTMB	<i>Digital Television Multimedia Broadcast</i>
DRM	<i>Digital Rights Management</i>
DSM CC	<i>Digital storage media command and control</i>
DTCP	<i>Digital Transmission Content Protection</i>
DVB	<i>Digital Video Broadcasting</i>
ECM	<i>Entitlement Control Message</i>
ES	<i>Elementary Stream</i>
EMM	<i>Entitlement Management Message</i>
EEPROM	<i>Electrically-Erasable Programmable Read-Only Memory</i>
FAPESP	Fundo de Amparo à Pesquisa do Estado de São Paulo
GEM	<i>Globally Executable MHP</i>
H.264	Parte 10 do MPEG-4 - mesmo que AVC
HE-AAC	<i>High Efficiency AAC</i>
HD	<i>High Definition</i>
HDTV	<i>High Definition Television</i>
HDCP	<i>High-bandwidth Digital Content Protection</i>
HDMI	<i>High-Definition Multimedia Interface</i>
ICP	Infraestrutura de Chaves Públicas
IDE	<i>Integrated Development Environment</i>
IDEF0	<i>Integration Definition for Function Modeling</i>
IEC	<i>International Electrotechnical Commission</i>
IGP	Infraestrutura de Gerenciamento de Privilégios
IP	<i>Internet Protocol</i>
ISDB	<i>Integrated Services Digital Broadcasting</i>

ISDB-T	<i>ISDB, Terrestrial Standard</i>
ISDB-T _B	<i>ISDB, Brazilian Terrestrial Standard</i>
ISO	<i>International Organization for Standardization</i>
JCE	<i>Java Cryptographic Extension</i>
JDK	<i>Java Development Kit</i>
JSA	<i>Java Security Architecture</i>
LCR	Lista de Certificados Revogados
LKH	<i>Logic Key Hierachy</i>
MDA	Memória de Dados Arbitrários
MHC	Memória de Hierarquia de Chaves
MCC	Memória de Chaves de Cifra
MD5	<i>Message-Digest algorithm 5</i>
MHP	<i>Multimedia Home Platform</i>
MMI	<i>Mother May I</i>
MPEG	<i>Moving Picture Experts Group</i>
MULTI-2	Algoritmo de criptografia proposto no ISDB
NCL	<i>Nested Context Language</i>
NIT	<i>Network Information Table</i>
NSA	<i>National Secutity Agency</i>
OAD	<i>On Air Download</i>
OCSP	<i>Online Certificate Status Protocol</i>
OID	<i>Object IDentifier</i>
PAT	<i>Program Allocation Table</i>
PAL	<i>Phase Alternating Line</i>
PID	<i>Packet Identifier</i>
PMT	<i>Program Map Table</i>

PSI	<i>Program and Service Information</i>
RCMM	<i>Revokated Certification Management Messages</i>
RFC	<i>Request For Comments</i>
RAM	<i>Random Access Memory</i>
ROM	<i>Read-Only Memory</i>
RSA	Nome de algoritmo criptográfico assimétrico
SBTVD	Sistema Brasileiro de Televisão Digital
SCMS	<i>Serial Copy Management System</i>
SD	<i>Standard Definition</i>
SDTV	<i>Standard Definition Television</i>
SHA	<i>Secure Hash Algorithm</i>
SO	Sistema Operacional
SOA	<i>Source of Authority</i>
SPDA-BR	Sistema de Proteção de Direitos Autorais Brasileiro
TDS-OFDM	<i>Time-Domain Synchronous OFDM</i>
TPM	<i>Trusted Plataform Module</i>
TS	<i>Transport Stream</i> – fluxo de transporte
TV	Televisão
TVD	Televisão Digital
UHF	<i>Ultra High Frequencies</i>
USB	<i>Universal Serial Bus</i>
VHF	<i>Very High Frequencies</i>
VSF	<i>Vestigial Side Band</i>
XML	<i>eXtensible Markup Language</i>
XrML	<i>eXtensible rights Markup Language</i>

Sumário

1	Introdução.....	17
1.1	Justificativa	20
1.2	Objetivos.....	22
1.3	Relevância.....	23
1.4	Trajectoria da pesquisa.....	24
1.5	Estrutura da dissertação	26
2	Segurança e televisão digital	28
2.1	Televisão Digital	28
2.1.1	Televisão no Brasil	28
2.1.2	Os padrões do grupo MPEG.....	30
2.1.3	Sistema de Televisão Digital.....	37
2.2	Estudos e análises do SBTVD fase I.....	49
2.3	Definição de Segurança da Informação.....	53
2.4	Proteção de direitos autorais	53
2.4.1	Legislação brasileira para proteção de direitos autorais	56
2.4.2	Fundamentação teórica para proteção de direitos autorais	57
2.4.3	Sistemas de proteção de direitos autorais	64
2.5	Autenticação de aplicativos	75
2.5.1	Ferramentas e mecanismos para a autenticação de aplicativos.....	75
2.5.2	Sistemas em uso para autenticação de aplicativos.....	86
2.6	Conclusão.....	98
3	Contribuições no sistema de segurança para o SBTVD.....	99
3.1	Sistematização da segurança para a TV terrestre brasileira.....	99
3.1.1	Proteção de direitos autorais: casos de uso e requisitos.....	100
3.1.2	Segurança em serviços: casos de uso e requisitos	103
3.2	Sistema de proteção de direitos autorais: SPDA-BR	106
3.2.1	Linguagem de direitos.....	107
3.2.2	Licenças de uso.....	109
3.2.3	Esquema de proteção do conteúdo	114
3.3	Segurança em serviços.....	122
3.3.1	Autenticação de aplicativos para TV digital: AUTV.....	123

3.3.2	O sistema AUTV aplicado a casos de uso	146
3.4	Conclusão.....	155
4	Viabilidade Funcional do AUTV e Análise de Eficiência do SPDA-BR	158
4.1	Análise de eficiência do SPDA-BR.....	158
4.1.1	Estratégias de distribuição de chaves.....	161
4.1.2	Análise de desempenho para o uso de cartões criptográficos	169
4.2	Viabilidade Funcional do AUTV	171
4.2.1	O aplicativo Autenticador	173
4.2.2	O aplicativo Verificador de Autenticação.....	176
4.2.3	Exercitando casos de uso sobre o AUTV.....	179
4.3	Conclusão da análise de viabilidade dos sistemas AUTV e SPDA-BR	181
5	Conclusão	183
5.1	Resultados, contribuições e impactos.....	184
5.1.1	Resultados do sistema de proteção de direitos autorais: SPDA-BR.....	184
5.1.2	Resultados do sistema de autenticação de aplicativos AUTV	188
5.1.3	Impactos no Sistema Brasileiro de TV Digital.....	191
5.1.4	Contribuições da dissertação	192
5.2	Trabalhos futuros.....	194
5.2.1	Modelo de gerenciamento da IGP para TV Digital	194
5.2.2	Contribuição com as especificações do <i>middleware</i> do SBTVD.....	194
5.2.3	Teste e aplicação do sistema AUTV em dispositivos embarcados	195
5.2.4	Segurança para a integração de redes diversas.....	195
5.2.5	Mecanismo de identificação de uso justo de conteúdo multimídia.....	195
5.2.6	Mecanismo de alteração dos direitos do conteúdo	196
5.3	Considerações finais	196

1 Introdução

A televisão digital já é realidade em muitos países no mundo. Segundo Zuffo ET AL (2007) existem três padrões consolidados e em uso: DVB (*Digital Video Broadcasting*), ATSC (*Advanced Television Systems Committee*) e ISDB (*Integrated Services Digital Broadcasting*). Adicionalmente, o sistema DTMB (*Digital Terrestrial Multimedia Broadcast*) foi criado e está em uso atualmente na China.

A televisão digital terrestre e aberta no Brasil é denominada SBTVD (Sistema Brasileiro de Televisão Digital). O SBTVD teve suas transmissões oficiais iniciadas em dezembro de 2007 e utiliza as especificações do ISDB-T_B (*ISDB Brazilian Terrestrial Standard*), um sistema novo, que foi desenvolvido em conjunto por diversos setores brasileiros como uma melhoria ao sistema-base, o ISDB-T (*ISDB Terrestrial Standard*).

No Brasil, o tema televisão digital é muito importante devido à capilaridade do sistema de televisão atual. A TV (televisão) analógica é considerada o principal meio de comunicação e entretenimento da população brasileira. São mais de 50 milhões de aparelhos presentes em cerca de 90% dos domicílios do país. Por isso, a digitalização do sistema de TV deve manter a sua universalização, além de trazer os benefícios do digital.

A transmissão digital do sinal de TV traz melhor qualidade de som e imagem, capacidade de mobilidade, além de melhor eficiência espectral. O sistema digital permite ainda a transmissão de dados codificados junto ao conteúdo áudio-visual, o que viabiliza o envio de programas de computadores pelo sistema de radiodifusão. Os programas de computador associados à programação da TV trazem um novo paradigma, a TV interativa.

A televisão digital poderá ser utilizada para entretenimento ou serviços, cada qual com necessidades específicas de segurança. Como entretenimento considera-se principalmente o tráfego de conteúdo multimídia com alta qualidade, com requisitos de segurança relacionados à garantia de qualidade de serviço e com questões de proteção de direitos autorais. Já em relação a serviços, considera-se a possibilidade de efetuar transações bancárias, acessar serviços de governo, saúde e educação. Para uso em serviços a necessidade de segurança é mais complexa, estando relacionada a sigilo, privacidade, autenticidade (integridade dos dados e identidade das entidades em interação) e não repúdio.

Os benefícios da televisão digital agregam mais valor para a sociedade brasileira do que em outros países, como nos Estados Unidos ou europeus. A qualidade do sinal da televisão analógica aberta está sujeita a interferências, resultando em piora da qualidade de imagem, gerando chuviscos e fantasmas. Como no Brasil a televisão é majoritária e universal, a melhoria do sinal de TV tem um alto valor percebido para a população. A possibilidade de oferecimento de serviços pela TV interativa também é muito atrativa na sociedade brasileira, considerando que apenas uma pequena parcela da população possui acesso a serviços digitais em suas residências.

Além da grande transformação da radiodifusão com a digitalização do sistema, esta área está passando por uma segunda revolução, a da convergência dos meios de comunicações e dispositivos de consumo. O crescente avanço das tecnologias de redes de computadores e do poder de processamento e armazenamento dos dispositivos eletrônicos, além das técnicas em processamento digital de sinais, está possibilitando o acesso à informação e a conteúdos em qualquer momento e lugar.

Com alto poder de processamento, tamanho reduzido e capacidade de comunicação, inclusive sem fio, os dispositivos eletrônicos passam a permear o dia a dia das pessoas com muito mais naturalidade. Este tipo de computação é denominado de computação ubíqua. Desta forma, as redes domésticas passam a abrigar uma série de dispositivos distintos em relação a poder de processamento e de comunicação.

Estas redes domésticas heterogêneas poderiam ainda possibilitar o compartilhamento de recursos tanto para processamento como para armazenamento de dados e comunicação. Atualmente, os serviços acessados são dependentes dos dispositivos, não podendo ser compartilhados. Por outro lado, o usuário almeja acessar os seus serviços de maneira simples e transparente, com independência do dispositivo ou da rede que está acessando.

Em um esforço de sistematização das redes convergentes – a saber: redes domésticas, redes de comunicação e de radiodifusão – é proposta neste trabalho a caracterização dos seus dispositivos em termos das seguintes funcionalidades: armazenamento (*media center*), portal (*gateway*), roteador (*router*) e transcodificação (*transcoder*). Por armazenamento entende-se a funcionalidade de manter conteúdo para compartilhamento com os demais elementos da rede. Os dispositivos com a funcionalidade de portal são utilizados como ponto de acesso para toda rede doméstica a uma rede externa, como, por exemplo, a rede de televisão digital terrestre, a rede mundial de computadores, dentre outras. Já a funcionalidade de roteador permite a conexão entre dispositivos da rede que não conseguem comunicar-se diretamente, atuando

como ponte. Já a funcionalidade de transcodificação pode ser utilizada para adaptar o conteúdo para a leitura por um elemento específico.

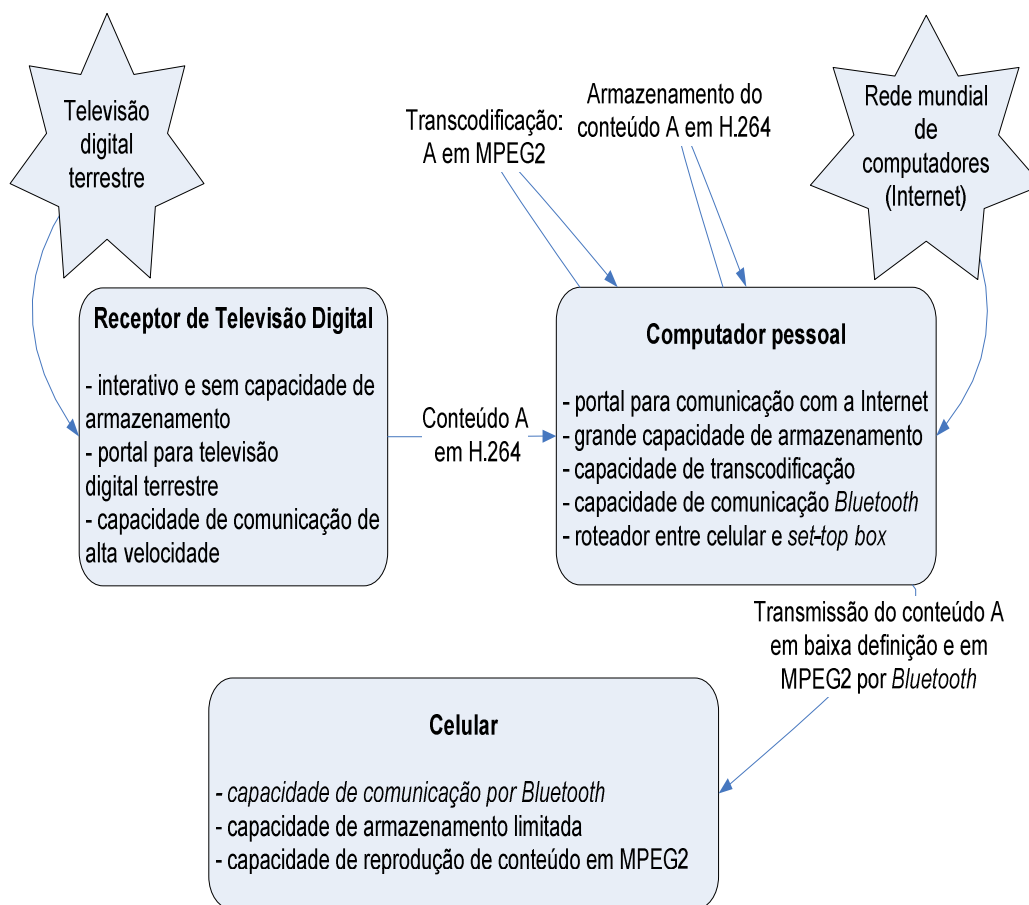


Figura 1. Exemplo simplificado de uma rede doméstica.

A Figura 1 apresenta um exemplo de arquitetura doméstica simplificada, nesta figura são apresentadas tecnologias H.264, MPEG-2 e *Bluetooth*, que serão discutidas posteriormente. Nela são apresentados três dispositivos, um receptor de televisão digital, um computador pessoal e um celular. O exemplo trata do acesso do celular a um conteúdo recebido da rede de televisão digital terrestre. Como o celular não possui um meio de comunicação direto com o receptor de televisão digital, e tampouco possui capacidade de decodificação do mesmo formato, o computador pessoal é utilizado como ponte entre ambos, processando (transcodificação) e repassando o conteúdo. Segundo este exemplo, para repassar o conteúdo, é alterada a tecnologia de rede para *Bluetooth*, possuindo o computador pessoal também o papel de roteador.

No cenário convergente, as questões de segurança passam a ter novos desafios, como a

identificação dos limites do ambiente doméstico e os seus indivíduos. Para alguns serviços, é importante que este sistema diferencie cada indivíduo e controle o acesso a esta rede de acordo com a sua identidade.

O trabalho aqui apresentado tem como contexto a primeira revolução citada, da digitalização do sistema de televisão, no âmbito do SBTVD. Fazendo um paralelo com o cenário convergente, o dispositivo de recepção do SBTVD seria caracterizado como o portal para a televisão digital terrestre e aberta. Neste trabalho serão abordados os aspectos de segurança aplicados ao SBTVD, levando-se em consideração as necessidades de escalabilidade da arquitetura de segurança para a sua evolução para o contexto da rede doméstica convergente e ubíqua.

1.1 Justificativa

O sistema de televisão digital cria demandas de segurança, praticamente inexistentes no sistema analógico. Estas demandas advêm de duas quebras de paradigma do sistema digital, são elas: a interatividade e a grande melhoria de qualidade de som e imagem. A interatividade possibilita o oferecimento de serviços, criando demanda de segurança para autenticação, sigilo e confidencialidade. A disponibilização de som e imagem com alta qualidade cria demanda a um sistema de proteção de direitos autorais.

O SBTVD considera o oferecimento de serviços interativos aos usuários, o que denominaremos como cenário expandido de televisão digital. Estes serviços podem ter caráter puramente de entretenimento e informação, podem aproveitar o potencial de anúncios em ambiente interativo, passando a competir com a Internet, ou oferecer serviços de utilidade pública.

Estes serviços interativos são importantes por: contribuir com a promoção da inclusão digital, possibilitarem a redução de custos tanto para acesso como para o oferecimento de serviços e por ser uma forma de atendimento às demandas emergentes da convergência digital.

A promoção da inclusão digital se dá pela massificação do acesso a serviços pela

televisão digital. É de conhecimento comum a disponibilidade de televisores em praticamente todos os lares brasileiros, ao mesmo tempo em que a quantidade de computadores com acesso à *Internet* é reduzida. O desenvolvimento do SBTVD considerou como premissa a possibilidade de acesso aos serviços pela tecnologia de TVD.

A redução de custos deve-se ao fato de que o uso de meios de comunicação eletrônica traz economia de recursos tanto com a diminuição do tempo gasto para acesso a estes serviços pelos usuários finais, como com a economia de investimento para oferecer o serviço. Segundo um estudo realizado pela empresa de consultoria Booz-Allen&Hamilton a economia em custo de uma transação financeira realizada via *Internet banking* quando comparada com a mesma transação realizada via agência bancária é de quase uma ordem de grandeza (10 vezes), e praticamente cinco vezes em relação ao *Home Banking* tradicional (redes telefônicas) (obtido de apresentação)¹. Estes dados podem ser extrapolados para outros serviços além dos bancários, mostrando o potencial de redução de custos pelo oferecimento de serviços pela TVD.

Já considerando as demandas da convergência digital, nota-se a crescente demanda por serviços acessíveis em diversos dispositivos eletrônicos pessoais, como exemplo pode ser citado o uso de aparelhos telefônicos e computadores pessoais; ambos utilizados tanto para reprodução de músicas como para realização de transações eletrônicas.

A questão da garantia dos direitos autorais em ambiente digital traz atualmente uma ampla discussão. As perdas causadas devido ao uso de cópias indevidas no Brasil em 2008 estão estimadas em US\$ 130 milhões, valor que corresponde a 35% do mercado legal, segundo União Brasileira de Vídeo (2008). Com a possibilidade advinda da *Internet* de divulgação de conteúdo de maneira anônima, associada à digitalização de conteúdos, passa a ser possível a reprodução, ilimitada, sem perdas em relação ao material original, tornando o uso de cópias indevidas um sério problema para a indústria fonográfica e cinematográfica contemporânea. Desta maneira surgem ferramentas para tentar inibir o uso de cópias indevidas do conteúdo digital submetendo-o às regras determinadas em cada país e para cada tipo de mídia.

A questão dos direitos autorais gera muitas discussões no Brasil, como pôde ser

¹ Informações obtidas em apresentação realizada por Paulo Barreto em 2006 na disciplina PCS5734 oferecida pelo programa de mestrado da Escola Politécnica da USP.

avaliado nas participações no Fórum SBTVD². Apesar das fortes pressões das emissoras de televisão para a adoção de técnicas avançadas para controle de cópias do conteúdo por elas distribuído, existem resistências por parte dos fabricantes de receptores de TV, devido ao aumento de custo de desenvolvimento e de preço dos produtos ao consumidor final. Outros setores governamentais também se posicionam contrariamente à adoção de mecanismos de controle de cópias, com o entendimento de que por o sinal de TV digital terrestre no Brasil ser aberto, não deve possuir nenhum mecanismo de restrição de uso. Não há consenso jurídico³ nesta questão, faltando leis claras e atualizadas para o cenário de TV digital. As principais motivações apresentadas pelas emissoras para a utilização de mecanismos de controle de cópias do conteúdo são as exigências de produtoras internacionais para a exportação de conteúdos de alto valor e a proteção de produção própria para exportação ou geração de DVD.

1.2 Objetivos

Este trabalho tem como objetivo investigar e desenvolver as questões de segurança no âmbito da televisão digital terrestre e aberta brasileira, sistematizando os requisitos de segurança para o cenário expandido da televisão digital. Como cenário expandido considera-se o uso da TV digital não somente para entretenimento, mas também para o oferecimento de serviços interativos aos seus usuários. Este cenário expandido estabelece várias necessidades de segurança, especificamente serão apresentadas contribuições à questão de proteção de direitos autorais e autenticação de aplicativos interativos.

São objetivos específicos desta dissertação:

- Investigar e apresentar os fundamentos teóricos e o estado da arte de segurança aplicada à televisão digital;

²A autora e seu orientador participam do Fórum SBTVD, do qual fazem parte representantes dos radiodifusores, governo, fabricantes de equipamentos para televisão e desenvolvedores de software para televisão digital.

³ A autora e seu orientador participaram de debate na Ordem dos Advogados do Brasil com a Comissão de Propriedade Imaterial, com o tema “Proposta de Segurança no Sistema Brasileiro de TV Digital” em 7 de novembro de 2007.

- Sistematizar as questões de segurança para os cenários de televisão digital para proteção de direitos autorais e uso de serviços;
- Propor um mecanismo para autenticação de aplicativos para o cenário de TV digital que seja adequado à infraestrutura brasileira;
- Propor um mecanismo para proteção de direitos autorais para TV aberta baseado em tecnologia de acesso condicional flexível e escalável;
- Apresentar evidências da viabilidade funcional e avaliar a eficiência das contribuições propostas por meio de prova de conceito.

1.3 Relevância

O uso de técnicas e mecanismos de segurança de acordo com as propostas deste trabalho permite o uso da televisão digital de uma maneira ampla, incentivando conteúdos de alto valor agregado e o oferecimento de serviços para a população.

Quando garantido o direito dos autores de recolher os ganhos com as suas obras, o conteúdo disponibilizado na TV terá aumento de valor. Por isso, há uma grande preocupação com as questões de proteção de direitos autorais na digitalização do sistema. Alguns estúdios e distribuidores de conteúdo áudio-visual condicionam a liberação de conteúdos em alta definição à comprovação de um sistema eficaz de gerenciamento de direitos digitais⁴. Esta preocupação com os direitos autorais é maior no Brasil justamente pela importância da TV aberta, ao contrário da maioria dos outros países que possuem uma televisão aberta marginalizada quando comparada à televisão paga. Por outro lado, a produção de conteúdo nacional também é afetada, pois uma vez apresentado o conteúdo em território nacional, se copiado e distribuído indevidamente, ele terá o seu valor de exportação reduzido.

Em relação ao oferecimento de serviços, este trabalho propõe a utilização de forma

⁴ Informação obtida durante as reuniões do Fórum SBTVD dos representantes da SET (Sociedade dos Engenheiros de Televisão)

segura de serviços interativos por meio da televisão digital. Uma contribuição importante é a realização da autenticação de aplicativos interativos utilizando a infraestrutura brasileira existente, pois os sistemas atuais fazem uso de uma infraestrutura de chaves públicas própria. Como o Brasil possui uma infraestrutura de chaves públicas com validade jurídica já estabelecida, é importante que a arquitetura de segurança seja proposta de maneira a aproveitá-la.

Um grande diferencial deste trabalho frente aos sistemas de segurança disponíveis atualmente para televisão digital é a sua adequação à realidade brasileira, considerando as necessidades do país e as tecnologias disponíveis mais adequadas a elas. Considerando a adoção tardia em relação aos demais países e o grande mercado em televisão, há abertura para propostas que sejam mais avançadas e se adéquem melhor às necessidades locais.

1.4 Trajetória da pesquisa

A autora iniciou seu trabalho na área de pesquisa e desenvolvimento para televisão digital com o projeto de iniciação científica apoiado pela FAPESP denominado: Pesquisa e Desenvolvimento de Uma Unidade Controladora de Vídeo, nos anos de 2003 e 2004. Neste trabalho foi desenvolvida, em FPGA (*Field Programmable Gate Array*), uma unidade para controle de memória de vídeo e sincronismo com televisor para um *set-top box* digital e reconfigurável, com foco em baixo custo.

Em 2005, durante a fase de pesquisa e desenvolvimento do projeto SBTVD, instituído pelo Decreto 4.901 (BRASIL, 2003), a autora participou do projeto do Terminal de Acesso de Referência do Sistema Brasileiro de Televisão Digital, onde contribuiu com a gestão de requisitos e coordenação técnica do projeto. Este trabalho considerou pontos importantes do receptor de televisão digital, inclusive tratando alguns elementos de segurança (focado principalmente no canal de retorno).

Em 2007, a autora participou do projeto Sistema de Recepção de Conteúdo para Cinema Digital, contribuindo com a especificação e análise de sistemas. Este projeto desenvolveu um sistema de cinema digital para recebimento de conteúdo no complexo de

cinema, com automatização da sala de projeções, sistema de geração de relatórios e distribuição de conteúdo entre as salas do complexo. O projeto considerou também importantes aspectos de segurança no que se refere ao gerenciamento de direitos digitais, sigilo de dados trafegados e autenticação de usuário.

Concomitantemente ao trabalho aqui apresentado, a autora contribui com o Fórum de especificações do SBTVD. Os grupos técnicos dos quais a autora participa são os que versam sobre Segurança, Receptores e Multiplexação. As contribuições apresentadas nesta dissertação foram disponibilizadas para o grupo de segurança do Fórum SBTVD. As contribuições no que tange a proteção de direitos autorais foram utilizadas como base para a decisão de adotar apenas a proteção contra cópias sem a criptografia do sinal. As contribuições para a autenticação de aplicativos estão sendo consideradas para adoção no padrão. As contribuições no fórum foram realizadas entre os anos de 2007 e 2009.

Além destes trabalhos desenvolvidos pela autora, é importante citar os trabalhos desenvolvidos no mesmo grupo de pesquisa, o Núcleo de Engenharia de Mídias. Estão em andamento trabalhos nas áreas de codificação escalável, sistemas de arquivos para análise conformidade de *transport stream* e sistemas autônomos de redes sem fio. Publicados:

- DALPOZ, M. A. S. **Um Terminal de Acesso Digital Reconfigurável Bidirecional Adaptável aos Padrões Multimídia Emergentes**. 2005. 195 p. Tese de Doutorado – Escola Politécnica, Universidade de São Paulo, São Paulo, 2005.
- BARROS, G. G. de. **A consistência da interface com o usuário para a TV interativa**. São Paulo, 2006. p. 200 Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.
- VAZ, R. A., **Uma Interface de Comunicação Sem Fio em TV Digital Baseada em Rádio Definido por Programa de Computador**. São Paulo, 2007. p. 200 Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.
- CARVALHO, E. R., **Uma Plataforma Modular Para Testes Com Interatividade Na TV Digital Brasileira**. São Paulo, 2008. p. 119. Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.
- HIRA, C. **Arquimedia: Uma Proposta de Arquitetura de Software para**

Terminais de Acesso à TV Digital Interativa. São Paulo, 2008. p. 133. Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.

1.5 Estrutura da dissertação

Esta dissertação possui cinco capítulos, são eles:

- Capítulo 1: Introdução – apresenta contexto, justificativa, objetivos, relevância, trajetória da pesquisa e a estrutura do texto.
- Capítulo 2: Segurança e televisão digital – este capítulo tem como objetivo investigar as questões de segurança em televisão digital. São apresentadas as fundamentações teóricas sobre televisão digital e segurança, incluindo soluções, métodos e técnicas importantes atualmente propostos e aplicados neste contexto. Apresenta também o estado da arte no tema.
- Capítulo 3: Contribuições no sistema de segurança para o SBTVD – apresenta a sistematização das questões de segurança para a televisão digital e contribuições para o sistema de segurança do SBTVD. Na sistematização do tema segurança na TV digital, são apresentados o levantamento dos cenários de uso e os seus principais requisitos. Foram definidas duas áreas para o escopo do trabalho: proteção de direitos autorais e autenticação de aplicativos. Para cada área foi criada uma subseção com a apresentação de proposta.
- Capítulo 4: Viabilidade funcional do AUTV e análise de eficiência do SPDA-BR – este capítulo apresenta a descrição dos experimentos e simulações teóricas realizados para testar a viabilidade funcional e eficiência das principais contribuições apresentadas. O SPDA-BR foi avaliado teoricamente para medida de consumo de banda e de desempenho em cartões criptográficos e o AUTV foi testado por meio da prototipagem de aplicações para prova de conceito.
- Capítulo 5: Conclusão – este capítulo apresenta os resultados obtidos com a

experimentação descrita no capítulo 4 e apresenta a análise destes resultados, elencando as principais contribuições e impactos do trabalho. Além disso, são apresentados alguns possíveis trabalhos futuros e os comentários finais da dissertação.

2 Segurança e televisão digital

O objetivo deste capítulo é investigar as questões de segurança em televisão digital, bem como apresentar soluções, métodos e técnicas relevantes e atualmente propostas e aplicadas neste contexto. Este capítulo vai fornecer os subsídios necessários para a proposta do AUTV e do SPDA-BR que serão apresentadas posteriormente.

Primeiramente são apresentados os fundamentos sobre televisão digital, posteriormente é apresentada uma definição de segurança e seus requisitos. Em seguida são apresentados os resultados na área de segurança do projeto SBTVD fase de pesquisa e desenvolvimento. Finalmente são apresentados os fundamentos teóricos e o estado da arte para as duas áreas de interesse deste trabalho: proteção de direitos autorais e autenticação de aplicativos.

2.1 Televisão Digital

Este item está subdividido em três seções. A primeira, Televisão no Brasil, apresenta o histórico da adoção da televisão digital no Brasil. A segunda seção apresenta os padrões do grupo MPEG com maior sinergia aos temas abordados por este trabalho. Finalmente a terceira seção apresenta os fundamentos sobre televisão digital, detalhando os mecanismos de transmissão e recepção.

2.1.1 Televisão no Brasil

A TV analógica no Brasil é considerada o principal meio de comunicação e

entretenimento da população. Segundo o IBGE, são mais de 50 milhões de aparelhos presentes em aproximadamente 90% dos domicílios do país. Por isso, as discussões para a digitalização do sistema de TV têm sido muito intensas e têm envolvido diversos setores da sociedade.

Ao longo da década de 1990 foram constituídos os primeiros grupos de trabalho em TV digital no Brasil. Em 2000, o grupo SET-ABERT foi constituído para a realização de testes comparativos entre os padrões DVB, ATSC e ISDB.

Em 26 de Novembro de 2003 é publicado o Decreto nº 4.901 (BRASIL, 2003) que instituiu o Projeto do Sistema Brasileiro de Televisão Digital (SBTVD). Através de chamadas públicas⁵, foram formados 22 consórcios constituídos por instituições de ensino e de pesquisa com o objetivo de estabelecer o modelo de referência a ser adotado para a TV Digital no Brasil. Cada consórcio foi responsável por uma parte do sistema, cabendo-lhe a tarefa de levantar os requisitos, alternativas e impactos das soluções tecnológicas. Ao final do projeto, cada consórcio apresentou uma recomendação para o seu objeto de estudo, acompanhada por um relatório técnico e protótipos utilizados para demonstração e prova de conceito.

Com os resultados de todos os consórcios do SBTVD chegou-se à proposição de um modelo de sistema de TV Digital para ser adotado no Brasil. Tendo por base este modelo, houve um intenso debate e após seis meses foi assinado o Decreto 5.820, de 29 de junho de 2006 (BRASIL, 2006), que instituiu o SBTVD tendo como base, o padrão de transmissão de sinais do ISDB-T, incorporando as inovações tecnológicas aprovadas pelo Comitê Interministerial de Desenvolvimento de que trata o Decreto nº 4.901, de 26 de novembro de 2003. O Decreto estabeleceu também a transmissão do sinal digital em alta definição (HDTV) e em definição padrão (SDTV); transmissão digital simultânea para recepção fixa, móvel e portátil e a interatividade.

Após a publicação do Decreto 5.820, foi criado o Fórum do Sistema Brasileiro de TV Digital Terrestre, com o objetivo de tratar as questões de implantação para o sistema de TV digital do Brasil, incluindo a elaboração das normas técnicas e aspectos de propriedade intelectual, divulgação do sistema, tarifas incidentes, dentre outros pontos.

No começo de 2007 ocorreram as primeiras transmissões de TV Digital em alta definição no padrão SBTVD em caráter experimental em São Paulo, pelas próprias emissoras.

⁵ As chamadas e os ganhadores podem ser vistos no site <http://sbtvd.cpqd.com.br/?obj=historico&mtd=texto&item=5> Último acesso em 25/07/2007.

No dia 30 de Novembro de 2007, a ABNT publicou oficialmente as normas essenciais referentes ao Sistema Brasileiro de TV Digital⁶, restando algumas em fase de conclusão e consulta pública. Com a publicação destas normas essenciais, houve o lançamento oficial da TV Digital no Brasil no dia 2 de Dezembro de 2007, na cidade de São Paulo.

2.1.2 Os padrões do grupo MPEG

O grupo MPEG (*Moving Pictures Experts Group*), que faz parte da ISO/IEC, é responsável pelo desenvolvimento de padrões internacionais para compressão, descompressão, processamento e representação codificada de áudio, vídeo e suas combinações. Estes padrões são extremamente relevantes para os sistemas de televisão digital, pois são amplamente empregados.

Os padrões MPEG atualmente publicados são: MPEG-1, MPEG-2, MPEG-4, MPEG-7 e MPEG-21. Os padrões MPEG A, B, C, D e E estão em processo de desenvolvimento.

O MPEG-1 é utilizado para codificação de filmes em CD (*Compact Disc*), com baixa qualidade e o MPEG-2 é utilizado em TV digital de alta qualidade. O principal avanço do MPEG-4 em relação aos seus antecessores, além da maior capacidade de compressão, é a maior interatividade permitida ao usuário, com as cenas representadas através de objetos audiovisuais, já o AVC (*Advanced Video Coding*) é a parte 10 das especificações do MPEG-4 e consiste em um padrão de codificação com aproximadamente o dobro de capacidade de compressão do que o MPEG-2 vídeo. O MPEG-7 é um sistema de descrição de conteúdo que visa permitir acesso eficiente a conteúdo multimídia. O MPEG-21 define um arcabouço multimídia que possibilita o uso transparente e ampliado dos recursos multimídia por uma ampla gama de redes e dispositivos.

Em adição a estes padrões mais consolidados, o MPEG iniciou uma nova linha de padrões: MPEG-A "Formato de aplicação multimídia", provê uma especificação para a integração dos padrões MPEG. MPEG-B, MPEG-C, MPEG-D são novos padrões focados em

⁶ Esta normas podem ser obtidas gratuitamente no site http://www.abnt.org.br/m3.asp?cod_pagina=1249 último acesso em 10 de Fevereiro de 2008.

reconfigurabilidade, respectivamente para sistemas, vídeo e áudio; e o MPEG-E "Middleware Multimídia MPEG" ou M3W provê uma camada de abstração para recebimento e execução de aplicações interativas.

Para o sistema de televisão digital, especialmente o brasileiro, são mais relevantes os padrões MPEG-2, MPEG-4, MPEG-7 e MPEG-21; que serão descritos a seguir.

2.1.2.1 Padrão para TV Digital: MPEG-2

O padrão MPEG-2, estabelecido em 1994, foi projetado para produzir imagens de alta qualidade com maiores taxas de bit (por exemplo, 720 x 485 com qualidade de estúdio CCIR-601) com taxas de vídeo entre 2 e 10Mbps. MPEG-2 foi criado para preencher os requisitos das redes planejadas de radiodifusão digital de TV. São características do MPEG-2:

- Largura de banda elevada (até 40 Mbps)
- Até cinco canais de áudio (isto é, *surround sound*)
- Maior faixa de tamanhos de quadro (incluindo HDTV)
- Possibilidade de operar com vídeo entrelaçado

O MPEG-2 é formalmente conhecido como ISO 13818 e é formado por seis camadas: sistemas, vídeo, áudio, testes, software e DSM-CC (*Digital Storage Media Command and Control*). A camada de teste (*conformance*) especifica uma metodologia de teste para os produtos que utilizam MPEG-2. A camada de simulação de software possui um código de referência em linguagem C do CODEC (codificador e decodificador).

O padrão define perfis e níveis relacionados com os recursos de processamento e com o formato de vídeo e taxa binária resultante, o que permite um padrão genérico, mas com CODECs padronizados.

O MPEG-2 foi desenvolvido para aplicações mais genéricas, precisando, por isso, de uma maior robustez do que o seu antecessor, o MPEG-1, que foi desenvolvido para armazenamento multimídia, que pressupõe baixas taxas de erros.

A Camada de sistemas do MPEG-2 define como compor fluxos de transportes binários, contendo áudio, vídeo e dados. A estes fluxos básicos é dado o nome de fluxo elementar (ES - *Elementary Stream*). Para isso, O MPEG-2 sistemas define tabelas e descritores, com os quais são inseridos meta-dados sobre os componentes do fluxo. Ela define dois tipos de fluxos: de programas (*Program Streams*) e de transporte (*Transport Streams*). Os fluxos de programas são muito parecidos com os fluxos da camada de sistemas do MPEG-1, apenas com algumas modificações de sintaxes e algumas modificações para suportar novas funcionalidades. Já os fluxos de transporte são muito diferentes, elas oferecem a robustez necessária para transmissão em canais ruidosos e permitem multiplexação de programas.

A parte de vídeo do MPEG-2 combina as ferramentas de compressão de vídeo do MPEG-1 com ferramentas novas. Uma importante funcionalidade acrescentada ao MPEG-2 é a escalabilidade. A escalabilidade permite que decodificadores de diversas complexidades possam decodificar um mesmo sinal de vídeo. Resumidamente, este processo é feito a partir de um pré-processamento resultando em um ES de menor qualidade e é realizado, também, um segundo processamento utilizando o sinal de vídeo e este ES, resultando em um ES de melhor qualidade, ambos são multiplexadas e enviadas para o decodificador.

O DSM-CC é definido na parte 6 do padrão MPEG-2 e utiliza o modelo de cliente-servidor para realizar uma série de funções. São definidos cinco protocolos distintos, sendo especialmente relevantes as extensões feitas à camada de sistemas do MPEG-2, permitindo a transmissão de eventos, sincronização e *download*. Também é no DSM-CC que está definido o carrossel de objetos e de dados que permitem o envio de aplicações interativas e pacotes de atualização de software junto ao fluxo de transporte.

O TS (*Transport Stream*), definido no MPEG-2 Sistemas, foi adotado por todos os sistemas de televisão digital terrestre atualmente em operação no mundo. Já o MPEG-2 Vídeo é utilizado nos sistemas ISDB, DVB, ATSC e DTMB. O sistema de áudio do MPEG-2 está em uso no DVB e ISDB.

Em relação às questões de segurança, o MPEG-2 sistema possui algumas tabelas e descritores com foco em questões de proteção de conteúdo, que serão abordadas com profundidade no item 2.4.3.1 (Acesso condicional no padrão MPEG-2 Sistemas).

2.1.2.2 Objetos audiovisuais e alta compressão: MPEG-4 e H.264

O MPEG-4 é um padrão de codificação de conteúdo audiovisual. A motivação da criação do MPEG-4 foi a criação de um método de codificação que facilitasse o acesso a “objetos visuais”, sendo estes naturais ou sintéticos, e associá-los a som, também natural ou sintético. A utilização de um padrão voltado a objetos permite maior interatividade com o conteúdo multimídia.

O padrão MPEG-4 é uma extensão do MPEG-1 e do MPEG-2. O principal avanço do MPEG-4 em relação aos seus antecessores é a maior interatividade permitida ao usuário. Como as cenas são representadas através de objetos audiovisuais, há maior flexibilidade e interatividade com o usuário.

Este padrão também possui maior flexibilidade ao sistema de rede e suas limitações – a parte do padrão ligada a essa camada é o DMIF (*Delivery Multimedia Integration Framework*). O esquema de descrição de cenas utilizado no MPEG-4 é o BIFS (*Binary Format for Scenes*), que é baseado numa linguagem aberta de programação em três dimensões, o VRML (*Virtual Reality Modeling Language*).

As principais funcionalidades oferecidas pela parte de vídeo do MPEG-4 podem ser divididas em três grupos: compressão eficiente, interatividade baseada em conteúdo e acesso global. A compressão eficiente segue os mesmos princípios dos padrões anteriores (MPEG-1 e MPEG-2). Já a interatividade baseada no conteúdo audiovisual, como mencionada anteriormente, é a maior novidade do MPEG-4, que é devida à representação e codificação do conteúdo orientada a objetos, permitindo a manipulação, edição e divisão em camadas de complexidade de cada objeto de uma cena. Já o acesso global, conforme definido por Soares e Pereira (1997), é entendido como a possibilidade de acessar a informação audiovisual a partir de qualquer local e através de qualquer meio, é obtido pela especificação de novos métodos de proteção, detecção e cancelamento dos efeitos dos erros introduzidos pelo canal. O requisito de acesso global inclui assim vários tipos de redes com características heterogêneas em termos de largura de banda e erros de canal, viabilizando aplicações móveis e sem fio.

O MPEG-4 AVC (*Advanced Video Coding*), também conhecido como H.264, é a décima parte do MPEG-4, posteriormente adicionada ao padrão. O H.264 oferece vídeo com qualidade de DVD e taxa de bits 50% menor do que a taxa do MPEG-2.

O H.264 melhora a eficiência de codificação de vídeo utilizando redundâncias temporais, espaciais e psicovisuais. Ele possui algumas novas funcionalidades, como a utilização de blocos para compensação de movimento com tamanhos variáveis, com menor tamanho 4x4 pixels e compensação de movimento com resolução de até um quarto de pixel. Outra nova funcionalidade é a predição espacial direcional para codificação intra, que é a formação de figuras intracodificadas utilizando áreas já decodificadas do quadro atual. Esta funcionalidade permite realizar predição baseada em áreas vizinhas, que não foram codificadas como intra.

A compressão de vídeo utilizando H.264/MPEG-4 AVC gera vídeos mais de 50% menores do que os seus antecessores (MPEG-2 ou MPEG-4 parte 2), para qualidade equivalente de imagem. O H.264 está atualmente sendo adotado para televisão digital no mundo para compressão de vídeo em alta definição, está presente nos sistemas SBTVD, DVB e DTMB.

2.1.2.3 Padrão para descrição de conteúdo multimídia: MPEG-7

Segundo Martinez (2007), o padrão MPEG-7 é denominado Interface de Descrição de Conteúdo Multimídia e define uma série de ferramentas para descrever conteúdos multimídia tanto para processamento por máquinas como por humanos. Nele é definida uma série de descritores e cenas de descrição para organizar as informações tornando o acesso ao conteúdo mais eficiente.

O MPEG-7 permite diferentes granularidades de descrição e pode ser aplicado a qualquer tipo de codificação de dados. Podem ser feitas descrições em alto nível, com necessidade de descrição por humanos, ou em baixo nível, podendo ser gerada automaticamente. Além da descrição do que está sendo apresentado no conteúdo, são inseridas informações sobre o dado multimídia: a codificação empregada, condições de acesso ao material, classificações (indicativa, outras), *links* para materiais relevantes relacionados e contexto.

Dessa maneira, os tipos de descrições que são possíveis com o MPEG-7, são: processo

de criação e produção do conteúdo (exemplos: diretor, título), informações sobre o uso do conteúdo (histórico de uso, informações de propriedade intelectual, guia de programação), informação sobre características de armazenamento (exemplos: codificação, formato), informação estrutural dos componentes do conteúdo (corte de cenas, segmentação em regiões, dentre outros), características em baixo nível do conteúdo (cores, texturas, descrição de melodia, dentre outros), informações sobre a realidade capturada (objetos, eventos, interação entre objetos, dentre outros), informações para busca eficiente do conteúdo (índices, por exemplo), informações sobre as interações do usuário com o conteúdo (histórico, configurações, por exemplo).

Os principais elementos definidos no MPEG-7 são:

- **Ferramentas de descrição:** são definidos dois tipos: descritores e cenas de descrição. Os descritores definem a sintaxe dos metadados para a caracterização dos elementos do conteúdo. As cenas de descrição especificam a relação (semântica) entre componentes da descrição, sejam eles descritores ou cenas de descrição.
- **Linguagem de Definição de Descrição:** define a sintaxe das **ferramentas de descrição**, permitindo a extensão destas. Esta linguagem é baseada na linguagem *XML Schema* (W3C, 2004) com algumas extensões adicionais específicas para conteúdo multimídia.
- **Ferramentas do sistema:** responsáveis por tornar eficientes os mecanismos de armazenamento e transmissão e pelo gerenciamento e proteção de direitos autorais. Inclui os processos de multiplexação de descritores e a sincronização deles ao conteúdo.

Em relação à proteção de propriedade intelectual o MPEG-7 possui uma ferramenta denominada Ferramenta de Descrição de Uso do Conteúdo. Esta ferramenta faz uso de uma *cena de descrição de informação de uso*, a qual inclui um *descriptor de direitos*, nenhum ou um *descriptor financeiro*, nenhum ou muitos *descritores de disponibilidade* e de *armazenamento*. O *descriptor de direitos* não trata explicitamente destas questões no MPEG-7, ao invés disso, são disponibilizadas referências para os detentores dos direitos além de locais para acesso às informações de gerenciamento dos direitos e proteção. O *descriptor financeiro* possui informações relacionadas aos custos gerados e à renda produzida pelo conteúdo. O *descriptor de disponibilidade* indica se o conteúdo pode ou não ser utilizado, já o *descriptor de gravação* armazena o histórico do conteúdo.

2.1.2.4 Arcabouço para aplicações multimídia: MPEG-21

Segundo Bormans ET AL (2003) e Brunett ET AL (2006), o MPEG-21 define a tecnologia necessária para permitir que os usuários possam trocar, acessar, consumir, vender e manipular conteúdo digital de maneira eficiente, transparente e interoperável. É dividido nas seguintes partes:

- MPEG-21 parte 1, “*Vision, Technologies, and Strategy*” – apresenta a visão geral da norma.
- DID (*Digital Item Declaration*): define o modelo, a representação e o esquema para declaração de um item digital (ex: álbum de música), que não precisa necessariamente ser um componente MPEG. O *Digital Item Declaration* define uma série de conceitos abstratos - como a definição da seção, *container*, componente, descritor e recurso – utiliza o XML (*Extensible Markup Language*) para a representação do modelo e o *XML Schema* (W3C, 2004) para determinar a sua sintaxe.
- DII (*Digital Item Identification*) inclui informações para identificação única dos itens digitais, já como descrição o MPEG-21 utiliza o legado do MPEG-7 ou de sistemas proprietários.
- IPMP (*Intellectual Property Management and Protection*): permite que em ambientes não controlados, como o de TV Digital, os Itens Digitais sejam protegidos. Devido ao aparecimento de diversos sistemas abertos interoperáveis de proteção de direitos autorais, o MPEG-21 define um sistema que possibilita o uso destes sistemas de proteção a direitos autorais como plug-ins. O sistema de DRM (*Digital Rights Management*) que será de fato utilizado é sinalizado por metadados específicos.
- REL: *Rights Expression Language* – Linguagem para máquina de definição de direitos autorais. A definição de direitos de uso de conteúdo no MPEG-21, utilizando o REL, pode ser colocada diretamente no interior do Item Digital ou pode ser externa, havendo no Item Digital uma referência para a definição dos direitos de uso. A vantagem de ficar externa é a possibilidade de aplicar-se a mesma definição de direitos de uso para diversos Itens Digitais.
- RDD: *Rights Data Dictionary* - foi desenvolvido para prover a semântica da REL e

possibilitar a interoperabilidade na expressão de direitos de uso. Aborda também a definição de uma metodologia para a criação de metadados interoperáveis que permitam a transação de propriedade intelectual. Esta parte do MPEG-21 define como um RDD pode ser criado, o que ele pode conter e como ser utilizado.

- *DIA: Digital Item Adaptation* – especifica requisitos relacionados ao ambiente de uso e recursos multimídia necessários, com relevância especial para a rede de mídias. Para isso a emissora pode incluir metadados no item digital que informem o conteúdo a ser selecionado para uma dada resolução de tela, ou banda disponível, por exemplo.
- *Relatório de eventos*: trata da geração de um relatório de uso do item digital, sendo aplicável para sistemas com canal de retorno disponível. Podem ser levantadas informações como os trechos assistidos do item digital, número de repetições, entre outras.

Atualmente o MPEG-21 vem sendo aplicado em uma série de padrões internacionais, entre eles na área de comunicação móvel de terceira geração, como no 3GPP (*Third Generation Project Partnership*) e no IMT2000/UMTS (*International Mobile Telecommunications 2000 / Universal Mobile Telecommunication System*). Também é importante citar a influência do MPEG-21 nas normas do DVB, principalmente no DVB-MHP (ETSI TS 101-812), TS 101 224 *Home Access Network*, TS 101 225 *In Home Digital Network* e TS 101 226 *In Home Digital Networks Guide*.

2.1.3 Sistema de Televisão Digital

A transição do sistema de televisão analógico para o digital é considerado uma ruptura tecnológica, devido aos grandes avanços em várias áreas: melhor qualidade de som e imagem, recepção móvel, melhor eficiência espectral e interatividade. A melhoria de qualidade e a mobilidade advêm da modulação digital, que possui códigos corretores de erros sendo muito mais robusta. A eficiência espectral é obtida principalmente pela codificação dos sinais, que permitem o tráfego de mais informação no mesmo canal de frequência antes utilizado pelo sistema analógico. O sistema digital viabiliza ainda a codificação de dados que permite o

envio *softwares* junto ao tradicional programa de TV, além de metadados (informações essenciais para possibilitar a decodificação do sinal). Os programas de computadores associados à programação de TV são responsáveis pela criação da TV interativa.

A Figura 2 apresenta os principais blocos para a transmissão de TV digital terrestre: aquisição digital de sinal, codificação de áudio e vídeo, adição de dados de sincronismo, decodificação e/ou programação interativa, multiplexação (mistura dos dados), modulação, amplificação e transmissão.

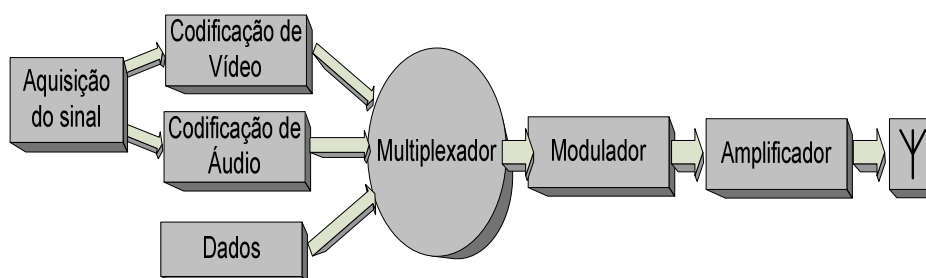


Figura 2. Diagrama de blocos para um sistema de transmissão de TV digital terrestre.

A aquisição do sinal é realizada transformando cada pixel da imagem em um formato digital de representação de cor e do áudio representando uma amostra sonora. Cada pixel pode ser representado por três valores um para cada primitiva de cor (RGB) de até 10 bits, resultando em um arquivo com tamanho excessivamente grande para transmissão. A codificação de áudio e vídeo tem como objetivo diminuir o tamanho dos arquivos adquiridos para a transmissão. A codificação também prepara o arquivo para transmissão serial (*streaming*).

O multiplexador é responsável por combinar os arquivos codificados de áudio e vídeo, inserindo informações necessárias para reprodução sincronizada do áudio e do vídeo, como identificação e sincronização de pacotes, além de informações extras, como sinopse e classificação indicativa dos programas, por exemplo. Estes arquivos combinados geram um único fluxo de dados (TS - *transport stream*) que pode ser interpretado de maneira serial.

É possível ainda, pelo multiplexador, inserir arquivos (ISO/IEC12818-6, 1998). A inserção de arquivos pode ser realizada pelo DSM-CC (carrossel de dados ou de objetos), ou pode ser inserido em pacotes IP (*Internet Protocol*) e depois diretamente em pacotes de TS, conforme formato MPEG-2 (ISO/IEC12818-1, 2000).

Depois de multiplexados os dados a serem transmitidos estão organizados em pacotes

de TS. Estes pacotes são encaminhados para o modulador que é responsável por prepará-los para a transmissão, inserindo códigos corretores de erros, codificando os dados para sinais digitais e modulando o sinal. Depois da modulação o sinal pode ser transmitido.

As configurações dos blocos de processamento apresentados dependem das etapas de processamento do conteúdo, conforme apresentado por Fernando ET AL (2008) e esquematizado na Figura 3. Durante estas etapas são definidas inclusive as regras de uso do conteúdo e inseridos os metadados relacionados à proteção de direitos autorais. Em Fernando ET AL (2008) são apresentadas quatro etapas: produção, aquisição, processamento do conteúdo, gerenciamento do recurso, distribuição e consumo.

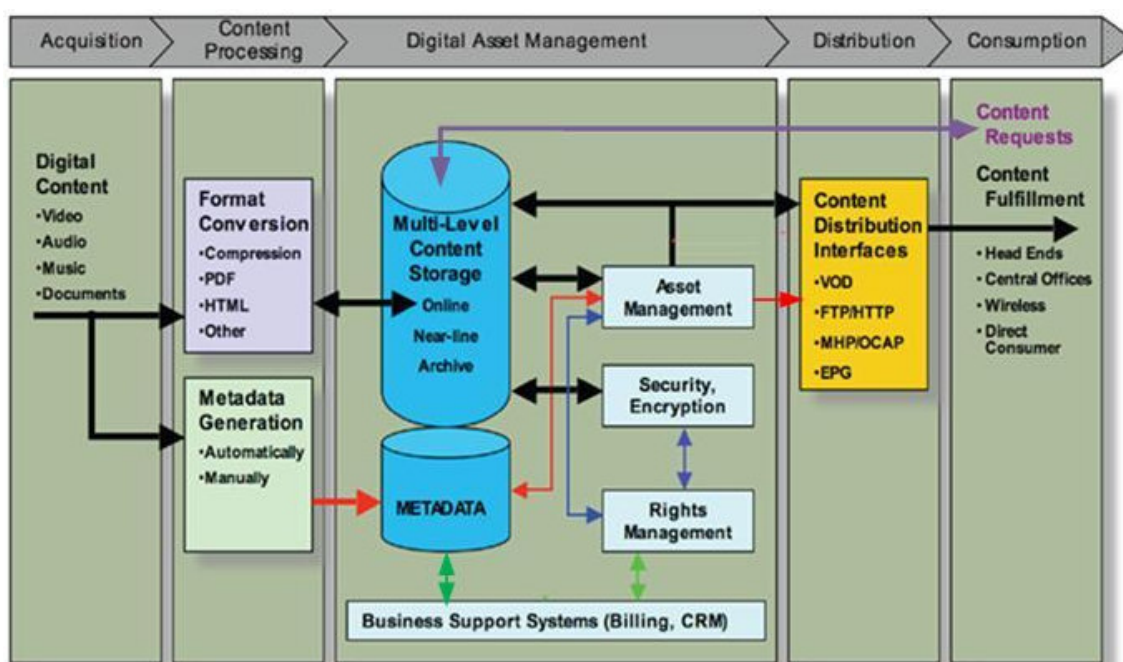


Figura 3. Produção de conteúdo e a inserção do DRM. Fonte: Fernando ET AL (2008)

Após a produção do conteúdo o mesmo é adquirido e em seguida passa para a fase de processamento. Esta fase irá prepará-lo para o formato adequado de distribuição e consumo. Por exemplo, um mesmo vídeo pode ser empregado para cinema digital ou recepção móvel em celular. Os requisitos de cinema digital são de conteúdos de altíssima qualidade e o emprego de métodos de compressão sem perdas, conforme apresentado na norma DCI (2008). Por outro lado, para uso de conteúdo em celulares a taxa de transmissão deve ser baixa e, devido ao tamanho das telas reduzido, a compressão pode ter perdas, com qualidade muito

menor. Os diferentes requisitos de cenários de compressão e consumo levam a tipos de processamento distintos para vídeo, alterando, por exemplo, formato de tela, resolução e tipo de compressão. Ainda na fase de processamento são gerados os metadados do conteúdo relacionado. A próxima fase no ciclo de vida do conteúdo, gerenciamento, integra ao conteúdo os metadados, define as suas regras de uso, aplica as ferramentas e métodos de proteção de conteúdo para posterior distribuição e consumo.

Existem atualmente quatro sistemas de televisão digital terrestre e aberta em operação no mundo: o SBTVD, o DVB, ISDB-T, ATSC, DTMB. A Tabela 1 apresenta as principais características de cada um deles. O *middleware* brasileiro Ginga, possui uma parte declarativa, que utiliza linguagens de programação desenvolvidas no Brasil, o NCL e LUA; e uma parte procedural, que utiliza como referência o GEM/MHP.

Tabela 1. Quadro comparativo entre sistemas de TV Digital (recepção fixa)

Sistema Padrão	SBTVD / ISDB-T _B	DVB	ISDB-T	ATSC	DTMB
<i>Middleware</i>	Ginga/NCL+GEM	MHP/GEM	BML	DASE/GEM	Não disponível
Camada de transporte	MPEG-2 Sistemas	MPEG-2 Sistemas	MPEG-2 Sistemas	MPEG-2 Sistemas	Não disponível
Codificação de vídeo	MPEG-4 AVC HD	MPEG-2 SD ou H.264	MPEG-2 HD	MPEG-2 HD	Não disponível
Codificação de áudio	MPEG-4 HE-AAC LATM/LOAS 5.1	MPEG-2 layer 2 e AC3 Dolby Digital	MPEG-2 AAC	AC3 Dolby Digital 5.1	Não disponível
Modulação	BST-COFDM–codificação hierárquica com 13 segmentos	COFDM	BST-COFDM codificação hierárquica com 13 segmentos	8-VSB e 16-VSB	TDS-OFDM

2.1.3.1 Televisão interativa

A digitalização da televisão permite a agregação de uma ampla diversidade de novas

funcionalidades ao usuário do televisor. O principal impacto é a mudança de paradigma trazida por esta novidade tecnológica, isto é, o telespectador passará agora a ser visto como usuário, já que ele deixa de ter um comportamento passivo em relação ao televisor e passa a participar e interagir com os programas oferecidos, LSI-TEC (2006).

Na TV analógica, assistir TV é basicamente uma experiência passiva. Nos últimos anos, as emissoras vêm se esforçando para mudar esse aspecto, inserindo o máximo de interatividade que o sistema analógico permite. Isso se resume a ligações telefônicas que permitem modificar a grade de programação, definir o final de um programa ou votar no vencedor de uma competição. A chegada da TV digital no Brasil trará novas perspectivas, permitindo a inclusão da interatividade de uma maneira mais integrada, como apresentado em LSI-TEC (2006). Os tipos de serviços interativos para TV digital seriam os seguintes:

- TV aperfeiçoada: Os serviços de TV aperfeiçoada consistem na disponibilização de informações adicionais à programação da televisão. Estes dados são enviados juntamente com o sinal de vídeo. Neste sistema, é possível ver a programação das emissoras, sinopses de filmes e novelas, ler notícias, ver a previsão do tempo, classificação de campeonatos, escalações de equipes esportivas, estatísticas de jogos, e propagandas interativas simples.
- TV individualizada: permite uma experiência personalizada a quem assiste TV. Este termo engloba escolhas de ângulos de visão de um mesmo programa; visualização de reapresentação de cenas em jogos esportivos e corridas automobilísticas; assim como respostas a perguntas em programas de auditório de televisão, podendo a resposta ser enviada à emissora ou apenas ser comparada à resposta correta na própria unidade de recepção digital.
- TV pessoal: O termo TV pessoal é utilizado especialmente para aplicações de Gravador Pessoal de Vídeo que permitem o armazenamento de programas para serem assistidos em momento posterior.
- TV com Internet: Exemplos de aplicações de TV por Internet são serviços de Internet adaptados para a televisão. Exemplos: *e-mail*, *chat*, navegação na Internet.
- TV sob demanda: aplicações de disponibilização de programação sob demanda, como filmes, programas, *shows* e noticiários. Este tipo de aplicação exige um grande investimento em infraestrutura de rede e de servidores de vídeo, além do pagamento dos direitos autorais do conteúdo disponibilizado.

- TV para jogos: designa aplicativos de jogos na TV. Jogos multiusuários e monousuário fazem sucesso em computadores e consoles, sendo esperado que repitam o mesmo desempenho em TV Interativa.
- Comércio eletrônico: são as aplicações bancárias e comércio eletrônico na televisão. Os bancos no Brasil, inclusive já permitem movimentações e alguns oferecem consulta a saldos e extrato via Internet, sendo esperado que todas as funcionalidades dos bancos sejam migradas também para a TVD. As aplicações de comércio eletrônico pela TV, também chamadas de *t-commerce*, possibilitam desde uma simples requisição de catálogo até a compra efetiva do produto.
- TV educativa: são aplicações voltadas para educação. Este serviço comporta aplicações de ensino a distância e de suporte ao ensino.
- TV comunitária: são os serviços de interesse comunitário, como votações, veiculação de informações, da mesma forma que o suporte a comunidades virtuais, como as da Internet.
- TV Global: TV Global significa acesso sob demanda à programação internacional com tradução automática de idioma. Vários serviços interativos se encaixam nesta classificação, como os portais de serviços das operadoras de TV por assinatura, mosaico de canais, propagandas interativas e aplicações de comércio eletrônico.

2.1.3.2 Receptor de Televisão Digital

Os receptores de televisão digital são responsáveis pelo recebimento e apresentação dos sinais enviados pelas emissoras de TV no sistema digital. Eles podem ser de vários tipos, com diferentes níveis de complexidade e valor agregado para o usuário final.

Como o sistema digital permite a mobilidade, uma primeira categorização poderia ser obtida dividindo os receptores em fixos ou móveis. Os receptores móveis são viabilizados pela maior robustez do sistema, podendo ser integrados a automóveis e dispositivos de mão,

como celulares. Já os receptores fixos podem ser de duas categorias principais, os adaptadores e os televisores integrados. Os adaptadores, conhecidos como *set-top box*, em inglês, são terminais de acesso ao sistema de televisão digital e adaptam o sinal aos televisores do sistema anterior, analógico. Eles não possuem monitores integrados e por isso, devem ter interfaces de saída para áudio e vídeo para conexão com monitores externos. Já os receptores integrados possuem monitores, sendo as interfaces de saída opcionais, apenas para distribuição de vídeo no ambiente doméstico.

Outro aspecto relevante a se considerar nos receptores de televisão digital é a expectativa do seu ciclo de vida. Enquanto o ciclo de renovação de computadores pessoais costuma ser da ordem de cinco anos, o de eletrônicos de consumo, como de televisores e DVDs, é de dez a quinze anos. Outra diferença significativa é que dispositivos de eletrônica de consumo costumam ser auto-suficientes, ao contrário de computadores pessoais que podem ter instalações de *softwares* e modificação de programas freqüentemente.



Figura 4. Arquitetura de software de receptores de televisão digital interativos.

Conforme apresentado na Figura 4, a arquitetura de software de um receptor de televisão digital interativo pode ser subdividida em cinco blocos: 1- *Software Genérico*, 2- *Middleware*, 3- *Software Específico de Arquitetura*, 4- *Sistema Operacional*, 5- *Drivers*. Estes blocos estão distribuídos em duas camadas: aplicação e infraestrutura.

A camada de aplicação engloba os blocos: *software específico de arquitetura* e *software genérico*. O *software específico de arquitetura* define códigos compilados a uma arquitetura específica e somente são executados na mesma. Esta camada é utilizada para desenvolver aplicativos como os que apresentam e controlam menus de configuração, os que realizam troca de canais e alteração de volume. Os aplicativos de televisão digital não podem ser construídos na camada de *software* específico, pois requereria a compilação e transmissão

de um mesmo aplicativo para os diversos tipos de receptores existentes. Nesse contexto, foi definida uma especificação que define chamadas de *software* responsável por garantir independência de arquitetura, o *middleware*. Sobre o *middleware* são executados os aplicativos interativos, na camada do *software* genérico. O aplicativo interativo é executado utilizando as funções e métodos disponibilizados pelo *middleware*.

Já a camada de infraestrutura engloba os blocos: *middleware*, sistema operacional e *drivers*. O *middleware*, como dito anteriormente é uma camada de abstração. O Sistema Operacional é responsável por gerenciar e alocar recursos para a camada de aplicação e *middleware*. Por gerenciar recursos entende-se gerenciar o funcionamento do sistema, indicando qual *software* entrará em execução, por quanto tempo ele executará sem interrupções até ceder o processamento a outro. Já os *drivers* são softwares de comunicação e controle de dispositivos de *hardware*.

Considerando agora a sua arquitetura de *hardware*, todos os receptores de televisão digital devem ter alguns blocos com funcionalidades essenciais para atender ao seu objetivo básico, que é receber o sinal digital de televisão e exibi-lo em um monitor. Para isso, devem estar presentes no terminal, a cadeia de recepção, sintonia, desmultiplexação, descompressão e processamento de sinais. No caso de terminais de acesso que levam a tecnologia digital ao legado de televisores existente hoje, também será necessário um dispositivo com interfaces de saída de áudio e vídeo para conexão com os aparelhos televisores. A Figura 5 apresenta a arquitetura de *hardware* do terminal de acesso.

O bloco *front-end* é responsável pela recepção, sintonia, demodulação e decodificação de canal (incluindo correção de erros), sendo composto do sintonizador, demodulador e decodificador de canal. O sintonizador (*tuner*) tem a função de não apenas selecionar o canal a ser tratado, mas também de amplificar, filtrar e converter o sinal recebido para uma frequência menor (frequência intermediária). Já o demodulador tem a função de converter o sinal modulado em sinal banda-base codificado. O decodificador de canal faz a detecção e correção de erros utilizando o código corretor de erros adotado pelo sistema de televisão digital em uso.

O *front-end* possui interdependência com o bloco de núcleo de processamento e recebe os sinais captados pela antena do receptor. Os comandos provenientes do núcleo de processamento têm por objetivo configurar a sintonia de canal que será visualizado pelo usuário final. Já os sinais recebidos pela antena são os sinais digitais que devem ser decodificados, obtendo-se sinais de áudio e vídeo, a serem exibidos e ouvidos no aparelho de

TV, podendo opcionalmente fornecer sinais de áudio para sistemas de som independentes.

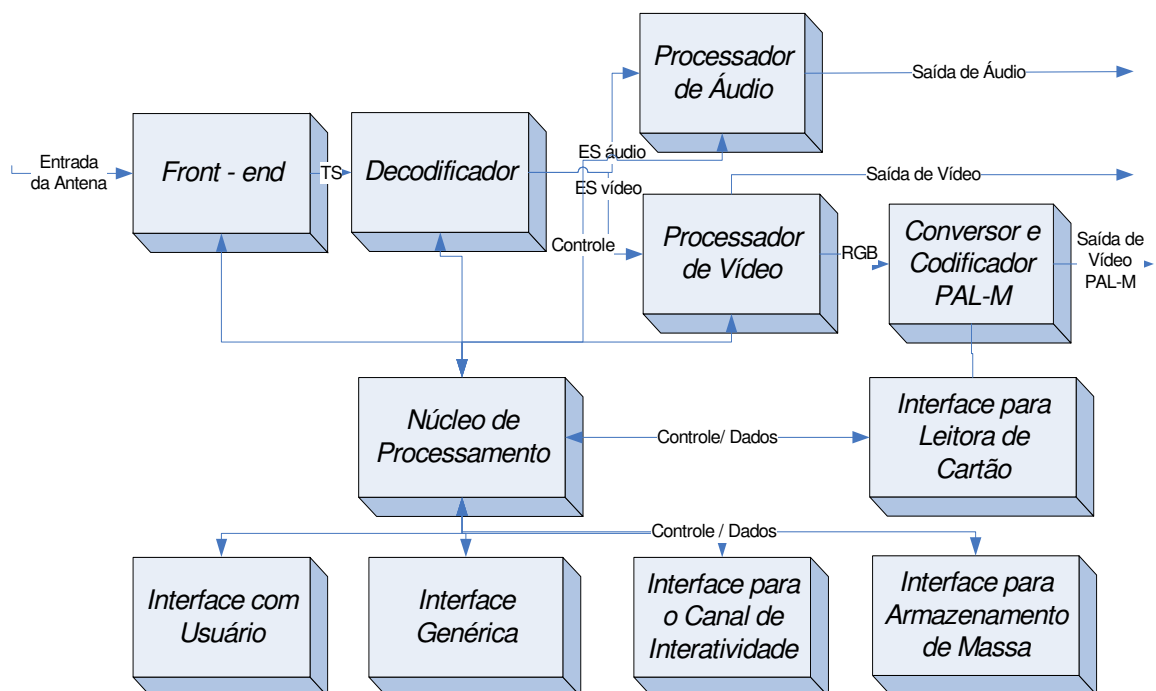


Figura 5. Arquitetura do Receptor de Televisão Digital

O bloco do decodificador é essencial por descomprimir os sinais enviados pelas emissoras de televisão. Estes sinais podem conter informações de áudio, vídeo ou dados. São considerados requisitos mínimos: a decodificação da camada de transporte, de áudio e de vídeo, excluindo-se a necessidade de decodificação de dados.

O decodificador tem interfaces com o núcleo de processamento, com o *front-end* e com a cadeia de tratamento de sinais de áudio e vídeo. O controle do decodificador é realizado pelo núcleo de processamento e os dados decodificados são enviados para a cadeia de tratamento de sinais de áudio e vídeo. Os sinais de entrada para este bloco são provenientes do *front-end* e são denominados *transport stream* (fluxo de bits) contendo informação comprimida.

O Conversor e Codificador PAL-M é responsável pelo processamento inicial de áudio e vídeo, realizando o tratamento dos sinais digitais de áudio e vídeo para prepará-los para exibição. Este bloco realiza a conversão dos sinais digitais para analógicos e a codificação destes sinais para o formato PAL-M.

A importância deste bloco para o terminal de acesso está intimamente ligada ao monitor utilizado. No caso de um televisor analógico simples, é necessário que seja inserido sinal codificado em PAL-M. No caso de monitores com entradas digitais, não há necessidade de passar o sinal por este bloco. O Conversor e Codificador PAL-M não possui interdependência significativa com os demais blocos do sistema, sendo a sua relação predominantemente com o núcleo de processamento para configurações iniciais.

O bloco de interface de comandos do usuário é importante por permitir a interação do usuário com o terminal de acesso. No caso das características essenciais, a principal interação do usuário é na seleção de programas e para o comando de ligar e desligar o equipamento. Para os receptores de televisão interativa, a interface de comandos do usuário permite interação com o *software* que está sendo executado sobre o *middleware*. Para receptores fixos, a interface de comandos essencial é via controle remoto e painel frontal.

O núcleo de processamento é composto pelo processador central, memórias de sistema e controlador de periféricos. Ele é responsável por executar a pilha de *software* na plataforma: receber os comandos do usuário, controlar o demodulador (sintonizador), configurar o dispositivo de conversão e codificação dos sinais de áudio e vídeo e executar os aplicativos e o *middleware*.

Estes são os blocos mínimos do receptor, que visam à recepção dos sinais digitais, o que permite o aproveitamento de imagem e som com qualidades muito superiores à oferecida pelo sistema atual. Para dar suporte à interatividade o receptor deveria apresentar módulos para possibilitar um canal de retorno e dispositivos de interação mais complexos como dispositivo apontador e teclado.

O bloco de interface genérica permite a escalabilidade do terminal para conexão de outros dispositivos, tais como: impressora, *modem* e *joystick*. Em LSI-TEC (2006) a interface USB (*Universal Serial Bus*) é recomendada como a interface genérica preferencial para receptores de televisão digital. Esta proposta foi mantida na normatização do SBTVD, conforme apresentado na ABNT NBR 15604 (2007), que considera a presença da interface como item recomendável. A USB é uma interface rápida e flexível para a conexão de dispositivos. Suas principais vantagens são: facilidade de uso (configuração automática, cabos simples, conexão e desconexão com o sistema ligado), capacidade de prover alimentação aos dispositivos e taxa de transmissão de dados. A USB possui *drivers* genéricos para determinadas aplicações, como teclados e dispositivos de armazenamento (*pendrives*), permitindo a instalação de *drivers* mais específicos para outros tipos de aplicações através de

memórias internas aos próprios dispositivos USB.

O bloco de interface para armazenamento de massa permite que o terminal de acesso possa ter funcionalidades diferenciadas a partir do armazenamento da programação exibida. Este armazenamento pode permitir novas funcionalidades, algumas requerendo muita capacidade de armazenamento e outras resolvidas com unidades de armazenamento mais modestas.

A interface para leitora de cartão refere-se à possibilidade de utilizar um cartão criptográfico para identificação de usuário ou acesso condicional.

O bloco de interface para o canal de interatividade é um bloco opcional. Ele seria responsável por possibilitar o retorno de informações para um servidor de serviços, tornando o canal de comunicação da televisão bidirecional. Por ser um bloco opcional, o ambiente de televisão digital possui a dificuldade intrínseca de ser um ambiente unidirecional, não havendo, portanto confirmação de mensagens recebidas, dificultando o desenvolvimento de alguns serviços e sistemas. A atualização de *software*, por exemplo, passa a ser um desafio, já que não há confirmação de recebimento de pacotes pelos receptores e o parque de receptores é muito extenso, Intel (2006).

LSI-TEC (2006) define categorias de interatividade para TV digital. As categorias para interatividade são: não-interativo, interativo-local e interativo pleno.

O receptor não-interativo possui como principal meio de comunicação o canal de radiodifusão, que recebe os sinais das emissoras de televisão. Este canal recebe *transport stream* em formato MPEG-2 sistemas, definido em ISO/IEC 13818-1 (2000), trafegando áudio, vídeo e dados. O receptor não interativo recebe os dados do *transport stream* para aplicações muito restritas, entre elas: atualização do seu *software* nativo, metadados para construção de guia eletrônico de programação e apresentação de informações sobre o programa, como a sua classificação indicativa. Aqui o usuário interage com a TV, mas apenas da maneira tradicional. A Figura 6 apresenta o diagrama de interações para os receptores não interativos.



Figura 6. Receptor não interativo.

Já os receptores interativos, com a presença do *middleware*, também recebem aplicações pelo canal de radiodifusão, pelo carrossel de dados, definido pelo MPEG-2. Os aplicativos interativos podem ser executados em qualquer plataforma, independentemente de fabricante e do sistema operacional. Os aplicativos que executam sobre a API do *middleware* podem ser residentes ou não residentes. Os não residentes são removidos da plataforma ao mudar o canal sintonizado ou ao finalizar o programa ao qual o aplicativo estava vinculado. Os residentes são aqueles que ficam instalados na plataforma por tempo indeterminado. A interatividade plena ou local é determinada pela presença do canal de interatividade.



Figura 7. Receptor interativo-local.

A interatividade na TV digital pode ter duas formas principais, com canal de retorno ou sem canal de retorno. A interatividade sem canal de retorno é denominada interatividade local. Este tipo de interatividade funciona unidirecionalmente, ou seja, os aplicativos interativos são enviados juntamente aos conteúdos áudios-visuais transmitidos pelas emissoras, mas não há informação de volta, trafegando da casa do usuário para a emissora. Neste cenário, o usuário poderia, por exemplo, participar de um programa de perguntas e respostas e ter os seus pontos para comparar com o dos participantes do programa, mas a emissora não teria como receber estes resultados. A Figura 7 apresenta o diagrama de interação do receptor com interatividade local.

Já com o canal de retorno, a interatividade é denominada plena. Este canal extra de comunicações é bi-direcional e permite o desenvolvimento de aplicativos para participação em enquetes, concursos, realização de compras (*T-Commerce*), entre outras. A Figura 8 apresenta o diagrama de interação para o cenário de interatividade plena.



Figura 8. Receptor interativo-pleno.

2.2 Estudos e análises do SBTVD fase I

No SBTVD fase I, de pesquisa e desenvolvimento, foram gerados estudos e análises em relação à segurança no terminal de acesso, LSI-TEC (2006). Nessa ocasião foram considerados apenas os mecanismos de suporte do receptor e não as funcionalidades de segurança de uma maneira geral. Na ocasião, foram levantados os seguintes requisitos de segurança para terminais de acesso, conforme apresentado na Tabela 2: identificação e autenticação do terminal de acesso, soquete de comunicação segura, segurança na atualização de *software/firmware*, identificação e autenticação de usuários locais, identificação e autenticação de usuários de serviços, restrição de programação, proteção de conteúdo, sincronização de relógio e armazenamento seguro de certificados digitais raiz.

O requisito de **identificação e autenticação do terminal de acesso** tem o objetivo identificar unicamente o equipamento terminal de acesso com capacidade de impedir a personificação do terminal de acesso por um terminal impostor. Foi proposto o uso de chaves assimétricas para o serviço de autenticação. O padrão proposto é o RSA de 2048 bits com armazenamento da chave privada em cartões criptográficos ICP ou hardware TPM (*Trusted Platform Module*). A chave pública deveria ser disponibilizada na forma de certificado digital, denominado certificado de autenticação do terminal de acesso. Já para a identificação, seria realizada pela composição do modelo do equipamento e um número serial com o apoio de alguma entidade nacional.

O requisito **Soquete de Comunicação Segura** provê comunicação segura para as mensagens a serem enviadas ou recebidas. Entre as duas alternativas técnicas identificadas no trabalho: segurança de canal de comunicação – necessita de canal de interatividade – e segurança de mensagens, o trabalho apresenta a segurança de mensagens como mais adequada para o desenvolvimento do soquete de comunicação segura.

Já o requisito de **segurança na atualização do *software/firmware*** tem por objetivo controlar a atualização de *software / firmware*, que é um processo importante do terminal de acesso. Como requisitos mínimos de segurança, para este processo foram identificados a integridade do conteúdo (*software/firmware*) e a autenticação de origem do conteúdo (*software/firmware*). Para isso, foi proposto o uso de um esquema de assinatura digital para a segurança do processo.

Tabela 2. Classificação dos Requisitos de Segurança

Requisitos de segurança considerados	Obrigatório	Opcional
Identificação segura do terminal de acesso;		
Soquete de Comunicação Segura		
Segurança na atualização de <i>software/</i> firmware		
Identificação e autenticação de usuários locais		
Identificação e autenticação de usuários de serviços		
Restrição de programação		
Proteção de conteúdo		
Sincronização do relógio		
Armazenamento seguro de certificados digitais raiz		

O **sincronismo do relógio** é necessário para atender às diversas funcionalidades do terminal de acesso que necessitam do relógio devidamente sincronizado para que opere de maneira correta como, por exemplo: validação de certificados quanto ao período de validade e à revogação; validade de credenciais de acesso a serviços; *time stamp* para verificação de integridade de mensagens quanto a ataques de rerepresentação (*replay*), principalmente nas transmissões realizadas através do canal de radiodifusão.

O trabalho propõe a existência de um processo de gerência do sistema operacional do terminal de acesso que deverá ser responsável pelo recebimento dos pacotes de sincronismo, validação e atualização do horário no terminal de acesso. Além disso, nenhuma aplicação do middleware deveria ter capacidade de alteração do horário do sistema.

O **Armazenamento seguro de certificados digitais raiz** é o ponto mais crítico, do ponto de vista de segurança, quando é utilizada uma infraestrutura de Chaves Públicas. A integridade da relação de certificados raiz confiável deve ser garantida. No SBTVD fase I, foi proposto que o mecanismo de proteção do certificado raiz devesse ser baseado em alguma

variante de cartões criptográficos de Infraestrutura de Chaves Públicas e hardware TPM (*Trusted Platform Module*).

O requisito de **Identificação e autenticação de usuários locais** tem o objetivo de prover o suporte ao conceito de Usuários de Terminal de Acesso para possibilitar algumas funcionalidades como, por exemplo, a customização de perfil por usuário (parâmetros de áudio, parâmetros de vídeo, canais favoritos, definição de parâmetros de restrição de programação, gerenciamento de usuários locais). Recomendou-se dar suporte a usuário local, com dois usuários nativos (mestre e padrão) e com autenticação baseada em senha.

O requisito de **Identificação e autenticação de usuários de serviços** trata os usuários de serviços gerenciados por entidades externas ao terminal. Recomenda-se o fornecimento de suporte à autenticação de usuários de serviços baseado em senha e *smartcard*.

O requisito de **restrição da programação** foi definido como podendo ser feito por seleção no perfil do usuário e/ou por outros parâmetros como, por exemplo: classificação indicativa. Foi proposto que o mecanismo de restrição de programação fosse baseado em alguma variante de cartões criptográficos ICP e com componente de *hardware Trusted Platform Module*.

Para o requisito de **Proteção de Conteúdo** que trata do acesso condicional para aplicações como canal de TV pago, programas de treinamento para profissionais de diferentes áreas do governo, saúde, sindicatos e da iniciativa privada. Neste trabalho não foram definidos os mecanismos de acesso condicional, apenas sugerido o uso de distribuição dinâmica de chaves, com par de chaves assimétricas para identificação do receptor, com a chave privada protegida por *hardware*.

A Figura 9, apresenta a infraestrutura proposta para prover cada um dos requisitos Tabela 2.

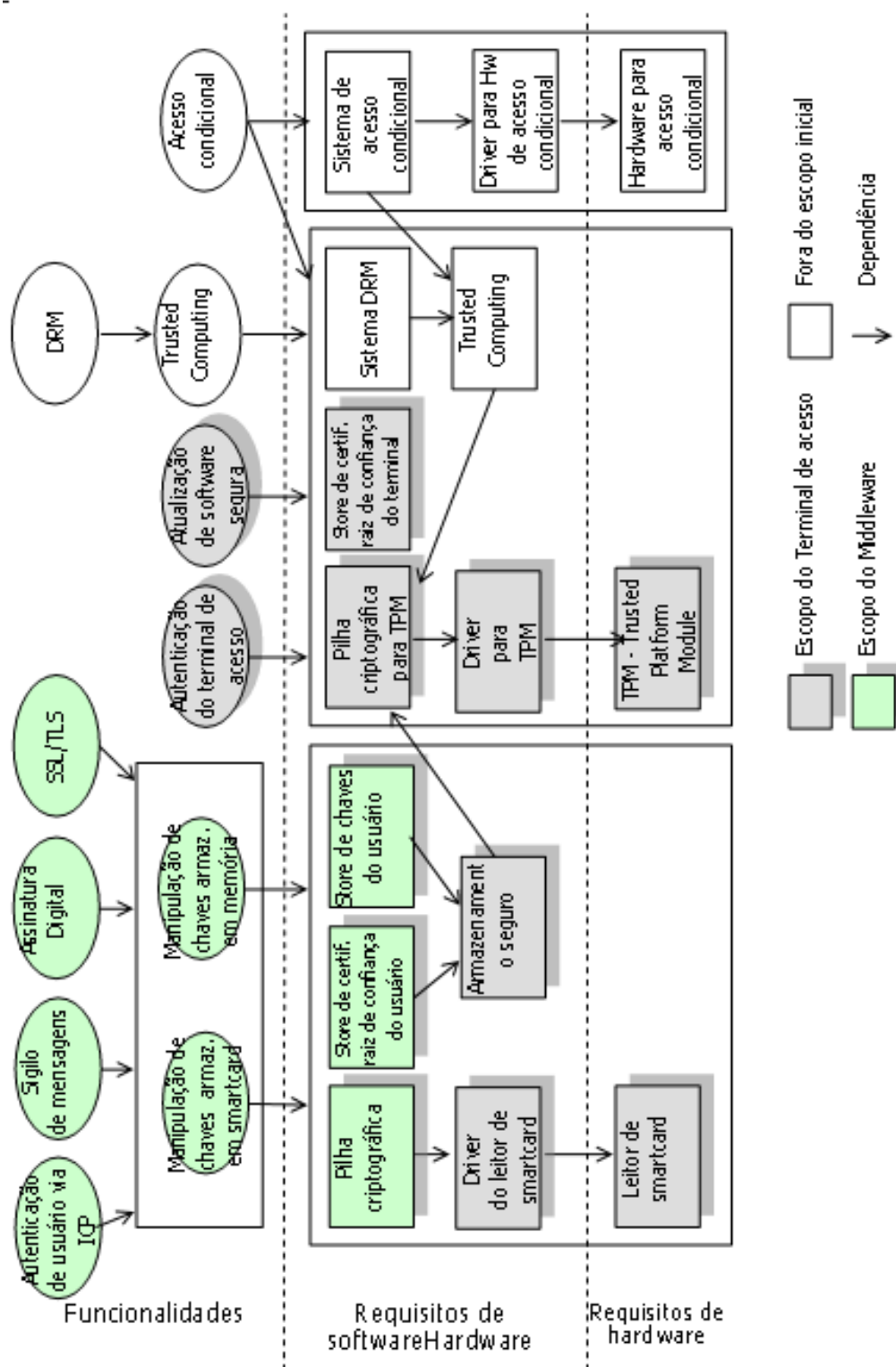


Figura 9. Escopo do Soquete de Segurança

2.3 Definição de Segurança da Informação

Segundo a definição do *US Code Collection* (2008), o termo Segurança da Informação significa proteger uma informação ou um sistema de informação do acesso, uso, divulgação, modificação ou destruição não autorizada; provendo integridade, confidencialidade e disponibilidade. A garantia de integridade significa proteger o conteúdo contra modificação ou destruição imprópria do conteúdo, inclui ainda a garantia da autenticidade da fonte da informação e o não repúdio pelo seu expedidor. A confidencialidade é relacionada à privacidade, restringindo o acesso e divulgação das informações. Já a característica de disponibilidade garante acesso à informação quando esta for necessária de maneira rápida e precisa. A segurança na televisão digital terrestre, nada mais é do que a aplicação destes conceitos aos casos de uso da televisão digital.

2.4 Proteção de direitos autorais

O sistema de proteção a direitos autorais é responsável por garantir o direito de exploração dos autores sobre as suas produções através de uma série de ferramentas. Ele é normalmente denominado DRM (*Digital Rights Management*) e refere-se a um conjunto de políticas, ferramentas e técnicas para garantir a obediência a algumas regras no uso do conteúdo. Deve ser levado em consideração, entretanto, que não há como garantir a segurança absoluta do conteúdo e que as ferramentas de um sistema de DRM não serão contornadas, como afirmado por Subramaya e YI (2006).

Segundo Jonker e Linnartz (2004), os principais elementos de um sistema de DRM são: descrição do item digital, linguagem de direitos, licenças, esquema de proteção do conteúdo, conformidade de dispositivos e robustez de dispositivos. Apesar de não citado diretamente pelos autores, é importante ressaltar o mecanismo de proteção de interfaces, que será acrescentado à lista dos itens que constituem um sistema de DRM a serem considerados neste trabalho. A seguir serão descritos cada um destes elementos:

- Descrição do item digital – é utilizada para descrever o item a ser protegido, para esta descrição podem ser utilizados desde padrões mais complexos como o MPEG-21 até padrões mais simples como a camada de sistemas do MPEG-2.
- Linguagem de direitos – são utilizadas para descrever as regras de uso de conteúdo, quem e como o conteúdo pode ser utilizado. Exemplos são o XrML, MPEG-21 e os citados em Iannella (2001) e Chong (2003).
- Licenças – as licenças são utilizadas como um mecanismo para distribuir os direitos expressos pela linguagem de direitos relacionada ao item digital descrito. Normalmente as licenças contêm as chaves de acesso ao conteúdo, caso este esteja protegido por criptografia.
- Esquema de proteção do conteúdo – o conteúdo pode ser protegido por criptografia, marca d'água com o conteúdo aberto, dentre outras técnicas.
- Conformidade de dispositivos – os sistemas de DRM requerem que os dispositivos que receberão os conteúdos protegidos obedeçam às regras do sistema.
- Robustez de dispositivos – os sistemas de DRM exigem dos dispositivos considerados conforme a um dado sistema uma série de requisitos de robustez, que garantam que os requisitos do sistema sejam mantidos.
- Mecanismos de controle de conteúdo exportado pelas interfaces – responsável por definir o mecanismo de proteção do conteúdo exportado do dispositivo caso seja necessário, informando as regras de uso e podendo proteger o conteúdo por criptografia.

Os sistemas de DRM podem ser utilizados para controlar o acesso e uso de um dado conteúdo em vários cenários, desde para conteúdos de áudio e vídeo gerados por grandes gravadoras até conteúdos gerados por pessoas físicas, como um relatório de escola, por exemplo. Com o avanço das redes de computadores e da Internet a distribuição de conteúdo é muito rápida e simples. Por outro lado, esta facilidade pode trazer problemas relacionados à privacidade e à pirataria. É com o objetivo de impor regras de uso ao conteúdo que surgem os sistemas de DRM. Ele pode ainda ser utilizado em ambiente corporativo, empresas organizadas em redes podem ter vários conflitos internos pela falta de definição de papéis e estabelecimento de contratos internos, o que pode ser propiciado pelo uso de sistemas de DRM, como apresentado por Fernando, Jacobs e Swaminathan (2005) e exemplificado por

Luoma e Vahtera (2004).

Apesar dos muitos modelos de negócio possibilitados por esses sistemas, devido a limitações ainda existentes nas tecnologias de DRM, existe uma série de movimentos contrários ao seu uso. Um exemplo seria o artigo de Walker (2003).

Observando as referências atuais, não apenas científicas, mas também de divulgação, pode-se afirmar que as limitações atuais de maior relevância nos sistemas de DRM são a falta de interoperabilidade entre sistemas existentes, limitação de movimentação do conteúdo protegido e o custo agregado. O custo advém principalmente da necessidade de processamento adicional e do uso componentes de hardware específicos.

Os sistemas de DRM para conteúdo áudio-visual comercialmente empregados hoje em sistemas como o Windows Media DRM, descrito por Cohen (2002), ou o sistema de DRM do iTunes, Roughly (2007), são proprietários e não permitem a interoperabilidade de conteúdo entre eles. Isto gera o inconveniente ao usuário final de possuir mais de um *software* de reprodução instalado no seu computador e de não poder optar pelo seu favorito para reprodução das músicas adquiridas. Existe mais de uma iniciativa que busca criar um sistema de DRM interoperável e padronizado, pode-se citar o Digital Media Project, o DReaM e o Coral. Esta falta de interoperabilidade afeta também a transferência de conteúdos para dispositivos embarcados, que não possuem poder de processamento e armazenamento para ser compatível com vários tipos de sistemas de DRM e *softwares* de reprodução.

Com a miniaturização de dispositivos e com o avanço das redes sem fio, tem-se cada vez mais a formação de uma rede ubíqua em torno do indivíduo, e o sistema de DRM atual passa a ser um problema para esta ubiquidade por gerar barreiras entre dispositivos. Uma vez que o usuário final adquire um conteúdo ele espera poder usufruí-lo em qualquer local, seja no seu carro, no *MP3 Player*, no computador ou no som da sala de estar. Desta maneira, torna-se importante que a reprodução de conteúdo não seja restrita a um único equipamento. Neste sentido pode ser citada a iniciativa de Merabti e LLewellyn-Jones (2006), na qual é proposto um método, ainda em desenvolvimento, de gestão de direitos autorais distribuído. Neste método, cada dispositivo da rede julga a operação que está sendo realizada e determina em função delas as restrições que devem ser empregadas.

Como ressaltado por Merabti e LLewellyn-Jones (2006), outro desafio dos sistemas de DRM utilizados é a agregação de custo aos dispositivos de consumo. Com o objetivo de assegurar robustez ao sistema podem ser empregados TPMs (*Trusted Computing Platform*) e

cartões criptográficos (*smartcards*) que não permitem violação interna, sendo possível estabelecer uma cadeia de confiança no sistema. O ponto negativo seria o custo destes componentes, que para evitar uma transgressão acabam atingindo pessoas honestas, que com uma proteção mais informativa já obedeceriam às regras de uso do conteúdo. Outra ferramenta que pode ser citada é a marca d'água (*digital watermarking*), que consiste de informações enviadas misturadas ao conteúdo que não são perceptíveis ao usuário final, nem removíveis sem danificar o conteúdo e que poderiam carregar as informações de DRM. O problema da marca d'água é que ela requer grande poder de processamento para a sua interpretação.

O sistema de proteção de direitos autorais depende por isso de uma série de ferramentas e mecanismos que juntos formam o sistema de proteção de direitos autorais. Mas, além destas questões técnicas, o sistema deve ainda estar intimamente ligado às leis e regras contratuais do local onde será utilizado. A seguir serão apresentados comentários em relação à legislação brasileira na área, em seguida será apresentada a fundamentação teórica dos mecanismos e ferramentas necessários ao sistema de proteção de direitos autorais e finalmente serão apresentados alguns dos sistemas em uso ou em fase de proposta.

2.4.1 Legislação brasileira para proteção de direitos autorais

A legislação brasileira apresenta uma série de leis relacionadas a direitos autorais, mas nenhuma delas é específica para o ambiente digital. Foram identificadas as seguintes leis relacionadas ao tema: lei 9.279/1996 – Direitos relativos à Propriedade Industrial -, lei 9.609/1998 – Direitos relativos à Propriedade Intelectual de Programa de Computador -, lei 9.619/1998 – Direitos Autorais.

Pela análise do texto destas leis, pode-se relacioná-las ao sistema de televisão digital. A lei de direitos autorais relativos à propriedade intelectual de programa de computador é aplicável ao ambiente de TV digital devido à possibilidade de existência de programas de televisão interativos, no sistema digital. A lei de direitos autorais garante a proteção aos direitos da produção do conteúdo propriamente dito e a lei de direitos relativos à propriedade industrial refere-se à proteção de invenção do formato de programas.

De maneira geral, estas leis garantem direito ao autor, inventor, ou produtor aos lucros obtidos com a revenda de suas obras ou uso de suas invenções e o seu direito ao controle de utilização da obra por quaisquer modalidades.

2.4.2 Fundamentação teórica para proteção de direitos autorais

Esta seção apresenta as principais ferramentas e mecanismos que podem ser empregados como base para propor um sistema de proteção de direitos autorais no ambiente de televisão digital. Inicialmente será apresentado o conceito de cifra simétrica, posteriormente os tipos de dispositivos criptográficos atualmente disponíveis para sistemas de acesso condicional e, finalmente, serão apresentados os conceitos e modelos para hierarquias de chaves lógicas.

2.4.2.1 Algoritmos de criptografia simétrica

Uma cifra simétrica é uma transformação matemática inversível cujo cálculo depende, no sentido direto e no sentido inverso, de uma mesma informação secreta (a chave). Desta maneira, é utilizada a mesma chave para cifrar e para decifrar a mensagem. Os principais algoritmos criptográficos simétricos são cifras de bloco – AES, DES e 3DES.

As cifras de bloco são algoritmos iterativos, ou seja, constituem-se de várias aplicações sucessivas de uma mesma transformação simples, dependente da chave. Nas cifras de bloco, a transformação efetuada para proteção do conteúdo opera em mensagens de tamanho fixo, sendo o tamanho dependente de cada algoritmo. Para aplicar as cifras de blocos em mensagens que não sejam múltiplas deste tamanho, são definidos modos de operação para extensão do algoritmo para outros tamanhos de mensagem.

O DES (*Data Encryption Standard*) foi originalmente proposto pela IBM e alterado pela NSA (*National Security Agency*), estabelecido como padrão governamental em 1977 e

apresentado oficialmente em 2004, tendo sido substituído pelo AES (*Advanced Encryption Standard*). O algoritmo DES utiliza a estrutura de Feistel, com blocos de 64 bits e chave de 56 bits. Como pode ser observado na Figura 10, a estrutura de Feistel considera o escalonamento de chaves linear (são utilizadas subchaves de 48 bits obtidas como subconjuntos da chave de 56 bits). Metade do bloco do dado claro é submetida à função F e somada à outra metade, fazendo esta iteração por diversas vezes.

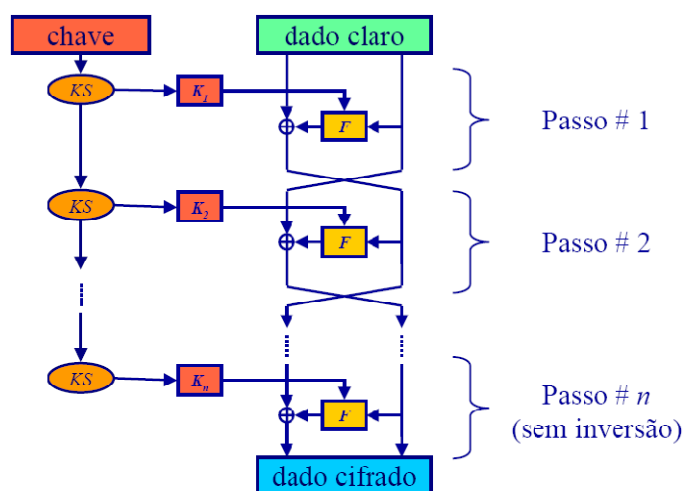


Figura 10. Estrutura de Feistel⁷

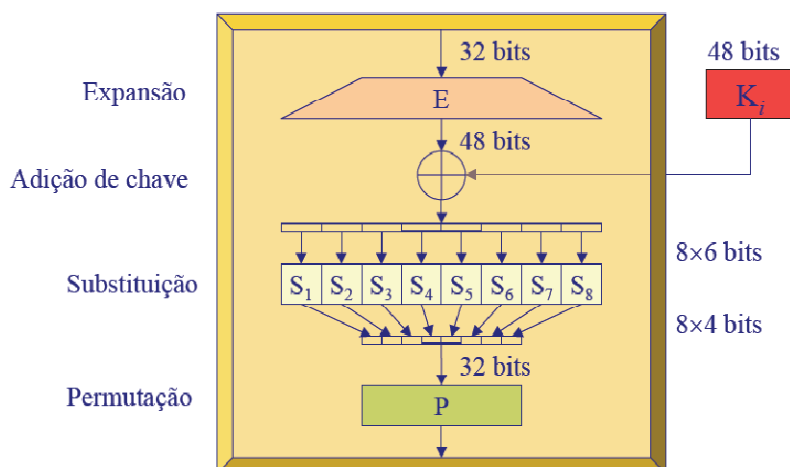


Figura 11. Função F da Estrutura de Feistel⁸

⁷ Ilustração obtida em apresentação realizada por Paulo Barreto em 2006 na disciplina PCS5734 oferecida pelo programa de mestrado da Escola Politécnica da USP.

A Figura 11 apresenta a função F que recebe a metade do bloco, 32 bits, e aplica uma expansão linear para 48 bits. Ao resultado da expansão é adicionada a subchave de 48 bits. Depois disso, é aplicada uma função de substituição que contrai o conteúdo para 32 bits novamente pelo mapeamento a partir de tabelas de conjuntos de seis bits em quatro bits. Finalmente, é realizada uma permutação dos valores obtidos nas tabelas, produzindo a saída de 32 bits.

O 3DES (*Triple Data Encryption Standard*) foi uma medida paliativa para aproveitar o legado DES, pela construção tripla: cifrar cada bloco três vezes, com três chaves distintas de 56 bits cada.

O AES tem estrutura simétrica e paralela, ele utiliza cifra iterativa, mas não a de Feistel. Ele utiliza a rede de substituição e permutação, conforme apresentado na Figura 12.

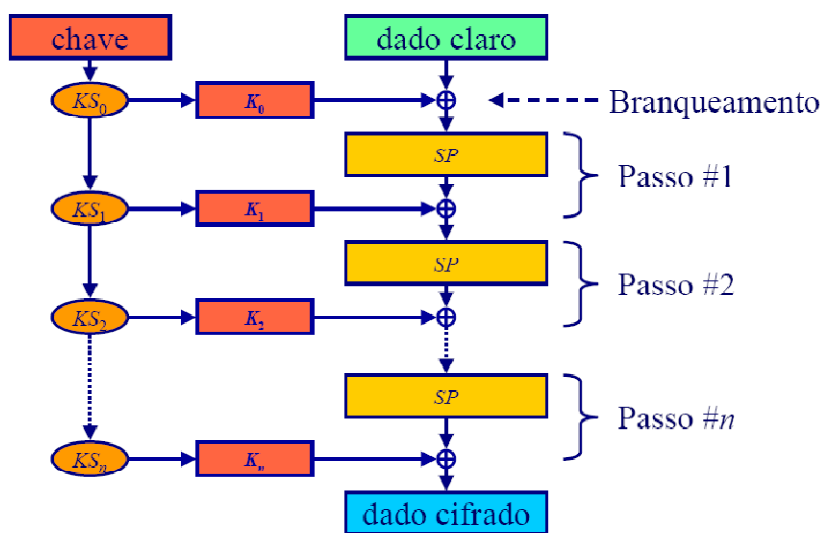


Figura 12. Rede de permutação e substituição.⁹

Os *bytes* da chave e do bloco de dados são organizados logicamente em forma de matrizes e lidos de maneira não direta (em *zig-zag*). Nos blocos de substituição e permutação (SP) quatro transformações são aplicadas, cada uma com sua própria finalidade:

⁸ Ilustração obtida em apresentação realizada por Paulo Barreto em 2006 na disciplina PCS5734 oferecida pelo programa de mestrado da Escola Politécnica da USP.

⁹ Idem

- *ByteSub*: não-linearidade.
- *ShiftRow*: difusão entre as colunas de dados.
- *MixColumn*: difusão dentro de cada coluna.
- *AddRoundKey*: aplicação da chave.

Em outubro de 2000, o NIST (*National Standards and Technology*) definiu o AES (*Advanced Encryption Standard*) como sucessor do DES (*Data Encryption Algorithm*), que foi o padrão de criptografia simétrica utilizado desde 1977. O AES tem boa eficiência de implementação, necessitando de pouca memória e permitindo implementação paralela; características importantes para soluções em *hardware* dedicado. Além disso, o AES é mais seguro do que o DES, apresentando como as suas duas principais vantagens: a utilização de componentes distintos para realização da cifra e da sua inversa e a não linearidade na expansão das chaves. Estas características praticamente eliminam a possibilidade de chaves fracas, semi-fracas ou equivalentes, como afirmado por Sanchez-Avilaf e Sanchez-Reillot (2001).

2.4.2.2 Dispositivos criptográficos

Normalmente, para o cenário de acesso condicional de televisão digital, pode-se dividir o mecanismo de processamento de recepção de conteúdo protegido em duas partes, uma responsável por decifrar o conteúdo protegido e outra por processar as informações de controle associadas. A Figura 13 ilustra as diferentes configurações dos módulos de acesso condicional em receptores, que podem conter parte deste processamento em *hardware* especializado ou não.

Como apresentado em Namba (2002), a configuração A, apresentada na figura, integra o módulo de decifração e de processamento de informações de controle na unidade receptora. Já a configuração B, inclui o módulo de decifração no receptor e o tratamento de informações de controle em um módulo de segurança removível, como um cartão criptográfico (*smartcard*). A configuração C mantém tanto o módulo responsável pelo decifrador como o

responsável pelo tratamento de informações de controle em um dispositivo removível.

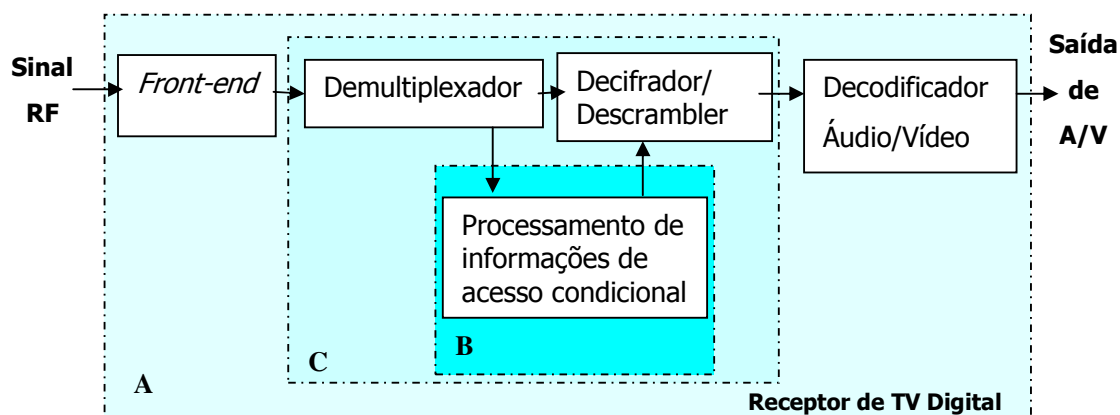


Figura 13. Configurações do módulo de acesso condicional em receptores.

Os cartões criptográficos são dispositivos eletrônicos com poder de processamento e armazenamento, possuindo processadores criptográficos dedicados com diferentes capacidades criptográficas (alguns possuem capacidade de criptografia apenas simétrica, outros assimétricas), diferentes capacidades de armazenamento, dentre outros parâmetros. Os cartões criptográficos são especificados pelas normas ISO/IEC 7816 e ISO/IEC 7810.

A norma ISO/IEC 7816-4 trata das questões de segurança na comunicação entre o cartão criptográfico e o seu leitor. Entre os tópicos abordados nesta parte da norma são definidos os pares de comando e resposta na interface, métodos para recuperar informações do cartão e métodos para garantir a segurança na troca de mensagens. Apesar dos *smartcards* serem desenvolvidos para garantir a sua integridade e a segurança das informações armazenadas, existe maneiras de recuperar informações indevidas deste tipo de cartão. Uma das técnicas empregadas é a utilização de análise da energia consumida pelo cartão. Realizando medidas das correntes necessárias para dadas operações e a sua variação no tempo, é possível descobrir as chaves secretas contidas no cartão. Outro tipo de ataque é realizado pelo acesso físico ao processador interno do cartão criptográfico e pela utilização de *softwares* de desmontagem (*disassembly*), que recuperam o *software* programado para executar no cartão.

Um exemplo da configuração C é a interface padronizada como CI (*Common Interface*). Os terminais de acesso do padrão DVB a utilizam para conectar cartões que fazem o processamento do acesso condicional por meio de um módulo externo, denominado Módulo

de Acesso Condicional (CAM – *Conditional Access Module*). A CI, especificada em EN 50221 (1997), possui duas interfaces lógicas: a primeira é uma interface de TS MPEG-2, que permite que o fluxo de dados trafegue nos dois sentidos, e a segunda é uma interface de controle, através da qual o terminal envia comandos ao módulo. A Figura 14 ilustra esta interface sendo utilizada para conectar um módulo de acesso condicional.

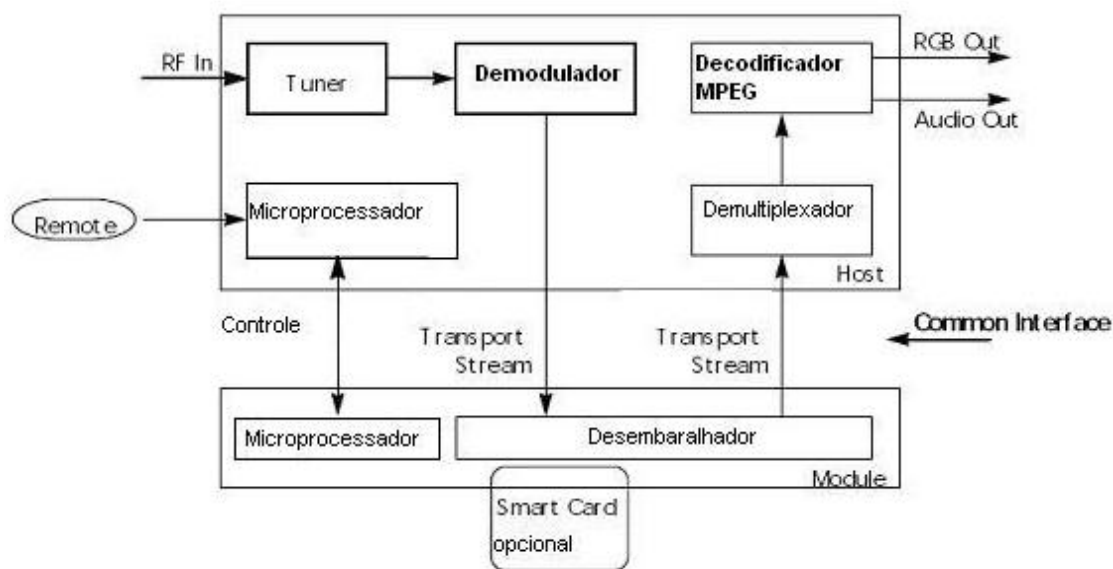


Figura 14. Diagrama da CI

Em caso de quebra do sistema de segurança, a configuração A requer a troca de todo o equipamento. Já a configuração B, pode atualizar o sistema de segurança substituindo o módulo removível dos receptores. Esta configuração, B, não permite a atualização do sistema de criptografia do conteúdo, mas permite a troca da chave mestra, do protocolo de comunicação entre cartão e receptor, do algoritmo de criptografia e do formato das mensagens de troca de chaves. Este tipo de solução, configuração B, tem sido adotado em diversos sistemas, podem ser citados o BskyB na Europa e a DirecTV nos EUA. A configuração C permite que o sistema completo de DRM seja atualizado.

O impacto das soluções no custo final é inversamente proporcional à flexibilidade oferecida. O acréscimo de módulos removíveis encarece o dispositivo por um aumento de complexidade física do sistema. Já o aumento de custo alternando entre a configuração B e C dá-se devido à necessidade de utilizar uma interface de alta velocidade na configuração C, para tráfego de MPEG-2 TS (20 Mbps), frente a uma de baixa velocidade na solução B, apenas para tráfego de mensagens.

Já em relação à segurança de cada uma destas soluções, tanto a opção de uso de cartão criptográfico como de módulo removível, configurações B e C, estão suscetíveis a ataques na comunicação entre cartão criptográfico ou módulo e receptor. Já a configuração A, por possuir o hardware integrado, está mais suscetível a ataques por software.

No cenário de televisão paga, quando há necessidade de atualização do sistema de DRM, as próprias operadoras de TV paga trocam os receptores ou os cartões criptográficos do seu parque de assinantes. Isto porque são proprietárias dos receptores de TV e o interesse em proteger o conteúdo e a programação é da própria operadora. Já no caso da TV aberta, os receptores são adquiridos diretamente pelos telespectadores, que não são os interessados na proteção do conteúdo. Por isso, na necessidade de atualização do sistema de DRM tem-se um impasse, pois os usuários não teriam interesse em realizar um investimento para proteção de um bem da emissora (conteúdo) e as emissoras de TV não teriam interesse em realizar investimento para atualização de um bem que não é dela (receptor).

2.4.2.3 Hierarquia lógica de chaves

A hierarquia lógica de chaves é um método de distribuição de mensagens de licenças, que busca facilitar a gerência de mensagens pelo agrupamento destinatários em diversos níveis. Existem muitas alternativas de esquemas de hierarquia de chaves. Dois exemplos de estratégias de distribuição de chaves são de tempo real e *batch*, como apresentado por Huang e Mishra (2003) e Li e Zhao (2004). Estas opções podem ser selecionadas e adotadas isoladamente ou adotadas e depois substituídas pelo servidor de gerenciamento de chaves, desde que os receptores possam lidar com os quatro tipos de chaves (Ks, Kw, Kg e Km).

A Figura 15 apresenta um exemplo de hierarquia lógica de chaves, LKH (*Logic Key Hierarchy*). A simbologia utilizada é: Ks é a chave criptográfica utilizada para cifrar o conteúdo audiovisual, Kw é a chave de trabalho utilizada para cifrar as mensagens utilizadas para atualização das chaves Ks e Km é a chave mestra, que é única para cada receptor e não atualizável. A LKH introduz chaves de grupo, Kg, utilizadas para reduzir o custo de atualização de chaves. O símbolo R representa um receptor de TV digital.

De acordo com a Figura 15, uma atualização de chave de trabalho (K_w) em todos os terminais requereria envio de três mensagens pela emissora, cada uma cifrada com uma chave de trabalho: $\langle \{kw\}kg_a; \{kw\}kg_b; \{kw\}kg_c \rangle$. Sem as chaves de grupos, para este conjunto de nove receptores, seria necessário enviar nove mensagens para atualização da chave K_w , cada uma cifrada com a chave mestra (K_m) de cada receptor: $\langle \{kw\}km_1; \{kw\}km_2; \{kw\}km_3; \{kw\}km_4; \{kw\}km_5; \{kw\}km_6 \rangle$. Utilizando LKH é possível também excluir ou incluir novos membros no grupo com menos mensagens de distribuição de chaves.

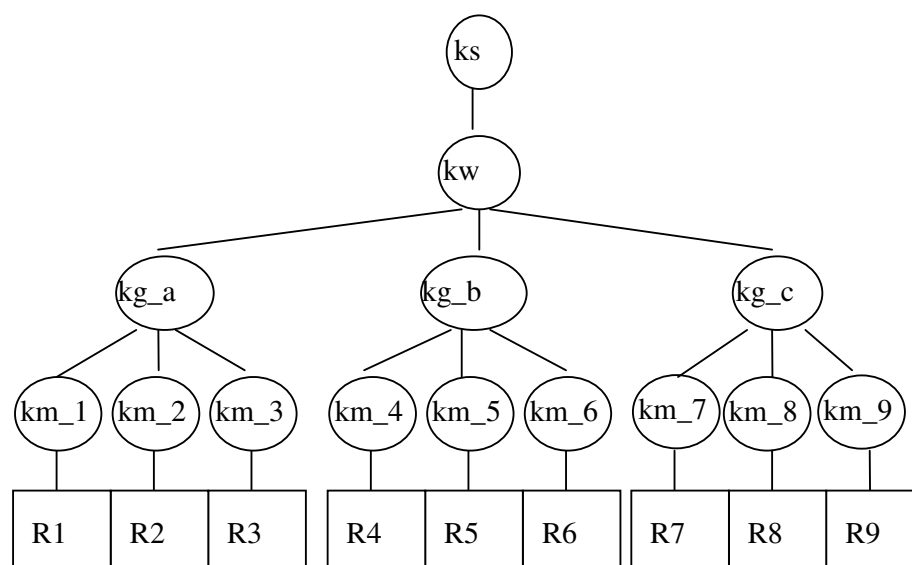


Figura 15. Exemplo de hierarquia lógica de chaves

O uso de LKH reduz a necessidade de envio de mensagens de $O(N)$ para $O(\log_d N)$, onde N é o tamanho do grupo e d é o grau da árvore onde está a chave a ser substituída, Snoeyink e Varghese (2001).

2.4.3 Sistemas de proteção de direitos autorais

Esta seção apresentará alguns sistemas de proteção de direitos autorais existentes

atualmente. Inicialmente serão apresentados, em maiores detalhes, os mecanismos presentes no MPEG-2 camada de sistemas para dar apoio à implementação de um mecanismo de acesso condicional, fundamental ao funcionamento de sistemas de proteção de direitos autorais.

Em seguida, serão apresentados como estudos de caso alguns sistemas de DRM existentes. O sistema mais relevante aqui apresentado será o sistema de proteção de direitos autorais utilizado no Japão, o ISDB-T, já que o sistema brasileiro é baseado nele. Além disso, serão discutidos o sistema em uso para TV digital na Europa, o DVB CAS – Sistema de Acesso Condicional do DVB –, e um projeto com enfoque em sistemas abertos e em interoperabilidade, o DReaM.

2.4.3.1 Acesso condicional no padrão MPEG-2 Sistemas

A família MPEG aborda em vários dos seus padrões as questões de proteção de direitos autorais, principalmente no MPEG-21, MPEG-7 e MPEG-2. Todos os sistemas de televisão digital terrestre em uso hoje, inclusive o sistema brasileiro, utilizam o MPEG-2 Sistemas como especificação do seu fluxo de dados (*transport stream*), por isso, muito relevante para as discussões de segurança do conteúdo desta dissertação.

A especificação do MPEG-2 Sistemas, por ISO/IEC13818-1 (2000), define como combinar um ou mais ES (*elementary streams*) – fluxos de áudio, vídeo ou dados – em um único fluxo de transporte (TS - *transport stream*). Em outras palavras, esta norma define a sintaxe necessária e suficiente para sincronizar a decodificação e a apresentação dos fluxos de áudio e vídeo.

A sintaxe prevê também suporte a cifra de conteúdo para o uso de mecanismo de acesso condicional, apesar de não definir um sistema de acesso condicional. Como cifra é considerada a alteração da mensagem original de maneira a não permitir a recuperação não autorizada da informação. O algoritmo de cifragem aplicado é definido pelo sistema de acesso condicional específico.

As especificações referentes ao acesso condicional no MPEG-2 Sistemas prevêem mensagens de controle, tabelas e descritores. São definidos dois tipos de mensagens: uma

denominada ECM (*Entitlement Control Message* – Mensagem de Controle de Direitos) e outra denominada EMM (*Entitlement Management Message* – Mensagem de Gerenciamento de Direitos). As mensagens ECM enviam parâmetros de controle do TS. As mensagens EMM especificam níveis de autorização e devem ser endereçadas a receptores ou grupos de receptores. As tabelas relacionadas são a CAT (*Conditional Access Table*) e a PMT (*Program Map Table*), como explicado adiante. O descritor definido para acesso condicional é o descritor de acesso condicional (*CA_descriptor*).

Um TS consiste de um ou mais programas. Um programa consiste de um conjunto de arquivos de áudio, vídeo e dados. Este material é comprimido e serializado separadamente, formando os ES de áudio, vídeo e dados. Os ES são inseridos em pacotes de TS. O TS é composto por uma seqüência de pacotes de TS. Os pacotes de TS têm comprimento fixo de 188 bytes, incluindo cabeçalho e área de carga útil. O cabeçalho possui um identificador de pacotes, o PID (*Packet Identifier*) que informa por meio das tabelas de informações específicas de serviços, tabelas PSI (*Program and Service Information*), a informação que está contida em cada pacote.

Segundo a norma MPEG-2, a área útil do TS (*payload*) pode ser cifrada pelo sistema de acesso condicional quando contiver os componentes de um programa, mas não quando contiver tabelas PSI. A cifra pode também ser aplicada no nível do ES. O cabeçalho do pacote do TS possui um campo de dois bits que indica se a sua área útil está cifrada ou não (“00” significa que os dados estão claros, os demais valores devem ser definidos pelo sistema de acesso condicional).

O MPEG-2 Sistemas define quatro tabelas PSI, são elas:

- PMT (*Program Map Table* – Tabela de mapeamento de programas): é enviada uma para cada programa transmitido no TS. Informa quais os componentes do programa e o número do PID dos pacotes que contém cada um destes componentes. Os componentes podem ser: áudio, vídeo, mensagens ECM e dados associados.
- PAT (*Program Allocation Table* – Tabela de Alocação de Programas): cada TS possui uma única PAT, que informa o número de programas do TS e o PID dos pacotes que contêm tabelas PMT.
- CAT (*Conditional Access Table* – Tabela de Acesso Condicional): está presente quando é empregado acesso condicional aos componentes dos programas do TS. Informa a identificação do sistema de acesso condicional ao qual se refere além de

informar o PID no qual a mensagem EMM pode ser encontrada.

- NIT (*Network Information Table* – Tabela de Informação de Rede): deve informar dados da rede, como nome da emissora, por exemplo. A sua existência é especificada na norma MPEG-2 sistemas, mas não o seu conteúdo.

O descritor de acesso condicional (*CA_descriptor*) é responsável por informar o PID onde podem ser acessadas as mensagens ECM e EMM, além do número de identificação do sistema de acesso condicional em uso. Descritores são segmentos de tabelas PSI que possuem sintaxe separada para simplificar a sua repetição dentro de uma tabela ou envio simultâneo. O descritor de acesso condicional é enviado dentro da área de dados da tabela CAT (envio de EMM) ou da PMT (envio de ECM). Estando presente sempre que algum componente do TS esteja cifrado.

2.4.3.2 DVB CAS – Sistema de Acesso Condicional do DVB

Segundo a ETSI ETR 289 (1995), no DVB, o acesso condicional (CA) é utilizado para distribuição de TV por assinatura e serviços de *Pay-Per-View*. Como o DVB utiliza o seu *transport stream* conforme a especificação do MPEG-2 sistemas, o seu sistema de acesso condicional é baseado nele. O DVB CAS permite que a cifra de conteúdo seja realizada tanto no nível do pacote de TS, como no nível do pacote de ES. No DVB CAS são enviadas em cada ECM duas chaves, uma chave par e uma chave ímpar e o cabeçalho do pacote cifrado informa pelo *scrambling control field* qual chave deve ser utilizada para a decifração do pacote.

No DVB o sistema de acesso condicional não é padronizado, sendo especificado apenas um algoritmo comum para criptografia do conteúdo. O recebimento e processamento das mensagens ECM e EMM podem ser realizados tanto em um cartão móvel como embarcados no receptor. Segundo a ETSI TR 102 035 (2002), o protocolo do sistema de acesso condicional do DVB pode seguir dois sistemas: o *Simulcrypt* ou o *Multicrypt*.

O sistema DVB-*Simulcrypt* é baseado no conceito de compartilhamento do método de cifra e decifração do conteúdo. O *Simulcrypt* permite que os terminais de acesso utilizem

sistemas de acesso condicional diferentes. As várias ECMs e EMMs requeridas por cada sistema de acesso condicional são transmitidas simultaneamente e cada terminal de acesso utiliza as ECMs e EMMs apropriadas. O *Simulcrypt* não consome banda extra para transmissão dos dados do sistema de acesso condicional.

O sistema DVB-*Multicrypt* permite que múltiplos sistemas de acesso condicional sejam utilizados em um terminal de acesso, o que permite o acesso a provedores diferentes. Isto é feito através da inclusão de módulos durante o processo de fabricação do componente central do receptor ou utilizando a DVB-CI (*Common Interface*). A DVB-CI é uma recomendação do DVB para os receptores. Na DVB-CI, cartões PCMCIA (*Personal Computer Memory Card International Association*) fornecem os módulos do sistema de acesso condicional para os receptores. Um fator a ser considerado é o custo dos cartões que é elevado.

2.4.3.3 Sistema de proteção a direitos autorais no ISDB-T

Esta seção apresenta o sistema de proteção de direitos autorais proposto pelo sistema de televisão digital em uso no Japão, aqui referenciado como ARIB (*Association of Radio Industries and Businesses*), o órgão responsável por esta padronização.

O sistema de proteção de direitos autorais do ARIB define um protocolo de restrições de uso do conteúdo e de proteção de interfaces de saída, além de empregar transmissão cifrada de TS. O protocolo de restrições de uso tem por objetivo determinar as regras de contrato sob as quais a transmissão do conteúdo está submetida. A proteção das interfaces de saída do terminal de acesso tem como objetivo repassar as regras de uso definidas no protocolo de restrição de uso aos dispositivos que recebam este conteúdo do terminal de acesso. Já o envio do TS protegido tem por objetivo restringir o acesso ao conteúdo, garantindo a obediência às regras de uso. (Yoshimura, T. (2006))

A restrição de acesso ao conteúdo proveniente da transmissão de TV aberta pode parecer contraditória, já que este conteúdo deveria ser acessível a todos pelo seu próprio conceito e regulamentação. A proteção do TS por meio de cifra é utilizada no sistema ARIB

como garantia de atendimento às normas do sistema de DRM por parte dos dispositivos receptores. Todo terminal de acesso aderente às regras de proteção de direito autorais da norma recebem o direito de exibir o conteúdo recebido, não havendo necessidade de pagamento de qualquer taxa para acesso.

O sistema de proteção do *TS* proposto no sistema ARIB é baseado na recomendação da ITU-R para sistemas de acesso condicional para a radiodifusão. O sistema de gerenciamento de direitos digitais do ARIB utiliza uma estrutura de três chaves simétricas: chave mestra, K_m ; chave de trabalho, K_w ; e chave de cifra, K_s . (Namba (2002), Yoshimura (2006), ARIB STD-B25 (2006)).

A chave de cifra, K_s , é utilizada para proteger o conteúdo transmitido pela emissora. Esta chave é alterada frequentemente, com período na ordem de segundos, e é transmitida em um pacote cifrado por outra chave, a chave de trabalho K_w . Tanto a chave K_s como a K_w são comuns para todos os receptores para a recepção de um determinado conteúdo.

A troca da chave K_w é realizada em períodos relativamente longos, na ordem de meses, e a sua transmissão é realizada através de pacotes protegidos por uma terceira chave, a chave K_m . A chave K_m , chave mestra, é única por receptor e é mantida em um cartão criptográfico (*smartcard* ou *IC Card*). A chave K_m é fixa, não sendo passível de atualização.

A Figura 16 apresenta o sistema de acesso condicional utilizado no ARIB. O módulo de segurança representa o cartão criptográfico. Tanto a chave K_w , como a chave K_m não são disponibilizadas ao receptor, sendo armazenadas de modo seguro no cartão. Apenas as chaves K_s são exportadas do cartão para o terminal de acesso.

O protocolo utilizado para expressar as condições de uso do conteúdo utilizado no sistema japonês é enviado nas tabelas PSI por meio de descritores específicos. Os descritores são subtabelas com um objetivo específico, definidos para o ISDB em ARIB STD-B25 (2006), ARIB STD-B21 (2007). Os descritores utilizados para informar as regras de uso do ISDB são: **descritor de acesso condicional**, **descritor de controle de cópias** e **descritor de disponibilidade de conteúdo**.

A norma ARIB utiliza o descritor de **acesso condicional**, definido no MPEG-2, que indica se o conteúdo é protegido e, neste caso, onde encontrar os pacotes com as atualizações de chaves. As mensagens as atualizações de chaves são as definidas também no MPEG-2, a ECM e a EMM, como apresentado na Figura 16.

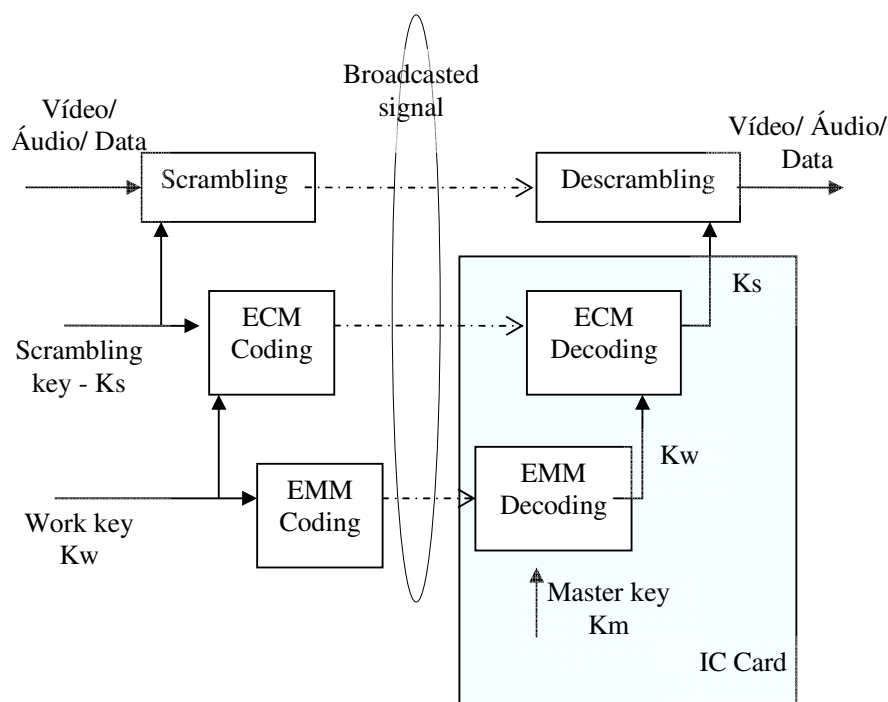


Figura 16. Configuração de um sistema de acesso condicional.

O sistema determina também a existência de um descritor de **controle de cópias** que controla as cópias de conteúdo tanto em formato digital como analógico. O controle de cópias digitais determina se as cópias são liberadas, se são proibidas ou permitidas apenas para a primeira geração (restringe a possibilidade de realização de cópia a partir de um conteúdo que já seja uma cópia). Já o de cópias analógicas informa apenas se elas são liberadas ou proibidas.

Além deste tipo de controle, há ainda, um descritor que determina se é possível realizar acúmulo de conteúdo no tempo ou não, o descritor de **disponibilidade do conteúdo**. Podendo realizar o acúmulo, ele determina se o conteúdo armazenado pode ser reproduzido por um período restrito ou irrestrito. O protocolo permite especificar um período de retenção, variando de 1h30min até uma semana.

O sistema permite ainda o uso de um mecanismo de revogação de cartões criptográficos, caso haja suspeita de falha de segurança na caixa, permitindo a correção de uma falha detectada. Este mecanismo é baseado na troca das chaves K_w , todos os terminais de acesso receberiam as novas chaves K_w , menos os terminais de acesso não revogados. Apesar disso, a revogação é complicada operacionalmente, pois requer o envio de mensagens

a todos os terminais válidos. A troca de chaves K_w é mais utilizada para evitar a entrada no mercado de receptores em não conformidade com a norma de DRM, sendo pouco viável a revogação dos receptores já existentes, para o sistema ISDB-T.

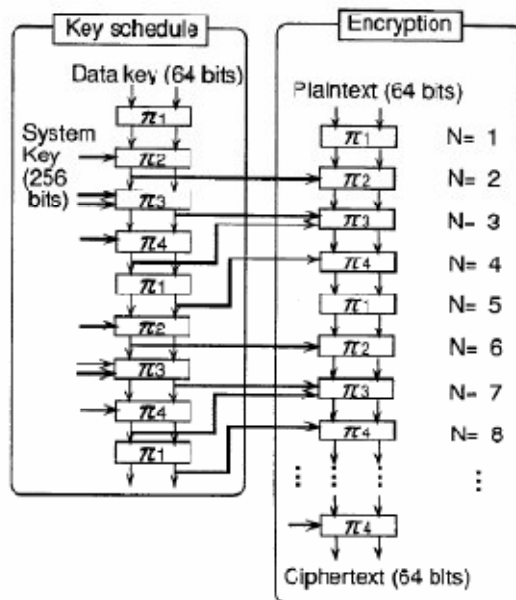


Figura 17. Algoritmo Multi-2. Fonte: Ougi ET AL. (2006)

O MULTI-2, patenteado por Ougi ET AL (2006), é o algoritmo criptográfico utilizado no ARIB. Ele é uma cifra simétrica, de Feistel, que utiliza uma chave de oito bytes, similar ao DES (*Data Encryption Standard*). A chave passa por uma expansão, passando para o comprimento de 64 bits, conforme Figura 18. O algoritmo é composto por várias rotações com blocos de entrada de 64 bits, conforme apresentado na Figura 17. Os dados de entrada passam por uma caixa de substituição e por quatro diferentes funções.

Devido à necessidade de transmissão de conteúdo entre dispositivos – como aparelhos de DVD, computadores e televisores – é importante garantir que o dispositivo que está recebendo o conteúdo do terminal de acesso também seja capaz de manter as regras de uso, respeitando todos os requisitos de distribuição de conteúdo assumidos. Sendo assim, protocolos foram desenvolvidos com a finalidade de garantir que apenas dispositivos que estejam certificados possam ter acesso ao conteúdo sendo transmitido. A ARIB utiliza os protocolos DTCP (*Digital Transmission Content Protection*) (Hitashi ET AL (1998)), para comunicação ponto a ponto entre dispositivos conectados por interface *firewire*, o HDCP (*High-Bandwidth Digital Content Protection*) (*Digital Content Protection LLC* (2006)) para

proteção de conteúdo áudio-visual em interfaces digitais HDMI. Já para as interfaces analógicas, são utilizados sistemas bastante difundidos: o APS (*Macrovision Analog Protection System*) para a interface de vídeo composto, CGSM-A (*Copy Generation Management System – Analog*) para a interface de vídeo componente e SCMS (*Serial Copy Management System*) para a interface de áudio digital SPDIF (*Sony/Philips Digital Interconnect Format*).

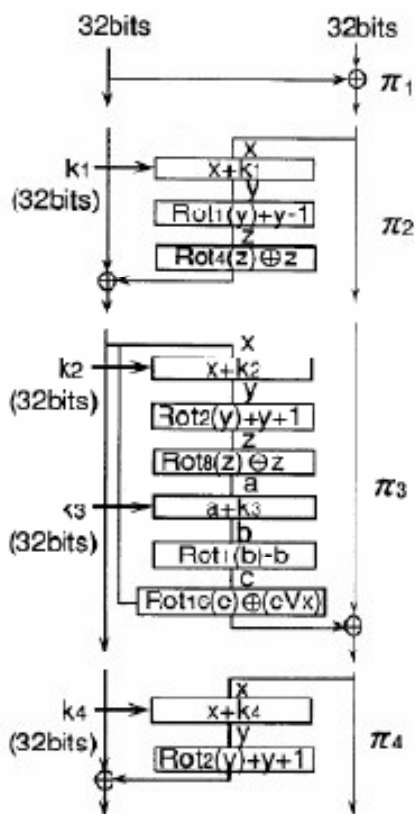


Figura 18. Geração de chaves expandida do Multi-2. Fonte: Ougi ET AL. (2006).

As interfaces digitais supracitadas possuem mecanismos de propagação das regras de uso do conteúdo, é possível determinar a saída tendo possibilidade de cópia livremente, cópias apenas de primeira geração, ou cópia proibida. Estas funcionalidades permitem ao sistema propagar as regras de uso em rede doméstica, por exemplo.

2.4.3.4 DReaM uma solução de DRM livre de *royalties*

O DReaM é uma iniciativa do *Sun Labs* para desenvolver uma solução de DRM baseada em padrões abertos livre de *royalties*. A visão da Sun é de ter um sistema de DRM não apenas para evitar cópias sem custo, mas também para prover serviços, não apenas de entretenimento, mas incluindo a categoria de negócios e vida. Na categoria de negócios, o DRM poderia prover controle de acesso a documentos ou gerar serviços como o de treinamento à distância sob demanda, outro exemplo seria o acesso a informações de pacientes em um sistema médico. Já na categoria vida, o DRM pode ser utilizado como meio de controle de acesso a câmeras de vigilância, por exemplo.

O DReaM consegue flexibilidade pelo desacoplamento das várias ferramentas dos sistemas de DRM (autenticação, licenciamento, descrição de direitos e tecnologias de proteção) e permite que o sistema funcione à base da identificação do indivíduo, não apenas da autenticação do dispositivo. As ferramentas propostas são selecionadas para uso de acordo com o contexto, formando sistemas dinâmicos de proteção a direitos autorais (Fernando, Jacobs e Swaminathan, 2008).

O sistema proposto pela Sun possui uma abrangência maior do que os do sistema de DRM para um sistema de televisão digital aberta:

- Trabalhar com qualquer tipo de conteúdo e com qualquer formato de arquivos e CODECs.
- Controlar o acesso em qualquer meio, como por exemplo: TV terrestre, satélite, disco de armazenamento.
- Dar suporte a vários modelos de negócios, incluindo conteúdo pago, livre, entre outros.
- Uso de padrões abertos e livres de *royalties*.

O projeto DReaM define o DReaM-CAS (*DReaM Conditional Access System*) e o DReaM-MMI (*DReaM Mother May I*) como soluções abertas, deixando livres para definição proprietária: o formato do conteúdo, gerenciamento de chaves e distribuição. O DReaM-MMI é um protocolo de negociação de direitos, diferentemente dos protocolos usuais que informam os direitos, no DReaM ocorre uma negociação entre o cliente e o servidor de licenças.

A Figura 19 apresenta os elementos considerados no projeto DReaM. Os blocos em coloração verde são os utilizados para o DReaM CAS, que considera um cenário de comunicação unidirecional. Já os blocos em cor azul são relacionados a um ambiente bi-direcional com o uso do DReaM MMI. O protocolo MMI é realizado entre o *Disintermediating Agent* do lado do cliente e o *Licensing Conductor* do lado do servidor. Com a negociação das ferramentas e permissões para o conteúdo, o *Licensing Conductor* gerencia os demais blocos do cenário para prover licença e conteúdo nos formatos adequados para o cliente.

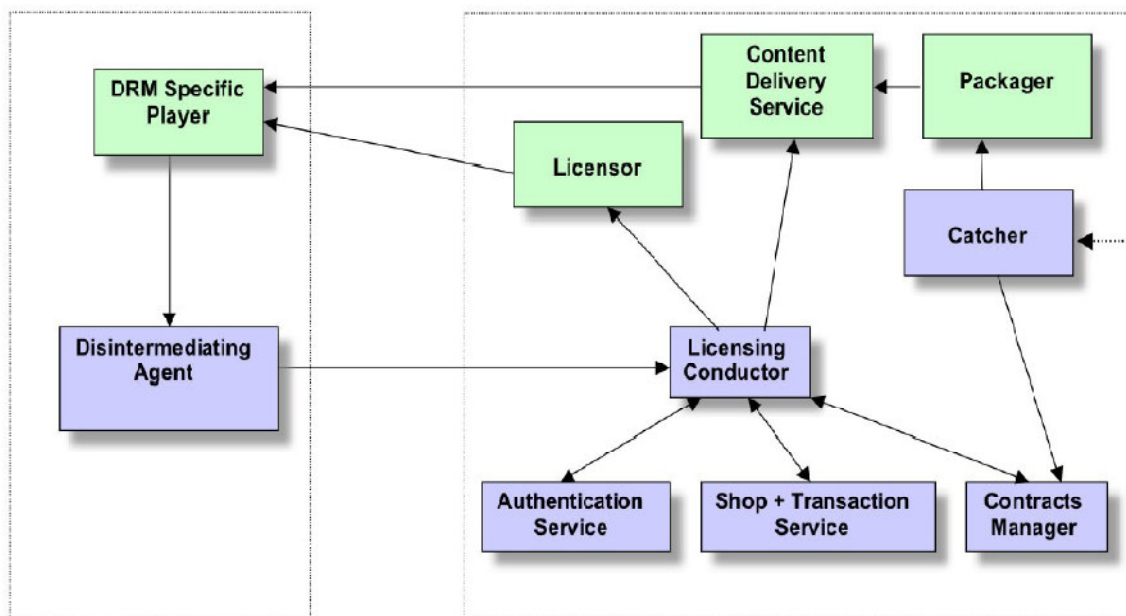


Figura 19. Arquitetura do DReaM. Fonte: Fernando, Jacobs e Swaminathan (2008)

O DReaM possibilita a interoperabilidade com vários padrões de DRM, entre eles:

- Open Mobility Alliance (OMA);
- Internet Streaming Media Alliance (ISMA);
- Microsoft Windows Media DRM;
- CORAL.

O DReaM utiliza um sistema de acesso condicional similar ao utilizado no ISDB-T. A área útil (*payload*) dos pacotes de *transport stream* é cifrada, deixando o cabeçalho dos pacotes em dados claros.

São utilizados apenas três níveis de chaves, K_s , K_w e K_m , como apresentado na

Figura 16, com mensagens ECM e EMM para distribuição de chaves. Uma diferença do DReaM é o uso da chave K_m assimétrica e apenas a K_s e a K_w são simétricas. A chave K_m utiliza algoritmo de criptografia assimétrica RCA, e as chaves K_s e K_w utilizam algoritmo de criptografia AES com chave de 128-bits.

O sistema de acesso condicional do DReaM não define proteção de interfaces de saída.

2.5 Autenticação de aplicativos

Nesta seção serão apresentados os principais pontos do levantamento do estado da arte em relação à autenticação de aplicativos para o cenário da televisão digital, fundamental para a agregação de serviços avançados ao sistema. Inicialmente será apresentada a fundamentação teórica, descrevendo mecanismos e ferramentas necessários à autenticação de aplicativos, em seguida serão apresentados sistemas de autenticação de aplicativos disponíveis atualmente.

2.5.1 Ferramentas e mecanismos para a autenticação de aplicativos

Esta seção apresenta as principais ferramentas e mecanismos que podem ser empregados para executar a autenticação de aplicativos no ambiente de televisão digital. Inicialmente será apresentado o código *hash*, utilizado na garantia da integridade na troca de dados, em seguida será apresentado o conceito de chaves públicas, assinatura digital, ASN.1, certificados de atributos, certificados de identidade lista de certificados revogados e mensagens criptográficas.

2.5.1.1 Código *Hash*

As funções *hash* são utilizadas para a geração de um código que é um resumo de um arquivo utilizado como fonte. Os algoritmos *hash* devem possuir o menor número de colisões possível e serem irreversíveis. Uma aplicação comum para o uso de códigos *hash* é na verificação de senhas de acesso. O método de verificação é, então, feito pela comparação dos dois cálculos de *hash*, um código *hash* previamente armazenado na base de dados do sistema, e o outro calculado sobre a senha informada na tentativa de acesso. O código *hash* é também bastante utilizado para conferir a integridade de conteúdos.

O MD5 (*Message-Digest algorithm 5*) é um algoritmo de *hash* de 128 bits unidirecional desenvolvido pela RSA *Data Security*, Inc., descrito na RFC 1321, por Rivest (1992), e muito utilizado por softwares com protocolo ponto-a-ponto (ou P2P (*Peer-to-Peer*), em inglês), verificação de integridade e acesso a sistemas (*login*). Já existem meios conhecidos e relativamente simples para gerar colisões com o MD5, por isso considerado obsoleto¹⁰.

A sigla SHA (*Secure Hash Algorithm*) refere-se a uma família de funções *hash* desenvolvida pela NSA dos Estados Unidos e publicada pelo NIST (*National Institute of Standards and Technology*) como o padrão americano para assinaturas digitais. Foram desenvolvidos os padrões SHA-0, SHA-1 e SHA-2. O SHA-0 e SHA-1 possuem resumo criptográfico de 160 bits. O SHA-2, publicado em FIPS PUB 180-2 (2002), possui variantes com tamanho de resumo igual ao valor que segue a sigla da família: SHA-224, SHA-256, SHA-384 e SHA-512. SHA-1 e SHA-2.

O SHA-1 é empregado em muitas aplicações de protocolos de segurança, como o TLS, SSL, SSH e IPsec. Segundo análise criptográfica, a segurança do SHA-1 já está comprometida, como apresentado por Wang ET AL (2005). Apesar de não haver ataques relatados para o SHA-2, por ser similar ao SHA-1, ele também está ameaçado. Por isso, nos EUA já foi iniciado o processo de definição de um novo algoritmo para publicação em 2012.

¹⁰ Informações obtidas em apresentação realizada por Paulo Barreto em 2006 na disciplina PCS5734 oferecida pelo programa de mestrado da Escola Politécnica da USP.

2.5.1.2 Chaves públicas

O par de chaves públicas tem a característica de que quando uma das chaves do par é utilizada para cifrar uma mensagem apenas a outra chave do par pode ser utilizada para decifrá-la e *vice versa*.

O **RSA** é um algoritmo de cifra de dados, que deve o seu nome a três professores do Instituto MIT (fundadores da empresa *RSA Data Security, Inc.*), Ron **R**ivest, Adi **S**hamir e Len **A**dleman, que inventaram este algoritmo em 1977. O algoritmo fundamenta-se em teorias clássicas dos números. O RSA baseia-se no fato de que a fatoração do produto de dois números primos de grandes dimensões (com cerca de 100 dígitos) é computacionalmente complexa. Não foi encontrado registro de quebras deste algoritmo. O RSA pode ser aplicado para operações de cifra e de assinatura digital.

O DSA (*Digital Signature Algorithm*) é o algoritmo utilizado pelo governo americano para assinaturas digitais. Foi proposto pelo NIST em 1991 para uso com o padrão DSS (*Digital Signature Standard*), especificado no FIPS 186, adotado em 1993. A última versão revisada deste algoritmo foi publicada em 2000 como FIPS 186-2. O DSA possui a sua base matemática no problema de logaritmo discreto. O nível de segurança obtido é muito semelhante ao RSA para chaves de tamanhos semelhantes. Com o RSA, leva-se mais tempo para assinar uma mensagem do que para verificar uma assinatura. Com o DSA, as operações de assinatura e de verificação levam a mesma quantia de tempo.

O ECDSA (*Elliptic Curve DSA*) é uma variante do DSA, que opera sobre curvas elípticas. Para a mesma segurança dada pelo algoritmo DSA ou RSA, o tamanho da chave necessária é muito menor, mas o tamanho da mensagem gerada é muito maior.

2.5.1.3 Assinatura digital

A assinatura digital foi desenvolvida para garantir a fonte de uma mensagem em

ambiente digital. Utilizando chaves públicas pode-se garantir a origem do pacote, já que se uma das chaves do par for utilizada para realizar a cifra do pacote, apenas a outra chave do par seria capaz de decifrá-la. Desta maneira, uma chave é mantida em sigilo, a chave privada, e a outra é divulgada, a chave pública. As mensagens que forem enviadas cifradas pela chave privada só poderão ser abertas pelo destinatário se ele utilizar a chave pública do remetente.

A assinatura digital é obtida através do cálculo do código *hash* da mensagem e da cifra sobre o valor do código *hash* obtido utilizando a chave privada da entidade remetente. Desta maneira, para conferir a assinatura seria necessária a chave pública da entidade remetente, para recuperar o *hash* e verificar se a mensagem recebida foi enviada de fato pela entidade remetente. Os processos que utilizam criptografia assimétrica, entre eles a assinatura digital, podem se valer de certificados digitais para distribuírem as chaves públicas. A assinatura digital permite a identificação do autor, através do uso de certificado de identidade, que contém a chave pública requerida e garante que ela pertence de fato à entidade esperada.

2.5.1.4 A sintaxe ASN.1

Em telecomunicações e em redes de computadores a sintaxe ASN.1 (*Abstract Syntax Notation One*) é frequentemente utilizada. Esta sintaxe é definida em ISO/IEC 8824 (2002). Ela define uma notação que descreve as regras e a estrutura de dados para representação, codificação, transmissão e decodificação, de forma a remover ambigüidades.

2.5.1.5 Certificado de identidade

O certificado de identidade, também denominado certificado digital, é definido pela ITU-T X.509 (2005) e utiliza sintaxe ASN.1 DER. Ele tem como função principal atribuir uma chave pública (para conferência de assinaturas) a uma entidade. Além disso, ele permite

um encadeamento de certificados, pois é assinado, assim requerendo uma nova conferência de assinatura, até alcançar um certificado que seja considerado confiável, o certificado raiz.

Ele possui uma série de campos necessários para o seu correto funcionamento. Estes campos informam: quais os privilégios que o detentor do certificado possui (campo atributos), identificação do detentor do certificado (*holder*), identificação do emissor do certificado (*issuer*), assinatura do certificado pelo emissor e informações sobre o certificado (versão, validade, identificação). A sintaxe de cada campo pode ser consultada em ITU-T X.509 (2005).

O certificado de identidade possui um perfil para a Internet definido pela RFC 2459 por Housley ET AL (1999). Este perfil é compatível com o certificado definido na ITU-T X.509 (2005) mas é mais restritivo, determinando o uso de campos opcionais e valores de campos com conteúdo indefinido na especificação original.

Neste capítulo não será apresentado um detalhamento dos campos das especificações de Housley ET AL (1999) nem de ITU-T X.509 (2005), que podem ser consultados nestas referências que estão disponíveis sem custo.

Enquanto os certificados de identidade vêm sendo amplamente utilizados – o protocolo mais comum para segurança na *Internet* é o SSL (*Secure Socket Layer*), Frier ET AL (1996), que se baseia em criptografia de chaves públicas e em certificados de identidade X.509 – os certificados de atributos, também definidos na ITU-T X.509, passaram a ser utilizados mais tardiamente. Os certificados de atributos não possuem chaves, mas atributos que carregam informações como permissões para controle de acesso, papéis. Em um esforço para integrar ambos os certificados, Park e Sandhu (1999) introduziram o conceito de certificados inteligentes, que seria um certificado de identidade X.509 com extensões que carregariam as informações de atributos, unificando os certificados de identidade e de atributos em um único certificado.

Neste sistema, uma autoridade de atributos inseriria atributos em uma extensão e assinaria este atributo, sendo esta assinatura também carregada como uma extensão. Entretanto, a solução de Park e Sandhu (1999) apresenta alguns problemas. O primeiro deles é que como os atributos nas extensões possuem assinaturas próprias, a validação do certificado não pode ser realizada da maneira convencional. Além disso, continua sendo necessário possuir os certificados de atributos de confiança para verificação dos atributos e é necessário que haja uma interface entre a autoridade de atributos e a de certificação, e que a os atributos

sejam inclusos junto à emissão do certificado de identidade.

Posteriormente, Lakshminarayanan e Zhou (2003), criaram o FlexiCert, um novo mecanismo para incluir atributos em certificados de identidade X.509 durante o seu uso. O FlexiCert é adaptado para o caso em que a Autoridade de Atributos (AA) e a autoridade de verificação de identidade (CA) são entidades separadas. A Autoridade de Atributos é responsável por atribuir privilégios ao sujeito. Esse conjunto de privilégios representa uma associação entre entidade final e atributos de autorização.

O sistema funciona com um módulo de atualização de certificados de identidade gerenciado pela CA. Para que a CA saiba quais atributos devem ser incluídos no certificado de identidade, seria necessário o uso do certificado de atributos, que agiria apenas como intermediário. Neste sistema os atributos não são assinados pela AA, apenas pela CA, que aprova os atributos concedidos.

O funcionamento do sistema se daria conforme a Figura 20. O usuário, que já possui um certificado de identidade, faria a requisição de permissões para uma AA e receberia um certificado de atributos. O usuário faria uma requisição de atualização do seu certificado de identidade para o módulo de atualização sob controle da CA enviando o seu certificado de atributos e de identidade. O usuário recebe um certificado de identidade atualizado com extensões contendo os seus atributos. Alternativamente, a própria AA poderia enviar os certificados para o módulo de atualização da CA e devolver para o usuário diretamente o certificado de identidade atualizado.

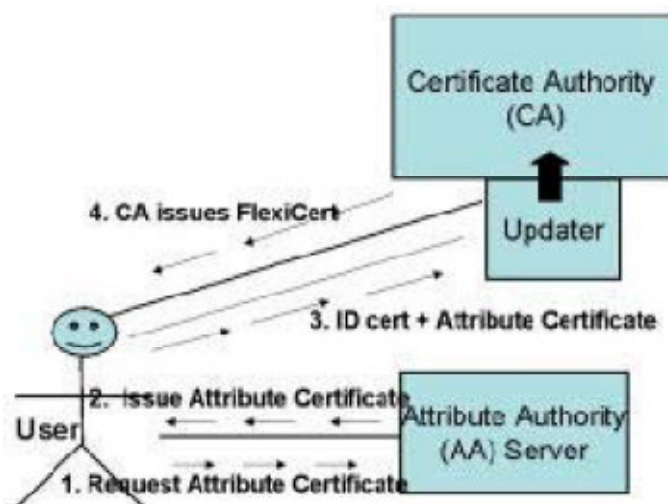


Figura 20. Processo de atualização do FlexiCert. Fonte: Lakshminarayanan e Zhou (2003)

A solução de Lakshminarayanan e Zhou (2003) possui a vantagem de não ser necessário ao verificador de certificados possuir o certificado fonte da autoridade de atributos. Por outro lado a responsabilidade da atribuição dos atributos recai sobre a AC que não necessariamente faz parte da cadeia de decisão de atribuição dos atributos. Além disso, esta solução exige a existência de AAs além de aumentar a carga de trabalho de uma AC, inclusive aumentando o seu escopo de trabalho, interferindo diretamente na organização da infraestrutura de chaves públicas.

2.5.1.6 Certificado de atributos

De acordo com Shirey (2000), um certificado de atributos é um certificado digital que associa, de forma direta ou indireta, um conjunto de informações a uma entidade final. A associação indireta faz com que um certificado de atributos se relacione logicamente a um certificado de identidade. Na verdade, um certificado de atributos é muito similar a um certificado de identidade. A principal diferença é que através de um certificado de atributos não são estabelecidas garantias acerca da autenticidade do proprietário. Em outras palavras, um certificado de atributos não contém uma chave pública. Ao invés disso, ele contém atributos que determinam associações a grupos, papéis, privilégios de segurança ou qualquer outra informação associada ao proprietário do certificado.

O certificado de atributos, definido em ITU-T X.509 (2005), requer a verificação de autenticidade e de privilégios do seu emissor. O certificado de atributos possui a assinatura do seu emissor e a partir desta assinatura é possível verificar a autenticidade do certificado de atributos utilizando um certificado de identidade da entidade signatária. Também é necessário verificar se a entidade emissora possuía o privilégio de delegar privilégios a partir de um conjunto de certificados de atributos. Desta forma, é constituída uma cadeia de certificados de atributos, a IGP (Infraestrutura de Gerenciamento de Privilégios). A IGP é análoga à ICP (Infraestrutura de Chaves Públicas).

O certificado de atributos possui uma série de campos necessários para o seu correto funcionamento. Estes campos informam: quais os privilégios que o detentor do certificado

possui (campo atributos), a identificação do detentor do certificado (*holder*), a identificação do emissor do certificado (*issuer*), a assinatura do certificado pelo emissor e informações sobre o certificado (versão, validade, identificação). A sintaxe do certificado de atributos segue notação ASN.1 e pode ser consultada em ITU-T X.509 (2005).

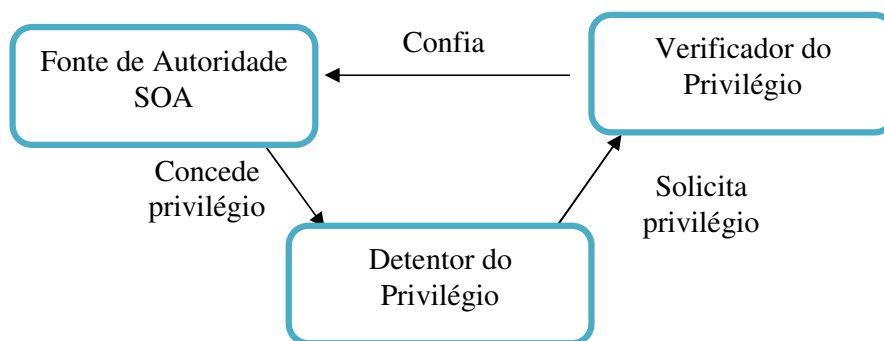


Figura 21. Componentes no modelo de operação geral da IGP. Fonte: ITU-T X.509 (2005)

Alguns modelos de operação para a IGP são definidos na ITU-T X.509 (2005). No modelo de IGP mais simples, apresentado na Figura 21, há três componentes: o Verificador de Privilégios, a Fonte de Autoridade (SOA – *Source Of Authority*) e o Detentor do certificado, aquele que possui um privilégio e quer fazer uso dele. Neste caso a Fonte de Autoridade emite certificados de atributos para dar privilégios aos detentores.

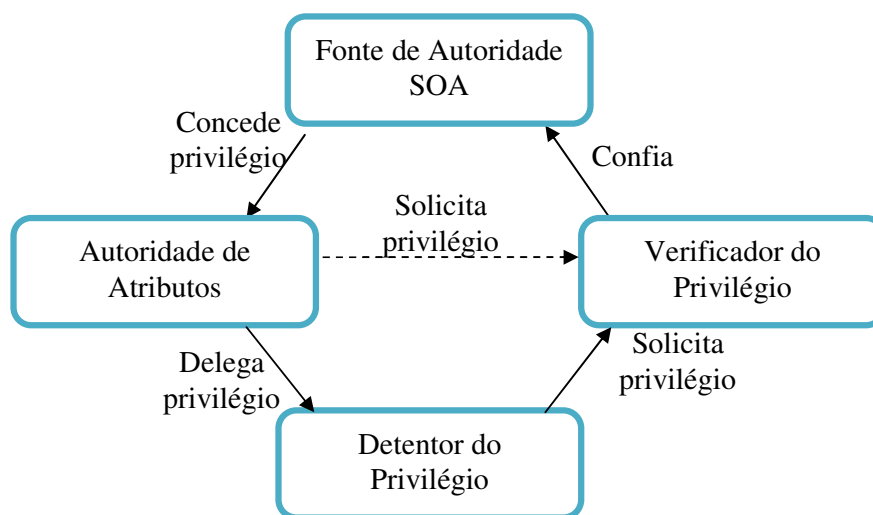


Figura 22. Modelo de delegação de privilégios. Fonte: ITU-T X.509 (2005)

Outro modelo de funcionamento da IGP definido na ITU-T X.509 (2005) é o modelo de delegação de privilégios, apresentado na Figura 22. Neste modelo é inserida uma quarta entidade, a Autoridade de Atributos. No ambiente com delegação, a SOA pode autorizar o detentor de privilégios a agir como uma Autoridade de Atributos, podendo ele gerar certificados de atributos delegando privilégios. Além disso, esta Autoridade de Atributos pode ainda fazer uso de seus privilégios, solicitando aos verificados acesso a recursos.

Segundo a norma ITU-T X.509 (2005) cada detentor de privilégios poderia delegar os seus privilégios para outras entidades. A fim de evitar cadeias muito extensas, é possível limitar a habilidade de delegação posterior, seja pela criação de um atributo específico de delegação, ou com o auxílio da extensão *basicAttConstraints*. Com esta extensão, além de limitar a delegação posterior, também é possível delegar apenas um conjunto de privilégios. De qualquer forma, independentemente das restrições que podem ser aplicadas aos privilégios delegados, uma restrição universal do modelo de delegação é que nenhuma entidade pode delegar mais privilégios do que possui.

Neste modelo, as autoridades de atributos podem delegar privilégio de atuação como autoridade de atributos a outras entidades. Esta delegação poderia ser repassada a entidades intermediárias até designar uma entidade final sem privilégio de delegação, que apenas pode utilizar os seus privilégios sem poder de criar uma Autoridade de Atributos.

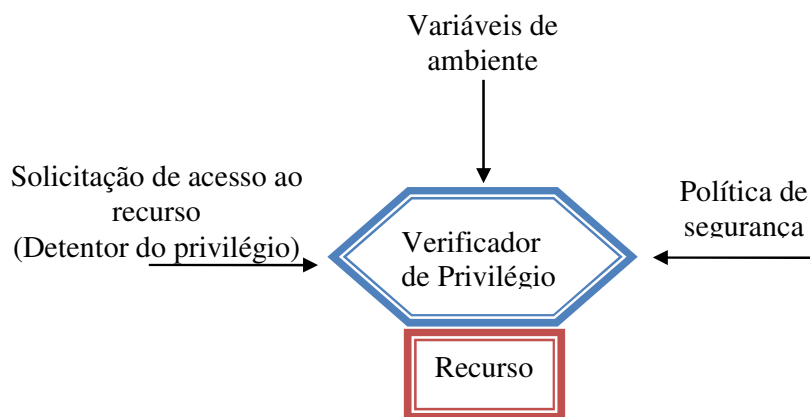


Figura 23. Liberação de recurso. Fonte: Adaptado de ITU-T X.509 (2005)

Sempre que uma requisição de acesso a um objeto for realizada, a validade dessa associação é examinada pelo verificador de privilégios. A liberação de acesso a um recurso

não se dá simplesmente com a verificação do certificado de atributos, mas também deve levar em consideração as informações relacionadas ao contexto de acesso, tais como o momento da requisição, a sensibilidade do objeto sendo acessado, ou mesmo à política de segurança. A Figura 23 apresenta as verificações necessárias para a realização de uma liberação de recurso.

A política de segurança especifica o grau de privilégios e o contexto considerados adequados para que se efetue o acesso ao recurso. Com ela, o verificador de privilégios determina, para um dado conjunto de informações, o limite de aceitação mínimo para que o acesso possa tomar parte. Na recomendação X.509 não há definição de qual sintaxe deve ser utilizada para expressar uma política.

O certificado de atributos possui um perfil para a Internet definido pela RFC 3281 por Farrel e Housley (2002). Este perfil é compatível com o certificado definido na ITU-T X.509 (2005) mas é mais restrito, determinando o uso de campos opcionais e valores de campos com conteúdo indefinido na especificação original.

Neste capítulo não será apresentado um detalhamento dos campos das especificações de Farrel e Housley (2002) nem de ITU-T X.509 (2005), que podem ser consultados nestas referências e estão disponíveis sem custo. No capítulo da proposta, os campos destas especificações serão explorados, mas com as considerações para aplicação ao caso da proposta.

Os certificados de atributos, apesar de definidos juntamente ao certificado de identidade passam a ter maior campo de aplicação nos últimos anos. Frausto e Antotne (2004) apresentam a necessidade de uma infraestrutura centralizada e hierárquica para as autoridades de certificação de identidade e um modelo de confiança descentralizado para autoridades de atributos (AA), simplificando o método de delegação de direitos.

O modelo descentralizado para AA baseia-se na delegação de privilégios de uma entidade para outra, formando uma cadeia de confiança. A cadeia de confiança para certificados de atributos deve ser reduzida para diminuir o tempo de verificação e transmissão. Em relação à revogação de certificados de atributos é sugerido o uso de certificados com curta duração, sem necessidade de revogação por listagem. Eles propõem o controle de acesso baseado em papéis, que pode ser utilizado em larga escala na Internet. Seria utilizado o certificado de chave pública para identificação e o certificado de atributos para permissões.

Neste sentido existem outros trabalhos com um esforço na sistematização do modelo

de operação deste tipo de infraestrutura, como o apresentado por Arrebola (2006) e Chadwick ET AL (2003).

2.5.1.7 Lista de certificados revogados

A Lista de Certificados Revogados (LCR) é uma listagem que contém os números seriais dos certificados digitais, de identidade ou de atributos, que não podem mais ser considerados confiáveis. Segundo a RFC 3280, por Housley ET AL (2002), os certificados podem ser considerados irreversivelmente revogados ou apenas suspensos. A causa mais comum de uma revogação de certificado de identidade é o comprometimento de uma chave privada. Já para o certificado de atributos, seria a suspensão ou troca de um privilégio designado.

A LCR deveria ser sempre consultada para garantia de que o certificado em verificação ainda encontra-se válido. A LCR pode ser enviada junto aos certificados ou consultada em um servidor remoto, indicado nas extensões do certificado em validação. A LCR possui a assinatura da autoridade de certificação para garantia da sua autenticidade.

Uma alternativa ao uso da LCR é o protocolo OCSP (*Online Certificate Status Protocol*), definido na RFC2560, por Myers ET AL (1999). O OCSP é utilizado para verificação pela Internet da validade de certificados, ele requer menos banda e permite a verificação de validade em tempo real.

2.5.1.8 Mensagens Criptográficas

A RFC3852, por Housley (2008), define uma sintaxe para mensagens criptográficas denominadas CMS (*Cryptographic Message Syntax*). Esta estrutura utiliza o ASN.1 e permite que sejam enviados em formato padronizado tanto um conteúdo cifrado, como o conteúdo

claro associado à sua assinatura digital. A vantagem da utilização desta estrutura é que ela padroniza o envio de todas as informações auxiliares para leitura da mensagem.

A CMS utilizada para envio de conteúdo cifrado é denominada envelope de dados. Neste tipo de CMS são enviados dados cifrados e informações específicas para a recuperação da chave por cada destinatário.

Para envio de conteúdo claro com a sua respectiva assinatura digital, existem duas variações de CMS, com ou sem o dado estar anexado à mensagem. A CMS de dado assinado anexado permite que sejam encapsulados na mensagem: o conteúdo a ser transmitido, a sua assinatura e as informações auxiliares para a verificação da assinatura. São informações auxiliares para a verificação da assinatura os certificados e informações de algoritmos utilizados. Já na variação dado assinado não-anexado, a CMS encapsula a assinatura e as informações auxiliares para a verificação da assinatura, mas o dado é enviado separadamente.

2.5.2 Sistemas em uso para autenticação de aplicativos

Esta seção apresentará dois sistemas de autenticação especialmente relevantes para a proposta aqui apresentada: a ICP-Brasil e o GEM.

2.5.2.1 Infraestrutura de Chaves Públicas Brasileira

A ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira) é um conjunto de entidades, padrões técnicos e regulamentos, elaborados para suportar um sistema criptográfico com base em certificados digitais. Os certificados digitais de identidade gerados por esta infraestrutura possuem validade jurídica, viabilizando a realização de negócios por meio de transações eletrônicas.

Estrutura da certificação digital no Brasil

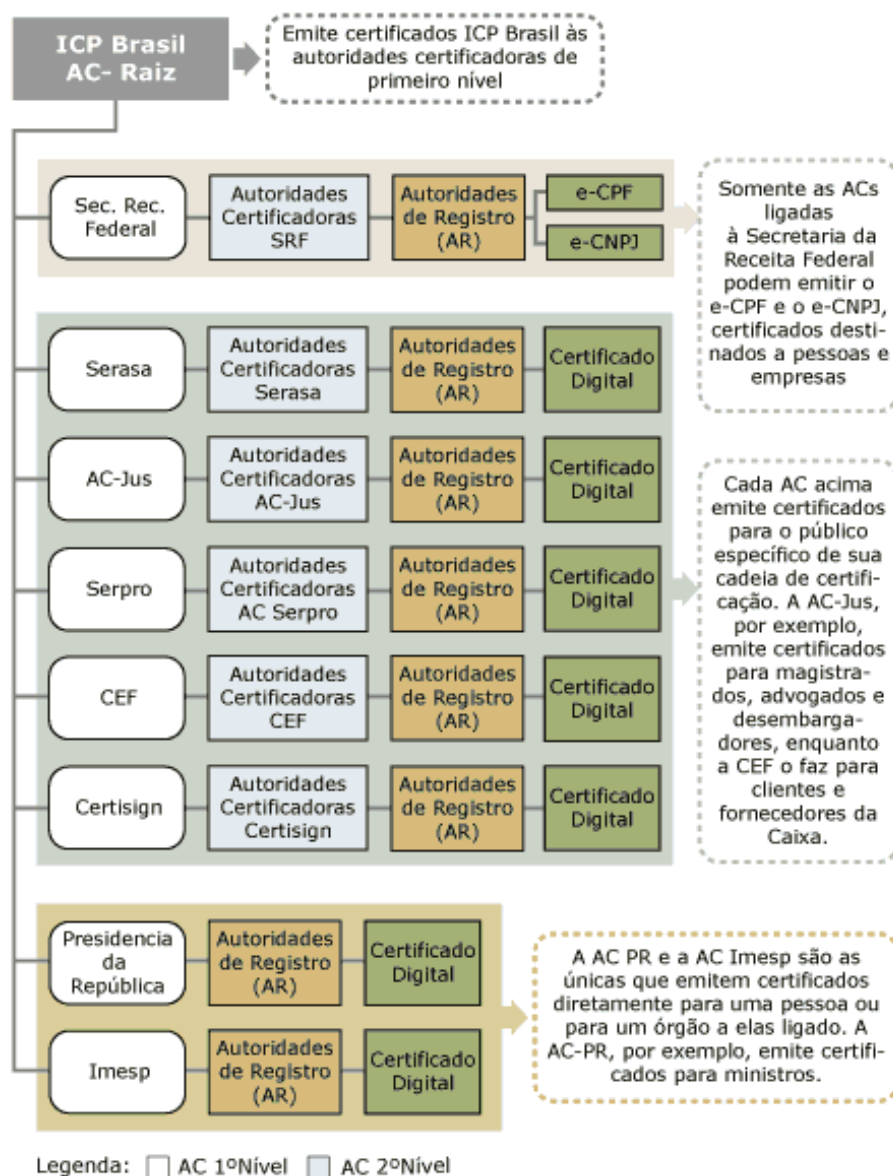


Figura 24. Estrutura de certificação digital no Brasil. Fonte: Ribeiro (2008)

A ICP-Brasil foi instituída pela Medida Provisória 2.200-2, de 24 de agosto de 2001, que define a sua estrutura. O modelo de infraestrutura adotado pela ICP-Brasil foi o de certificado com raiz única. Foi delegado ao Instituto Nacional de Tecnologia da Informação - ITI a operacionalização da infraestrutura, tendo ainda o papel de Autoridade Certificadora Raiz - AC Raiz da Infraestrutura de Chaves Públicas Brasileira. Cabe ao ITI credenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

Uma das principais características da ICP-Brasil é sua estrutura hierárquica, conforme

ilustrado na Figura 24. No topo da estrutura encontra-se o ITI (AC Raiz) e, abaixo dela, as diversas entidades (ACs de primeiro e segundo nível e Autoridades de Registro). Atualmente, a ICP-Brasil tem credenciadas oito Autoridades Certificadoras de primeiro nível (Presidência da República, Secretaria da Receita Federal, Serpro, Caixa Econômica Federal, AC Jus, *Certisign*, Imprensa Oficial de São Paulo - Imesp e Serasa), 20 ACs de segundo nível e mais de 800 Autoridades de Registro (AR). As Autoridades de Registro são a presença física da certificação digital no Brasil. Elas são as responsáveis por autenticar o titular do certificado. Quando alguém pede um certificado digital, deve comparecer a uma Autoridade de Registro para que esse certificado seja validado antes de ser usado.

Tabela 3. Padrões da ICP-Brasil. Fonte: ITI (2006)

Formato para entrega de certificados emitidos pela AC	ITU-T X.509, que especifica um PKCS#7 degradado
Formato de solicitação de certificados à AC	PKCS #10
Algoritmo criptográfico e tamanho da chave para geração de chaves assimétricas de AC	RSA 2048 bits
Algoritmo criptográfico e tamanho mínimo de chaves assimétricas de usuário final	RSA 1024 bits para os certificados digitais dos tipos A1, A2, A3, S1, S2 e S3 RSA 2048 bits para os certificados digitais dos tipos A4 e S4
Algoritmos criptográficos para assinatura de certificados de AC	SHA-1 com RSA
Algoritmos criptográficos para assinatura de certificados de usuário final	SHA-1 com RSA SHA-1 com DAS
Algoritmo simétrico para guarda de chave privada da entidade titular e de seu backup	3-DES, IDEA, SAFER+

Embora contadores e analistas fiscais tenham sido pioneiros no uso da tecnologia, ela está se expandindo, primeiro para as grandes corporações, depois para as micro e pequenas empresas e finalmente atingirá os cidadãos comuns. Atualmente, o Brasil tem cerca de um

milhão de certificados no padrão ICP Brasil (Fonte: Valor Econômico por Françoise Terzian).

Além da demanda natural para a ICP Brasil, serviços do governo estão sendo gradualmente digitalizados exigindo o uso destes certificados. Por exemplo, a Instrução Normativa 696 da Secretaria da Receita Federal (2006) determinou o uso da certificação digital para a entrega da Declaração de Informações Econômico-Fiscais em 2007, atingindo 180 mil empresas. Além disso, foi criado o e-CNPJ, nova versão do certificado digital ICP-Brasil, com foco nos quase 3,5 milhões de micro e pequenos negócios brasileiros, que devem passar a usar o certificado até 2011. Já a adoção dos certificados digitais para pessoas físicas, deve vir pelo novo sistema de identificação anunciado pelo governo, o RIC - Registro de Identidade Civil que unifica documentos como Registro Geral, Cadastro de Pessoa Física (CPF), Carteira Nacional de Habilitação e Título de Eleitor. O RIC foi anunciado em agosto de 2008 e deve entrar em vigor a partir de janeiro de 2009. Com o RIC o cidadão receberá automaticamente uma certificação digital.

Os padrões adotados na ICP-Brasil estão apresentados na Tabela 3. O padrão PKCS #7 é o precursor da RFC3852, que define a CMS, definindo uma estrutura de dados para armazenamento do certificado.

Na ICP-Brasil fala-se em certificado digital tipo A ou S, para designar os certificados digitais de identidade utilizados para assinatura ou criptografia. São duas séries de certificados, com quatro tipos cada. A série A (A1, A2, A3 e A4) reúne os certificados de assinatura digital, utilizados na confirmação de identidade com verificação da integridade de suas informações. A série S (S1, S2, S3 e S4) reúne os certificados de sigilo, que são utilizados na codificação de documentos e de outras informações eletrônicas sigilosas. Os oito tipos são diferenciados nível de segurança e pela validade. A Tabela 4 apresenta uma comparação entre os diferentes tipos de certificados.

Nesta seção foi evidenciada a relevância da infraestrutura brasileira de chaves públicas e apresentada a tendência de que cada pessoa física e jurídica possua um certificado ICP-Brasil. Para que certificados digitais que não façam parte da ICP-Brasil possuam validade jurídica, deve existir previamente um acordo formal entre as partes. Desta forma, no cenário de televisão digital, o uso de certificados de identidade deveria aproveitar a ICP-Brasil visando minimizar as necessidades de investimento para a criação de uma nova infraestrutura e os riscos de não validade pela falta do embasamento jurídico que a ICP já possui.

Tabela 4. Tabela comparativa entre tipos de certificados ICP-Brasil.

Tipo de certificado	Chave criptográfica			Validade máxima do certificado (anos)
	Tamanho (bits)	Processo de geração	Mídia Armazenadora	
A1 e S1	1024	Software	Smartcard ou token, ambos <u>sem</u> capacidade de geração de chave e protegidos por senha	1
A2 e S2	1024	Hardware	Smartcard ou token, ambos <u>sem</u> capacidade de geração de chave e protegidos por senha	2
A3 e S3	1024	Hardware	Smartcard ou token, ambos <u>com</u> capacidade de geração de chave e protegidos por senha <u>ou</u> hardware criptográfico aprovado pelo Comitê Gestor da ICP-Brasil	3
A4 e S4	2048	Hardware	Smartcard ou token, ambos <u>com</u> capacidade de geração de chave e protegidos por senha <u>ou</u> hardware criptográfico aprovado pelo Comitê Gestor da ICP-Brasil	3

2.5.2.2 GEM: Globally Executable MHP

O sistema brasileiro de televisão digital adota como referência para a API do *middleware* procedural a especificação ETSI TS 102 543 (2008), com variações ainda não oficialmente publicadas. A especificação ETSI TS 102 543 (2008) é conhecida como GEM (*Globally Executable MHP*) e foi desenvolvida pelo DVB como sendo um subconjunto da sua especificação de *middleware*, o MHP, para facilitar o porte de aplicativos entre diferentes sistemas de televisão digital.

O GEM especifica a segurança do sistema para aplicativos interativos pela definição de duas categorias de aplicativos: os autenticados e os não autenticados. Os aplicativos interativos são um sistema hierárquico de arquivos, com pastas e subpastas. Os aplicativos, independentemente de serem autenticados ou não, possuem acesso a um subconjunto de APIs do *middleware*, este subconjunto de APIs é denominado caixa de areia. As APIs contidas na caixa de areia não são consideradas sensíveis, ou seja, não representam um problema de segurança para o receptor. Para ter acesso às demais APIs do *middleware*, é necessário fazer uma requisição de permissões adicionais ao receptor, por meio da autenticação do aplicativo e de um arquivo de solicitação de permissões. Este arquivo de solicitação tem formato XML e é definido na especificação do GEM. A concessão das permissões extras solicitadas deve ter a anuência do usuário do receptor, mas o modo como esta anuência é dada não é especificado em norma.

O mecanismo de autenticação proposto no GEM faz uso de assinatura digital de código de *software* com verificação por certificação digital. Este tipo de ferramenta permite a garantia da integridade do aplicativo (garante a sua fonte e o seu conteúdo). Porém, desta maneira, caso a entidade emissora do aplicativo possua um certificado digital, ela automaticamente passa a ter permissão de envio de aplicativos com requisição de permissões extra. Este mecanismo garante o não repúdio da aplicação por parte do seu emissor. Para garantir que a entidade que está assinando o *software* tem permissão para tal, os certificados digitais para TV digital precisam possuir uma infraestrutura relacionada, que emita certificados específicos para as entidades com direito de transmissão de aplicativos para TVD, adicionando um campo de privilégio para estes certificados.

No caso de recebimento de atualização de software, o GEM sugere utilização do mesmo sistema especificado ou o uso de um sistema proprietário por parte do fabricante do receptor.

Maiores detalhes sobre os mecanismos de autenticação de aplicativos utilizados no GEM serão apresentados nos subitens a seguir.

Cálculo da função do *hash*

Para evitar a assinatura de todos os arquivos que fazem parte de um aplicativo para TVD interativa, o GEM utiliza um mecanismo que permite a assinatura de apenas um arquivo

da estrutura de diretórios enviada. Este mecanismo permite que apenas o nível superior de uma árvore de diretórios seja assinado, mas que ainda assim todos os arquivos tenham as suas integridades garantidas. Este resultado é obtido a partir da assinatura de um arquivo que contém o *hash* da estrutura de diretórios abaixo dele.

Cada diretório contém um arquivo de *hash* denominado *hash.dvb* que lista todos os arquivos deste diretório e as subpastas dele. Todos os arquivos são listados e, para cada um, é informado se o mesmo é autenticado ou não. Em caso positivo, é informado o tipo de *hash* e o valor do código *hash*. Arquivos contendo assinaturas digitais não são autenticados. No caso de subdiretórios, o valor do *hash* deve ser igual ao valor do cálculo de *hash* para o seu arquivo *hash.dvb*. A Figura 25 apresenta o mecanismo descrito de cálculo do *hash*.

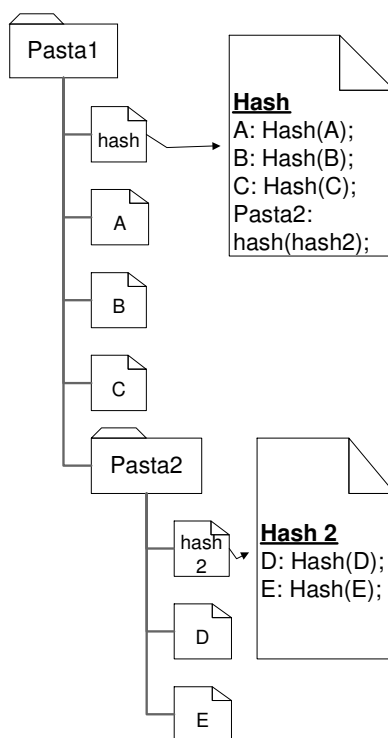


Figura 25. Cálculo do valor de hash de diretórios.

A Tabela 5 apresenta a sintaxe do arquivo contendo a informação do código hash do aplicativo interativo. Os seus campos possuem o seguinte significado:

- *digest_count*: informa o número de arquivos listados no diretório em questão.
- *digest_type*: tipo de código *hash* aplicado. São suportados algoritmos MD5 e SHA-1.
- *name_count*: número de nomes de objetos associados com esta entrada.

- *name_lenght*: tamanho do nome do arquivo em caracteres.
- *name_byte*: caracteres do nome do objeto.
- *digest_byte*: caracteres com o valor do cálculo da função hash.

Tabela 5. Sintaxe do arquivo de hash. Fonte: GEM (2008)

Syntax	Num. Bits	Format
<pre> Hashfile () { digest_count for(i=0; i<digest_count; i++) { digest_type name_count for(j=0; j<name_count; j++) { name_length for(k=0; k<name_length; k++) { name_byte } } for(j=0; j<digest_length; j++) { digest_byte } } } </pre>	16	uimsbf
	8	uimsbf
	16	uimsbf
	8	uimsbf
	8	bslbf
	8	bslbf
Other data may follow but can be ignored by implementations conforming to this profile.		

Tabela 6. Interpretação do campo *digest_type*

<i>digest_type</i>	Comprimento do <i>hash</i> em bits	Algoritmo
0	0	Não autenticado
1	16	Cálculo sem prefixo utilizando MD-5
2	20	Cálculo sem prefixo utilizando SHA-1
3	20	Cálculo com prefixo utilizando SHA-1
Outros		Reservado para uso futuro

A Tabela 6 apresenta os valores possíveis para preenchimento do campo *digest_type*, informando o algoritmo de hash que deve ser aplicado e o seu respectivo comprimento resultante.

A Tabela 7 apresenta as diretivas para cálculo do *hash*, considerando o tipo do objeto, o valor do *digest_type* e do *entry_type*.

Tabela 7. Diretivas para cálculo do hash

Tipo de objeto	<i>digest_type</i>	<i>entry_type</i>	Dados utilizados para o cálculo do hash
Arquivo	1 ou 2	Não aplicável	Conteúdo inteiro do arquivo
Diretório			Conteúdo do arquivo <i>hash.file</i> deste diretório
Arquivo	3	1	<p>Prefixo concatenado a todo o conteúdo do arquivo.</p> <p>O prefixo é determinado como o <i>entry_type</i> codificado em 32 bits uimbsf concatenado com o comprimento do arquivo em bytes utilizando a mesma codificação.</p>
Diretório		0	<p>Prefixo concatenado a todo o conteúdo do arquivo <i>hash.file</i> do diretório.</p> <p>O prefixo é determinado como o <i>entry_type</i> codificado em 32 bits uimbsf concatenado com o comprimento do arquivo em bytes utilizando a mesma codificação.</p>

Assinatura digital

A assinatura digital é enviada no topo da uma árvore de diretórios que ela assina. A assinatura digital é realizada sobre o arquivo *hash.dvb* do mesmo nível onde estará o arquivo contendo a assinatura. Ela é gerada calculando o *hash* sobre o arquivo *hash.dvb* e então realizando a cifra com a chave privada do emissor sobre o *hash*.

O nome do arquivo que contém a assinatura digital é dado como "dvb.signaturefile."<x>, onde o x é um número inteiro utilizado para que seja possível que o aplicativo seja assinado por múltiplas entidades.

O GEM envia assinatura digital em um arquivo de formato proprietário em estrutura ASN.1 como se segue:

```
Signature ::= SEQUENCE {
  certificateIdentifier AuthorityKeyIdentifier,
  hashSignatureAlgorithm OBJECT IDENTIFIER,
  signatureValue BIT STRING }
```

- **certificateIdentifier:** indica o certificado digital utilizado para conferir esta assinatura. Este campo segue a definição da ITU-T X.509 (2005) para o campo *AuthorityKeyIdentifier*, com o formato apresentado abaixo:

```
AuthorityKeyIdentifier ::= SEQUENCE {
  keyIdentifier [0] KeyIdentifier OPTIONAL,
  authorityCertIssuer [1] GeneralNames OPTIONAL,
  authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL }
```

Para o uso dos certificados no GEM o campo *authorityCertIssuer* e *authorityCertSerialNumber* são obrigatórios. O campo *authorityCertIssuer* indica o nome do diretório que deve corresponder ao *issuerName* do certificado que contém a chave para verificação da assinatura.

- **hashSignatureAlgorithm:** este campo identifica o algoritmo de *hash* a ser utilizado. São suportados MD-5 e SHA-1.
- **signatureValue:** o valor da assinatura segue o definido em Housley ET AL (1999) na RFC 2459, seção 7.2.

Certificado digital

O certificado digital para conferência da assinatura do aplicativo interativo é enviado em um arquivo que contém toda a cadeia de certificação necessária, até o certificado raiz. O arquivo com os certificados digitais é enviado no mesmo diretório em que o arquivo de assinatura digital. O nome deste arquivo é "dwb.certificatesfile."<x>, onde o x é um número inteiro correspondente ao número no nome do arquivo de assinaturas.

O certificado utilizado é o de identidade conforme definido em ITU-T X.509 (2005) com suporte à assinatura RSA. O perfil utilizado é baseado em Housley ET AL (1999). A sintaxe deste certificado é apresentada na Tabela 8.

Tabela 8. Sintaxe dos arquivos de certificados de identidade no GEM. Fonte:GEM.

Syntax	Num. Bits	Format
<pre> Certificatefile () { certificate_count for(i=0; i<certificate_count; i++) { certificate_length certificate() } } </pre>	16	uimsbf
	24	uimsbf

- *certificate_count*: Contém o número de certificados no arquivo de certificados
- *certificate_length*: Informa o número de bytes do certificado.
- *certificate()*: Este campo segue a estrutura definida em ITU-T X.509 (2005).

```

Certificatefile () {
  certificate_count 16 uimsbf
  for( i=0; i<certificate_count; i++ )
  {
    certificate_length 24 uimsbf
    certificate()
  }
}

```

Inclusão/Revogação de certificados de confiança

O GEM especifica um mecanismo de atualização dos certificados de confiança nos receptores utilizando mensagens. Estas mensagens são denominadas RCMM (*Root Certificate Management Messages*), que consistem em arquivos com codificação ASN.1.

A estrutura da RCMM é:

```
RCMM ::= SEQUENCE {
    Issuer                Name,
    thisUpdate            Time,
    nextNbOfSignatures   INTEGER OPTIONAL,
    addedCertificates     SET OF Certificate
    removedCertificates  SET OF CertificatesReference
}
CertificatesReference ::= SEQUENCE {
    issuerName            Name,
    serialNumber         CertificateSerialNumber
}
```

Os campos *addedCertificates* e *removedCertificates* especificam os certificados a serem adicionados ou removidos, respectivamente.

Revogação de certificados

No GEM os mecanismos de verificação de revogação de certificados que devem ser suportados pelos receptores são: através do canal de retorno do receptor ou através do TS transmitido pela emissora de televisão. Pelo canal de retorno é realizado o acesso às LCRs através das informações de acessos contidas em extensões dos certificados em verificação. Caso o receptor não tenha um canal de retorno disponível, a lista de certificados revogados é recebida pelo carrossel de objetos, transmitida em um arquivo específico contendo diretamente a LCR no formato especificado na RFC 2459.

2.6 Conclusão

Neste capítulo foram apresentados os fundamentos sobre televisão digital e segurança, além de apresentar o estado da arte em segurança aplicada à televisão digital. O Brasil escolheu um sistema de televisão digital de alta qualidade com ênfase em interatividade. Estes dois pontos alta qualidade e interatividade geram diretamente necessidades de segurança em duas áreas distintas, são elas, respectivamente: proteção de direitos autorais e segurança em serviços.

Analisando o estado da arte na área de proteção de direitos autorais, pude-se perceber que o sistema adotado como base para o SBTVD, no caso, ISDB, pode ser melhorado significativamente para implantação no Brasil. O Brasil possui um cenário particular em termos de legislação, parque de receptores e cultura de comercialização de cópias não legalizadas. Além disso, o sistema ISDB utiliza algumas ferramentas, como o algoritmo criptográfico MULTI-2 que poderiam ser atualizados para a sua inserção no SBTVD.

Já em relação à segurança em serviços, pela análise do estado da arte, podemos perceber que uma oportunidade de contribuição da melhoria do sistema de autenticação de aplicativos. Considerando a tendência de uso de certificados de atributos para o gerenciamento em escopos separados de autenticação e delegação de privilégios, a autenticação de aplicativos do SBTVD poderia fazer uso deste mecanismo, já que o Fórum SBTVD é responsável pelas especificações do sistema e cadastramento de instituições e seus papéis, enquanto a ICP-Brasil já possui responsabilidade na autenticação de instituições.

Desta maneira, o capítulo 3, apresentará propostas de contribuições nestes dois temas. Para isso, inicialmente é realizada uma sistematização destes temas, pela identificação de casos de uso e pelo levantamento de seus requisitos e posteriormente configurando a proposta.

3 Contribuições no sistema de segurança para o SBTVD

Neste capítulo serão apresentadas as contribuições desta dissertação ao sistema de segurança do SBTVD. O capítulo apresenta inicialmente uma sistematização do tema no qual são identificadas duas áreas principais: proteção de direitos autorais e segurança em serviços. Para cada uma destas áreas foram identificados casos de uso e seus requisitos de segurança. Posteriormente são propostos dois sistemas com enfoques específicos para o SBTVD, um em cada uma destas áreas.

Considerando os casos de uso e requisitos, foram realizadas contribuições para o sistema de proteção de direitos autorais do SBTVD e um sistema de autenticação de aplicativos. O sistema de proteção de direitos autorais proposto é denominado SPDA-BR e apresenta contribuições ao esquema de proteção do conteúdo, à linguagem de direitos e às licenças. Já o sistema de autenticação de aplicativos proposto, foi denominado AUTV. Ele é aplicável à segurança em serviços, podendo ser utilizado para vários tipos de aplicativos, desde os aplicativos interativos para o *middleware* Ginga, como para *drivers* do sistema e *software* para atualização do sistema de arquivos do receptor. As propostas tanto do SPDA-BR como do AUTV serão apresentadas neste capítulo, em seções subseqüentes.

3.1 Sistematização da segurança para a TV terrestre brasileira

Conforme apresentado no capítulo 2, foram identificadas duas áreas principais para o sistema de segurança no contexto da televisão digital: proteção de direitos autorais e segurança em serviços. Para cada uma delas é discutida a necessidade de integridade, confidencialidade e disponibilidade; identificados os seus casos de uso principais; e levantados os requisitos de segurança para cada caso de uso.

3.1.1 Proteção de direitos autorais: casos de uso e requisitos

O sistema de proteção a direitos autorais (DRM) no contexto de consumo de material áudio-visual tem como motivação principal o cumprimento de leis que asseguram a propriedade do conteúdo aos seus autores e produtores. Além do cumprimento das leis, existem outros fatores geradores de requisitos para o sistema de DRM, são eles econômicos e funcionais, como será apresentado nas descrições de casos de uso relacionados. Cada um possui requisitos para o sistema de segurança.

O cenário de proteção de direitos autorais requer confidencialidade e disponibilidade. Confidencialidade para restringir o uso e o acesso ao conteúdo de forma a garantir a obediência às regras de uso definidas para o conteúdo. Disponibilidade para garantir o amplo acesso ao conteúdo da TV aberta, como enfatizado pelo Decreto nº4.901 (BRASIL, 2003). O aspecto de integridade do conteúdo não é muito relevante neste caso, pois caso houvesse a transmissão de conteúdo de áudio e vídeo de uma fonte não legalizada, mesmo se o conteúdo fosse recebido com sucesso, não traria dano ao equipamento de recepção. Este caso é muito raro devido ao custo dos equipamentos de transmissão e à interferência causada pelos canais legalizados em operação.

Os casos de uso identificados para a proteção de direitos autorais foram: Televisão simples, vídeo sob demanda limitado, controle de reprodução, armazenamento de conteúdo por tempo indeterminado, distribuição de conteúdo em ambiente doméstico, reprodução de cópias para venda, uso do material em outras produções, retransmissão do conteúdo pela Internet. Cada um deles será descrito e analisado a seguir.

a) Televisão simples

Descrição: usuário assiste à televisão de maneira passiva com o conteúdo sendo transmitido ao vivo pela emissora de TV.

Requisitos: Este tipo de uso não possui requisitos de segurança.

b) Vídeo sob demanda limitado

Descrição: ao ser ligado, o receptor apresenta ao usuário um *menu* no qual pode selecionar os seus programas preferidos passados durante o período em que o receptor esteve desligado (em *standby*). Esta funcionalidade permite que o usuário selecione uma das programações exibidas por um dado canal em um intervalo de tempo limitado, durante as últimas 24h, por exemplo. Esta funcionalidade é operacionalizada pelo constante armazenamento da programação pelo receptor durante o *standby*.

Requisitos: Armazenamento de conteúdo recebido por TV aberta por tempo limitado – deve ser especificado nos meta-dados do conteúdo o tempo que o conteúdo pode ser armazenado, para esta funcionalidade poderia ser restrito o tempo de armazenamento com controle na ordem de grandeza dias, um dia por exemplo.

c) Controle de reprodução

Descrição: durante a reprodução de um vídeo recebido pela emissora de TV, o usuário seleciona a interrupção da exibição do vídeo, depois de alguns minutos, seleciona continuar a assistir o programa do ponto em que havia parado. Pode ainda acelerar o tempo de reprodução do vídeo até o ponto em transmissão ao vivo. – Esta funcionalidade é possibilitada pelo armazenamento do conteúdo recebido a partir do comando de parar reprodução, e a partir do momento de retomada de reprodução o conteúdo é reproduzido a partir da unidade de armazenamento enquanto o conteúdo recebido pela emissora passa a ser continuamente armazenado.

Requisitos: Armazenamento de conteúdo recebido por TV aberta por tempo limitado – para que seja possível disponibilizar este tipo de funcionalidade os conteúdos, mesmo que não possam ser armazenados por tempo ilimitado devem ter pelo menos a possibilidade de armazenamento por tempo restrito. Neste caso o tempo que o conteúdo deveria ser armazenado seria na ordem de grandeza de minutos; por uma hora, por exemplo.

d) Armazenamento de conteúdo por tempo indeterminado.

Descrição: usuário armazena o conteúdo para uso pessoal, de maneira similar ao que é feito atualmente por um vídeo cassete, no qual pode ser armazenado o conteúdo para reprodução posterior por número de vezes ilimitado.

Requisitos: armazenamento sem limite de tempo – possibilidade de permissão para manter uma cópia do conteúdo por período indeterminado.

e) Distribuição de conteúdo em ambiente doméstico

Descrição: usuário transfere o conteúdo armazenado no receptor de televisão digital para um dispositivo móvel com capacidade de reprodução de áudio e vídeo. Esta funcionalidade refere-se à possibilidade de transmissão do conteúdo para diferentes dispositivos pertencentes ao mesmo usuário, com fins de entretenimento, possibilitando a reprodução do conteúdo em computadores de mão (*handhelds, palmtops*), no computador, em celulares, em outros monitores, dentre outros.

Requisitos: controle do número de cópias do conteúdo permitidas e repasse das informações de direitos e proteção do conteúdo através das interfaces (entre dispositivos) – deve ser possível permitir a distribuição de conteúdo em ambiente doméstico para uso pessoal, evitando a cópias indevidas.

f) Reprodução de cópias para venda não autorizada

Descrição: usuário realiza diversas cópias de um dado conteúdo em dispositivo a partir de uma fonte armazenada no próprio receptor ou retira o dado do receptor por meio das suas interfaces e utiliza este conteúdo como fonte para reprodução de cópias. O conteúdo copiado é utilizado para fins comerciais sem repasse de lucros aos autores.

Requisitos: controle do número de cópias do conteúdo permitidas e proteção das interfaces de saída do terminal de acesso – deve haver métodos que controlem a pirataria pela limitação do número de cópias de um dado conteúdo no receptor. Também é preciso que o conteúdo exportado pelas suas interfaces esteja protegido e que as regras de uso sejam exportadas junto ao conteúdo.

g) Uso não autorizado do material em outras produções

Descrição: usuário realiza cópia do conteúdo e dada a qualidade do conteúdo o aplica em outra produção, sendo esta comercializada. Não há repasse de verbas para o autor do conteúdo original.

Requisitos: possibilidade de rastreamento/identificação do conteúdo transmitido – deve haver uma ferramenta que identifique o autor/produtor do conteúdo para evitar o seu aproveitamento por terceiros.

h) Retransmissão do conteúdo pela Internet

Descrição: usuário retransmite um dado conteúdo por rede de difusão. O conteúdo é utilizado sem fins comerciais, mas não há acordo nem repasse financeiro aos autores.

Requisitos: controle do número de fluxos de transferências do conteúdo – este requisito é importante para limitar a difusão por IP (IPTV) de conteúdos sem permissão por parte do autor.

Os casos de uso f, g e h são extremamente relevantes do ponto de vista econômico, já que a produção nacional de conteúdo costuma ser exportada para outros países após a sua exibição em solo nacional e que a legislação brasileira não permite que um conteúdo seja distribuído sem que haja anuência de seu autor/detentor. A qualidade de conteúdo importado exibido pela televisão brasileira também é influenciado pela qualidade do sistema de DRM adotado no país, já que o custo da licença de exibição do conteúdo está diretamente relacionado à garantia de existência, e à efetividade, de barreiras ao comércio ilegal de obras.

3.1.2 Segurança em serviços: casos de uso e requisitos

A segurança em serviços na televisão digital possui, de maneira geral, necessidade de confidencialidade, integridade e disponibilidade. Confidencialidade para permitir o uso de serviços com necessidade de sigilo, a compra de uma mercadoria por comerciais interativos. Integridade para garantir valor jurídico a estas transações para permitir serviços com valor de inclusão digital, como fazer a declaração de isento no imposto de renda pelo terminal de acesso de TVD. E a disponibilidade, pois os aplicativos geralmente são relacionados à programação de TV e possuem uma banda pequena de transmissão, por isso, eles devem ser verificados rapidamente, não prejudicando a experiência do usuário.

Os casos de uso identificados para a segurança em serviços foram: serviço de engenharia, conexão de dispositivo externo, execução local de aplicativo interativo simples, execução local de aplicativo interativo com uso de recursos críticos, execução de aplicativo interativo com necessidade de canal de retorno e execução de aplicativo com necessidade de autenticação do usuário. Cada um deles será descrito e analisado a seguir.

a) Serviço de engenharia

Descrição: consiste no recebimento de *software*, juntamente à programação de TV, para manutenção das unidades receptoras de maneira transparente para o usuário final. Este serviço inclui a correção de erros, solução de problemas relacionados à transmissão, correção de problemas derivados da diferença na interpretação de operação entre unidades receptoras, melhora da exibição, aceleração da resposta e melhora da operabilidade de receptores de TVD. Este tipo de *software* é dependente do receptor de televisão digital, sendo destinados a marcas e modelos específicos, não sendo executados sobre o *middleware*.

Requisitos: para o serviço de engenharia é importante que seja garantida a integridade do pacote de atualização, pois o recebimento de dados corrompidos ou modificados maliciosamente poderia danificar o receptor. Por isso, é importante que haja garantia da autenticidade da fonte do pacote de atualização e que esta seja responsável pelos pacotes recebidos (não-repúdio).

b) Conexão de um dispositivo

Descrição: consiste na instalação pelo usuário de um novo dispositivo como forma de garantir a expansibilidade do sistema. A interface genérica dos receptores de televisão digital é a USB, que permite o recebimento do *driver* pela própria interface, podendo este ser instalado de maneira transparente para o usuário. Este tipo de aplicativo é dependente do receptor de televisão digital, não sendo executados sobre o *middleware*.

Requisitos: é importante que seja garantida a integridade do *driver*, pois o recebimento de dados corrompidos ou modificados maliciosamente poderia danificar o receptor. Além disso, dada a ampla variedade de sistemas receptores de TV é necessário que haja um sistema de homologação de *drivers*, identificando para cada receptor quais *drivers* poderiam ser instalados.

c) Execução local de aplicativo interativo simples

Descrição: recebimento de aplicativo interativo junto ao conteúdo de áudio e vídeo. Este aplicativo não requer canal de retorno e não faz uso de funções que possam ser nocivas ao receptor de TVD. Um exemplo de aplicativo nesta categoria seria um programa de TV com um jogo de perguntas e respostas, no qual o usuário pode responder às perguntas do jogo e comparar com os resultados dos participantes do programa. Ao alterar o canal a pontuação é perdida e o jogo interrompido. Este aplicativo é executado sobre o *middleware*.

Requisitos: Não há requisitos de segurança, já que este aplicativo não utiliza funções que deixem o receptor vulnerável.

d) Execução local de aplicativo interativo com uso de recursos críticos

Descrição: recebimento de aplicativo interativo junto ao conteúdo de áudio e vídeo. Este aplicativo não requer canal de retorno, mas faz uso de funções que podem ser nocivas ao receptor de TVD. Um exemplo de aplicativo nesta categoria seria um serviço de agendamento de programação que em determinado horário selecionado pelo usuário, o aplicativo troque o canal da TV. Este aplicativo ficaria permanentemente no receptor, mesmo na troca de canais e depois do *standby*. O acesso à alteração do canal programa de TV pode permitir a um aplicativo que ele impeça o usuário de entrar em determinado canal, podendo ser desenvolvido um aplicativo malicioso que prejudique a experiência do usuário. Este aplicativo é executado sobre o *middleware*.

Requisitos: Controle de acesso a APIs avançadas do *middleware* e garantia de integridade das aplicações com acesso a estas APIs.

e) Execução de aplicativo interativo com necessidade de canal de retorno

Descrição: recebimento de aplicativo interativo junto ao conteúdo de áudio e vídeo. Este aplicativo requer canal de retorno e é executado sobre o *middleware*. Um exemplo de aplicativo nesta categoria seria um programa de TV com um jogo de perguntas e respostas, no qual o usuário pode responder às perguntas do jogo e ao final quem responder mais perguntas corretas ganha um prêmio.

Requisitos: Protocolo de comunicação com o canal de retorno permitindo segurança, considerando confidencialidade e integridade do canal.

f) Execução de aplicativo com necessidade de autenticação do usuário

Descrição: recebimento de aplicativo interativo junto ao conteúdo de áudio e vídeo. Este aplicativo requer canal de retorno, é executado sobre o *middleware* e requer a autenticação do usuário. Um exemplo de aplicativo nesta categoria seria um serviço que permite ao usuário declarar isenção no imposto de renda.

Requisitos: Autenticação do usuário pelo canal de retorno com validade jurídica, sigilo.

3.2 Sistema de proteção de direitos autorais: SPDA-BR

Esta seção descreve o sistema de gerenciamento de direitos autorais para televisão digital, considerando o consumo de conteúdo audiovisual. Para a consolidação da proposta de DRM aqui apresentada foram considerados os casos de uso e os requisitos brasileiros e os sistemas no estado da arte, especialmente o sistema ARIB. A partir disto foi proposto um sistema de DRM para o SBTVD considerando melhorias ao sistema de DRM do ISDB-T.

A proposta resultante será denominada SPDA-BR e é um conjunto de recomendações para o SBTVD, consolidando uma solução flexível, que pode ou não utilizar cartão de circuito integrado (*smartcard*), além de possuir melhor eficiência em consumo de banda para distribuição das chaves.

As premissas utilizadas neste trabalho para realização da proposta apresentada foram:

- Utilização de um padrão aberto. Alguns padrões proprietários têm baseado a sua segurança na obscuridade dos mecanismos utilizados, o que pode gerar o inconveniente de uma premissa de segurança falsa além de monopólios;
- Gerar um sistema para proteção dos direitos autorais de conteúdos transmitidos para

TV aberta brasileira;

- Escalabilidade para permitir a melhoria do sistema sem a geração de legado.

O SPDA-BR aborda os tópicos na área de proteção de direitos autorais com maiores contribuições identificadas na linguagem de definição de direitos e no esquema de proteção do conteúdo.

3.2.1 Linguagem de direitos

Nesta seção será proposta uma linguagem de direitos para o sistema de proteção de direitos autorais para o SBTVD. Como o sistema base é o ISDB-T, será analisada linguagem de direitos do sistema ISDB-T frente aos requisitos brasileiros identificados. Com base nesta análise, será consolidada a proposta para o SBTVD.

A linguagem de direitos do DRM no sistema ISDB-T é composto pelos descritores: **controle de cópias** e **disponibilidade de conteúdo**. O descritor de **controle de cópias** possui configurações para: cópia livre, nunca copiar, copiar uma geração. Além disso, ele possui um campo para liberar ou restringir a saída de conteúdo por interface analógica e outro para restringir a exportação de TS por qualquer tipo de interface. Já o descritor de **disponibilidade do conteúdo** determina se é possível realizar acúmulo de conteúdo no tempo ou não. Podendo realizar o acúmulo, ele determina se o conteúdo armazenado pode ser reproduzido por um período restrito ou irrestrito.

Comparando este protocolo com os casos de uso identificados para a proteção de direitos autorais pode-se perceber que a maioria dos requisitos identificados é satisfeita com os dois descritores do ISDB-T.

O caso de uso de *vídeo sob demanda limitado* e o caso de uso de *controle de reprodução* que requerem a possibilidade de configuração *armazenamento de conteúdo recebido por TV aberta por tempo limitado*, com a diferença de um requerer esta configuração na ordem de grandeza dias e o segundo na ordem de grandeza de minutos, são ambos satisfeitos pelo **descritor de disponibilidade de conteúdo** que permite este tipo de

funcionalidade variando de 1h30min até uma semana. O caso de uso de *armazenamento de conteúdo por tempo indeterminado*, que necessita de *armazenamento sem limite de tempo* também é atendido por este mesmo descritor.

O caso de uso de *distribuição de conteúdo em ambiente doméstico e reprodução de cópias para venda não autorizada* requerem o controle do número de cópias do conteúdo permitidas, sendo que o primeiro requer também proteção das interfaces de saída do terminal de acesso – deve haver ferramentas que controlem a pirataria pela limitação do número de cópias de um dado conteúdo no receptor. Com a configuração de cópia de uma geração, o requisito de controle de número de cópias é atendido, pois é possível permitir apenas uma cópia do conteúdo por dispositivo, sem permitir a reprodução de mais de uma unidade a cópia para pirataria fica impossibilitada. Já a questão da proteção das interfaces de saída do terminal é coberta pelo sistema japonês com o emprego de sistemas de proteção de interfaces, o HDCP, DTCP, CGMS-A, SCMS, que exportam o conteúdo protegido e podem exportar os metadados de regras de uso, como o de cópia livre, proibida ou por uma geração.

O caso de uso de *retransmissão do conteúdo pela Internet* que requer o controle do número de fluxos de transferências do conteúdo não requer nenhuma ferramenta criptográfica, podendo ser realizado com a determinação de regras de conformidade que limitem o número de fluxos, como é feito na ARIB, não requerendo qualquer alteração.

Já para o caso de *Uso não autorizado de material em outras produções* seria necessária a *possibilidade de rastreamento/identificação do conteúdo transmitido* esta ferramenta não está presente no protocolo do ARIB e nem em suas ferramentas de segurança. Uma proposta para o sistema brasileiro de televisão digital seria a inclusão da inserção de identificação do receptor no conteúdo apresentado nas suas interfaces de saída. É proposta a criação de um novo descritor a ser inserido nas mensagens ECM que seria interpretada como uma requisição de exibição na tela da identificação do receptor, por um período de tempo definido na própria mensagem.

Os descritores de **controle de cópias** e de **disponibilidade de conteúdo** são transmitidos nas tabelas SI. Este tipo de protocolo de transmissão torna o conteúdo vulnerável, já que o conteúdo da tabela SI poderia facilmente ser substituído, sendo ele claro (não cifrado). Por isso, uma proposta de melhoria para o sistema brasileiro seria a inclusão destes descritores dentro das mensagens ECMs, mantendo-os protegidos.

Concluindo, a proposta uma linguagem de direitos para o sistema de proteção de

direitos autorais para o SBTVD considera o uso dos descritores: **controle de cópias** e **disponibilidade de conteúdo**, com envio não apenas no *transport stream*, mas também no interior das mensagens ECM. Além disso, foi incluído um **descritor de rastreamento** também enviado no interior das mensagens ECM.

3.2.2 Licenças de uso

Nesta seção será analisado o sistema ISDB-T e feita uma proposta de adaptação para o cenário brasileiro. Os aspectos analisados foram: níveis hierárquicos de chaves e uso de chaves mestras simétricas ou assimétricas.

3.2.2.1 Níveis hierárquicos

Em relação aos níveis hierárquicos, o ISDB-T, segundo a norma ARIB STD B25 (2006), explicita apenas três níveis de chaves. Esta configuração possui algumas vantagens, tanto do ponto de vista da transmissão como da recepção. Considerando a transmissão, esta configuração simplifica muito o gerenciamento de chaves do sistema, o número em chaves é igual ao número de receptores em operação mais uma chave de trabalho e um par de chaves de cifra. Do ponto de vista de recepção, também há simplificação do sistema, já que cada receptor precisa armazenar e gerenciar apenas quatro chaves, diminuindo a necessidade de memória protegida do receptor. As quatro chaves são: a chave mestra única e não atualizável, a chave de trabalho e o par de chaves de cifra.

Por outro lado, a atualização das chaves de trabalho vai requerer que cada chave seja colocada em uma mensagem EMM criptografada com a chave mestra do receptor. Desta maneira, a atualização das chaves de trabalho requer o recebimento de uma mensagem EMM para cada receptor. Além disso, não bastaria o envio de uma única mensagem por receptor, já

que não há mensagem de confirmação de recebimento da EMM. Isto porque, no cenário de televisão digital o recebimento de dados é unidirecional. A bidirecionalidade é obtida pela presença do canal de retorno que não está presente em todos os receptores. Por isso, para aumentar as chances de recebimento das mensagens EMM elas são re-enviadas ciclicamente por um determinado intervalo de tempo. Para um parque de televisores extenso como o brasileiro, seria demandando elevado consumo de banda, ou tempo de distribuição extenso.

Como os receptores dependem da chave K_w para visualizar o conteúdo, deve ser garantida a presença de uma chave K_w válida nos receptores. Uma alternativa para garantir K_w válida seria enviar K_s cifrado simultaneamente para chaves K_w de diferentes momentos temporais, até que seja considerado seguro desativar uma K_w . O aumento da disponibilidade de K_w aos receptores acaba diminuindo a agilidade de troca de chaves e aumentando o consumo de banda para a distribuição de chaves.

A atualização da chave de trabalho é especialmente importante, pois uma vez descoberta a chave K_w , é possível abrir todo o conteúdo cifrado, já que esta chave é comum para todo o parque de receptores e é utilizada para abrir as ECM com as chaves que cifram o conteúdo. Por isso, se uma marca de receptores foi produzida sem conformidade às normas de segurança e podem ser utilizados para fins de pirataria, para fazer a revogação de acesso destes receptores, pode ser atualizada a chave de trabalho para todo o parque de receptores com exceção dos receptores desta marca. Além disso, se um indivíduo com interesse na cópia indevida de conteúdo utilizar um método de força bruta para a descoberta das chaves, ele tentará fazer isto sobre a chave de trabalho, pois a chave de cifra é atualizada aproximadamente a cada segundo. Por isso, é necessário que a chave de trabalho seja atualizada periodicamente para retirar este tipo de ataques ao sistema de DRM.

O uso de três níveis de chaves torna a revogação de receptores constatados como fonte de pirataria impraticáveis do ponto de vista operacional, já que demandaria uma banda de mensagens de atualização de chaves K_w muito grande (aproximadamente 60 milhões no caso brasileiro). Neste cenário, a atualização de chaves K_w seria realizada apenas com o objetivo de evitar a entrada de receptores não homologados e nunca para a retirada dos identificados como maliciosos, posteriormente. Mesmo para atualização periódica da chave K_w , o número de mensagens a ser enviada é muito grande, prejudicando a disponibilidade do sistema.

Por isso, o SPDA-BR insere no modelo do ARIB o uso de chaves de grupo, permitindo o uso de hierarquia de chaves. O uso de hierarquia de chaves (*logic key hierarchy* – LKH) permite a escalabilidade do sistema, reduzindo o número de mensagens para a

operação de atualização de chaves (distribuição com mensagens para atualização das chaves do receptor). Existem muitas alternativas de esquemas de hierarquia de chaves, estas opções podem ser postas em prática ou alteradas pelo servidor de gerenciamento de chaves, desde que os receptores possam lidar com os quatro tipos de chaves (Ks, Kw, Kg e Km).

A operacionalização da distribuição das chaves de grupo seria feita enviando-as dentro das mensagens EMMs. Elas não poderiam ser enviadas dentro das mensagens ECMs, pois estas são recebidas em intervalos muito curtos e devem ser interpretadas rapidamente, sendo importante não inserir neste processo verificação de hierarquia de chaves e de endereços na interpretação de ECMs. Desta maneira, seria adicionada à mensagem EMM proposta pelo ARIB, um endereço que indique qual chave deve ser utilizada para a abertura da mensagem recebida, permitindo flexibilidade do sistema em número de chaves e tipos de hierarquia.

3.2.2.2 Modelo centralizado *versus* descentralizado e tipos de chave mestra

O modelo de operação do sistema está diretamente relacionado com o tipo de chave mestra utilizado. Foram consideradas, para chaves mestras, as opções de uso de chaves simétricas, como utilizado no sistema ISDB-T ou o uso de chaves assimétricas, como utilizado no sistema DReaM e proposto no SBTVD fase I.

No sistema de chaves simétricas, a entidade responsável pela montagem das mensagens EMM deve ter acesso à base de dados das chaves mestras de todos os terminais de acesso. As chaves mestras devem ser protegidas com alto grau de segurança, já que todo o sistema de acesso condicional baseia-se no sigilo destas chaves. Por isso, o uso de chaves simétricas subentende um modelo centralizado de geração de EMMs, com uma entidade responsável pela manipulação das chaves Km, de maneira a manter o sistema confiável.

Neste modelo, apresentado na Figura 26, a entidade centralizadora é responsável pela geração das chaves de trabalho e pelo encapsulamento destas chaves nas mensagens EMMs. A entidade centralizadora envia as EMMs para todas as emissoras que encaminham as mensagens ao parque de receptores em funcionamento. Com a chave de trabalho, as emissoras geram as suas próprias chaves de cifra e geram e transmitem as suas mensagens ECM

individualizadas. No cenário de hierarquia de chaves, a entidade centralizadora também se responsabilizaria pelo gerenciamento da árvore de chaves de grupo e geraria mensagens EMM comuns a todas as emissoras para o gerenciamento de grupos de receptores.

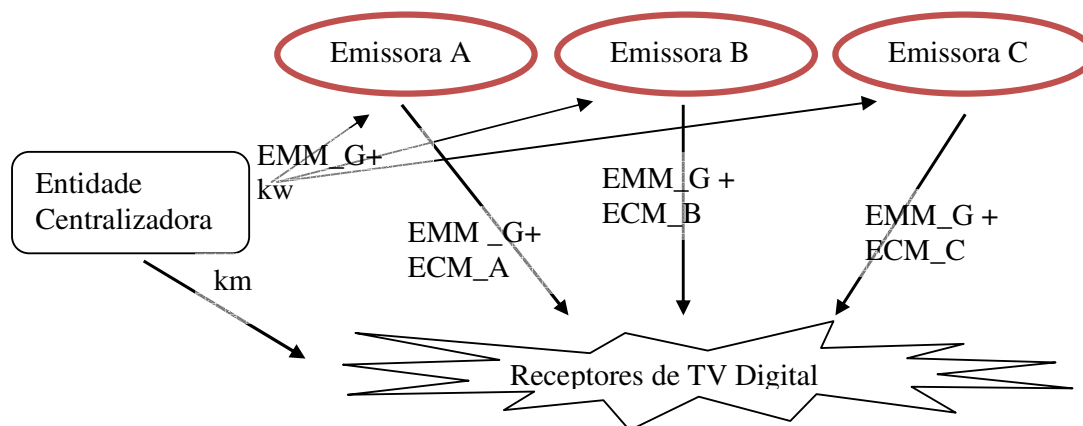


Figura 26. Modelo centralizado de geração de EMMs.

O modelo centralizado de geração de EMMs, que é necessário pelo uso de chaves simétricas, possui como desvantagem a falta de autonomia pelas emissoras para determinar tanto a banda consumida com mensagens EMMs como o período de atualização das chaves que protegem o seu próprio conteúdo. Por outro lado, retira a responsabilidade e o custo de manter uma estrutura para a geração das mensagens EMM e para o gerenciamento das chaves do sistema.

Para permitir o uso do modelo descentralizado de distribuição de EMMs, seria necessário o uso de chaves mestras assimétricas. O que faria com que as chaves privadas dos receptores estivessem protegidas dentro de cada receptor e com que as chaves públicas estivessem disponíveis para a geração das mensagens EMM sem necessidade de segurança.

Neste modelo as emissoras seriam responsáveis pela geração tanto das mensagens ECM quanto das EMMs, sendo inclusive responsáveis pela gerência da hierarquia de chaves no caso do uso de chaves de grupo.

Esta configuração possui a vantagem de permitir que cada emissora defina a banda utilizada e o período da atualização das suas chaves. Por outro lado, este modelo requereria a alteração das chaves mestras para assimétricas, o que aumentaria o custo do cartão, o tempo de processamento e o tamanho das mensagens EMMs. Além disso, cada receptor precisaria

gerenciar uma hierarquia de chaves para cada emissora, fazendo com que a necessidade de memória para este gerenciamento fosse proporcional ao número de emissoras. Esta dependência seria extremamente negativa, pois poderia gerar legado limitando o aumento do número de emissoras. Essa dependência também faria com que o tamanho da hierarquia de chaves devesse ser definido a priori. Com o modelo centralizado, o tamanho da hierarquia pode ser alterado pela entidade centralizadora de maneira transparente aos demais elementos do sistema.

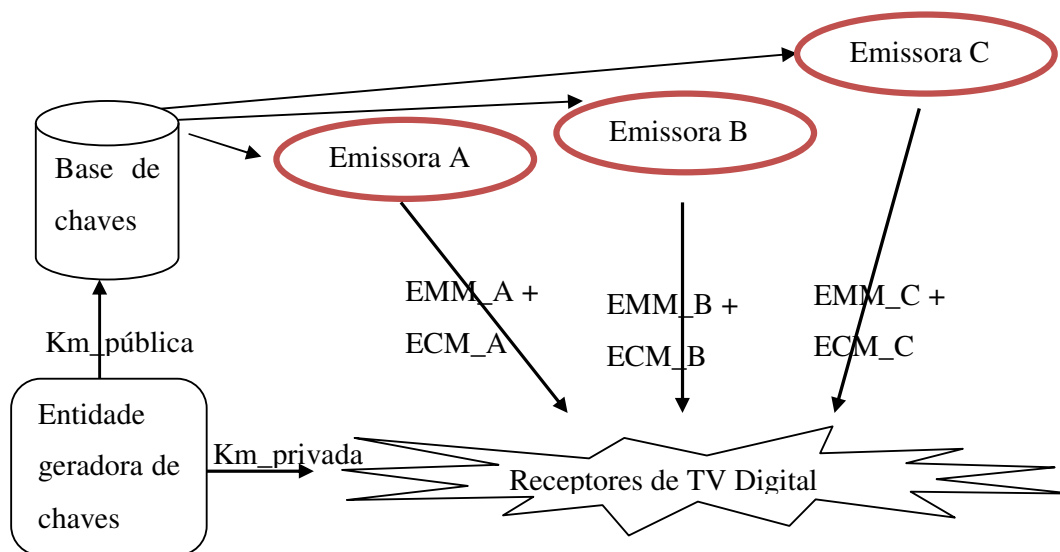


Figura 27. Modelo descentralizado de geração de EMMs.

Analisando os pontos positivos e negativos do uso de chaves mestras simétricas e assimétricas, o trabalho aqui proposto propõe o uso de chaves simétricas, com uma entidade centralizadora.

3.2.2.3 Proposta para licenças

Esta seção apresentou uma análise dos sistemas de uso de chaves em relação aos níveis hierárquicos e ao tipo de algoritmos criptográficos utilizados para fazer uma proposta ao sistema de acesso condicional para o SBTVD. Foram propostos:

- Uso de hierarquia de chaves lógica, utilizando chaves de grupo, além das chaves mestra, de trabalho e de cifra.
- Chaves mestra, de grupo, de trabalho e de cifra, todas simétricas.

3.2.3 Esquema de proteção do conteúdo

Esta seção discute o esquema de proteção do conteúdo para o Sistema Brasileiro de Televisão Digital. Será discutido o uso da criptografia do conteúdo, nível de criptografia, algoritmo e *hardware* criptográfico.

3.2.3.1 Criptografia

O sistema ISDB-T considera a proteção do conteúdo com criptografia, mesmo para televisão aberta, e utiliza o sistema de acesso condicional para dar acesso aos receptores em conformidade do sistema. Esta solução possui como vantagem a garantia de proteção do conteúdo. Sem a sua criptografia, poderia haver a aquisição do conteúdo e, apenas ignorando ou alterando as mensagens com informação de regras de uso, ele estaria disponível. Como desvantagem, o uso de criptografia requer um sistema complexo, que encarece tanto a infraestrutura de transmissão como de recepção. Para que o sistema de proteção de direitos autorais seja efetivo o uso de criptografia é necessário e será mantido no sistema SPDA-BR.

3.2.3.2 Nível da criptografia

A criptografia para proteção do conteúdo, segundo o MPEG-2 Sistemas, pode ser aplicada à área útil (*payload*) tanto do pacote de *transport stream* como no pacote de *elementary stream*. O sistema ISDB-T utiliza a criptografia no pacote do *transport stream*, o que é suficiente para a criptografia de qualquer tipo de componente, dado que os componentes

são identificados pelo PID. O nível de criptografia do SPDA-BR será também na área útil do TS.

3.2.3.3 Algoritmo criptográfico

Como os algoritmos criptográficos são continuamente tornados obsoletos e aprimorados, o algoritmo de proteção de conteúdo do sistema japonês, adotado em 1999, será atualizado no SPDA-BR pela adoção do sistema AES CBC de 128 bits (FIPS 197), considerado atualmente um dos algoritmos mais eficientes para cifra simétrica, segundo Al Hassib e Haque (2008). A Tabela 9 apresenta uma comparação entre os sistemas AES e MULTI-2.

Tabela 9. Quadro comparativo: MULTI-2 x AES

Parâmetro Algoritmo	Tamanho de blocos/chaves	Transformações internas dos algoritmos	Desenvolvimento em hardware	Tipos de Operações na cifra
MULTI-2	64 bits	Inversíveis	Não paralelizável	Aritméticas
AES	128 bits	Não inversíveis	Paralelizável	Não aritméticas
Obs.:	Quanto maior o tamanho de chaves, maior robustez contra ataques de força bruta.	Transformações inversíveis estão sujeitas a ataques fracos e semifracos.	Operações paralelizáveis possuem maior eficiência para implementação em <i>hardware</i> .	Operações não aritméticas são mais rápidas de serem efetuadas.

3.2.3.4 Hardware criptográfico

Considerando as alternativas para o mecanismo de processamento do módulo de recepção de conteúdo protegido com acesso condicional, conforme a Figura 13, o SPDA-BR faz uso da combinação das configurações embarcada (A) e com cartão criptográfico (B), respectivamente.

Normalmente, os sistemas de DRM têm uma validade limitada, a validade do sistema

é o prazo no qual o mesmo não foi quebrado. Após esta validade o sistema é considerado obsoleto e deve ser substituído. Como o parque de receptores para televisão digital terrestre no Brasil é muito extenso e a responsabilidade de troca do sistema de DRM é incerta, é proposta a configuração embarcada combinada com o uso de cartão criptográfico que permitiria que os receptores saíssem de fábrica com o sistema de DRM embarcado, mas com capacidade de adição de um cartão criptográfico, caso haja quebra do sistema original.

Esta solução permite o lançamento dos receptores a um custo menor por não encarecer a lista de materiais com o cartão criptográfico, mas permitindo a atualização posterior do sistema pela inserção futura do cartão. Neste cenário, para a atualização dos sistemas, as emissoras teriam que prover cartões criptográficos para inserção no receptor, o que seria um investimento menor e previamente definido pela especificação do sistema, simplificando o processo de atualização.

Proposta de solução embarcada

Na solução embarcada, a chave mestra e a identificação do receptor, que estariam em um cartão criptográfico para a outra solução, devem ser armazenadas no componente principal do receptor. A inserção de endereço e chave secreta (Km) únicos no componente personaliza os componentes durante o processo de produção.

A arquitetura de segurança do sistema embarcado, apresentada na

Figura 28, conta com duas partes: o **decodificador de fluxo** e o **núcleo de segurança**. O **decodificador de fluxo** recebe o TS cifrado e o transforma em dados claros a partir do uso das chaves Ks. As chaves Ks estão armazenadas em uma área do **núcleo de segurança** acessível apenas para o **decodificador de fluxo**. Já o **núcleo de segurança** recebe as mensagens EMM e ECM, organiza a hierarquia de chaves e extrai os dados contendo as regras de uso do conteúdo. As regras de uso também ficam em uma área de memória disponível para leitura a processos externos ao **núcleo de segurança**. Apesar de tanto o **decodificador de fluxo** como o **núcleo de segurança** possuírem decodificadores AES, é necessário que este seja duplicado, pois a decodificação de fluxo deve ocorrer de maneira contínua e concomitantemente deve haver a decodificação das mensagens ECM e EMM.

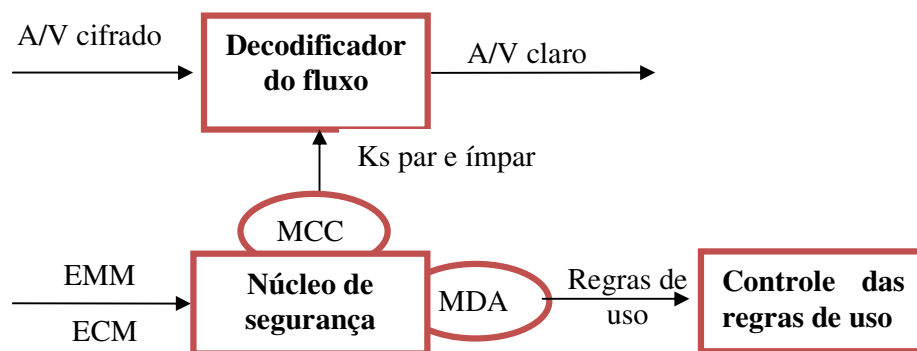


Figura 28. Arquitetura do sistema embarcado.

No cenário de TV digital conforme proposto, o núcleo de segurança pode receber as mensagens ECM e EMM contendo dois tipos de dados: chaves protegidas e dados protegidos. Para tratar estes dados são definidos abaixo os tipos de memória, os modos de operação e os comandos que o **núcleo de segurança** do SPDA-BR deve possuir.

A implementação de um sistema embarcado requer quatro tipos de memórias com diferentes características de acesso. São elas:

- **Memória para armazenamento da chave mestra (MCM):** esta memória armazena a chave mestra, que é única por receptor. A chave mestra pode ser utilizada apenas para referência, não sendo permitido o acesso à leitura dela para nenhuma tarefa em execução. Também não é possível alterá-la. Por isso, esta memória deve ser não volátil, apenas de leitura e privada ao núcleo de segurança.
- **Memória para armazenamento da hierarquia de chaves (MHC):** utilizada para armazenar outras chaves do sistema (chaves de grupo e de trabalho). As chaves armazenadas nesta memória podem ser utilizadas no contexto de decifração sendo utilizada também apenas como referência pelo subsistema de segurança, nenhuma tarefa em execução tem acesso a estas chaves. É necessária uma área de memória proporcional ao tamanho da hierarquia de chaves, com 128 bits para cada chave. Esta memória deve ser não volátil, de escrita e leitura e privada ao **núcleo de segurança**.
- **Memória para Dados Arbitrários (MDA):** utilizada para armazenar o resultado da decifração de dados enviados no interior das mensagens ECM. As chaves utilizadas para decifrar estas mensagens são provenientes da **MHC**. Apenas tarefas autorizadas devem ter acesso aos dados claros. Esta memória deve ser volátil, de escrita e leitura e

acessível por processos externos ao **núcleo de segurança**.

- **Memória para chaves de cifra (MCC):** utilizada para armazenar as chaves que serão utilizadas para decifrar o fluxo de áudio e vídeo. Apenas tarefas autorizadas devem ter acesso aos dados claros. Esta memória deve ser volátil, de escrita e leitura e acessível por processos externos ao **núcleo de segurança**.

São propostos ao **núcleo de segurança** os quatro comandos definidos abaixo para permitir a sua operação:

- **Seletor de chaves:** permite a seleção de uma chave da **MHC**, ou chave mestra, para uso com o modo de Gerenciamento de chaves.
- **Seletor de local de armazenamento de chaves:** identifica o local de armazenamento de uma dada chave na **MHC**.
- **Seletor de modo de operação do núcleo de segurança:** seleciona um dos modos de decifração de conteúdo.
- **Seletor de local de armazenamento de dados:** identifica o local de armazenamento de dados na **MDA**.

Desta maneira, existiriam dois modos de operação para o mecanismo de segurança. O local de encaminhamento do dado claro após a decifração depende do modo selecionado. Os modos são:

- **Gerenciamento de chaves:** este modo é utilizado para decifrar chaves armazenadas nas **EMMs**, neste modo as chaves são decifradas e em seguida armazenadas na **MHC**.
- **Decifração de dados arbitrários:** neste modo os dados que informam as regras de uso e as chaves de cifra são recuperados das mensagens **ECM** e são escritos na **MDA** e **MCC** respectivamente.

Exemplo de funcionamento para recebimento de conteúdo protegido:

- Sistema recebe tabela **CAT** indicando quais pacotes contém **ECMs** e **EMMs** e o sistema de **DRM** utilizado.
- Sistema verifica que o sistema de **DRM** sinalizado na **CAT** é o mesmo embarcado.
- Recebimento de **ECM**.
- Sistema seleciona modo de **Decifração de Dados Arbitrários** com o **Seletor de**

modo de operação.

- Sistema seleciona área de memória a ser utilizada com o **Seletor de local de armazenamento de dados**.
- Núcleo de segurança decifra os dados da ECM com a chave Kw os armazena na área selecionada da **MDA** e as chaves Ks na **MCC**.
- O decodificador de fluxo recebe o conteúdo e decifra os pacotes utilizando a chaves Ks lida da **MCC** de acordo com a informação do cabeçalho do TS que o conteúdo está cifrado e com qual das chaves.
- Sistema aplica regras de uso informadas na **MDA**.

Exemplo de funcionamento para atualização de chave de grupo:

- Sistema recebe tabela CAT indicando quais pacotes contém ECMs e EMMs e sistema de DRM utilizado.
- Sistema verifica que o sistema de DRM sinalizado na CAT é o mesmo embarcado.
- Recebimento de EMM.
- Núcleo de segurança lê a EMM e consulta a identificação da chave que deve ser utilizada para decifrar a EMM.
- Núcleo de segurança verifica se a chave necessária para decifrar a EMM está na **MHC** (caso não esteja o procedimento é encerrado e a EMM descartada).
- Sistema seleciona a chave de decifração da EMM com o **Seletor de chaves**.
- Sistema seleciona modo de **Gerenciamento de chaves** com o **Seletor de modo de operação**.
- Sistema seleciona endereço de armazenamento da chave extraída da EMM com o **Seletor de local de armazenamento de chaves**
- Núcleo de segurança decifra EMM e armazena a chave e a sua identificação no local da **MHC** selecionado.

Chaveamento entre uso do sistema embarcado e cartão criptográfico

O chaveamento entre cartão criptográfico ou sistema embarcado é realizado em função da identificação do sistema de DRM em uso no TS recebido, conforme apresenta a Figura 29. A tabela CAT definida pelo MPEG-2 sistemas possui um campo que identifica a qual sistema de acesso condicional as mensagens ECM e EMM referem-se. Todos os sistemas de proteção de direitos autorais terão um número de identificação, esteja ele embarcado ou no cartão criptográfico. Com base nesta identificação as mensagens ECM e EMM são processadas no núcleo embarcado ou transferidas ao cartão criptográfico.

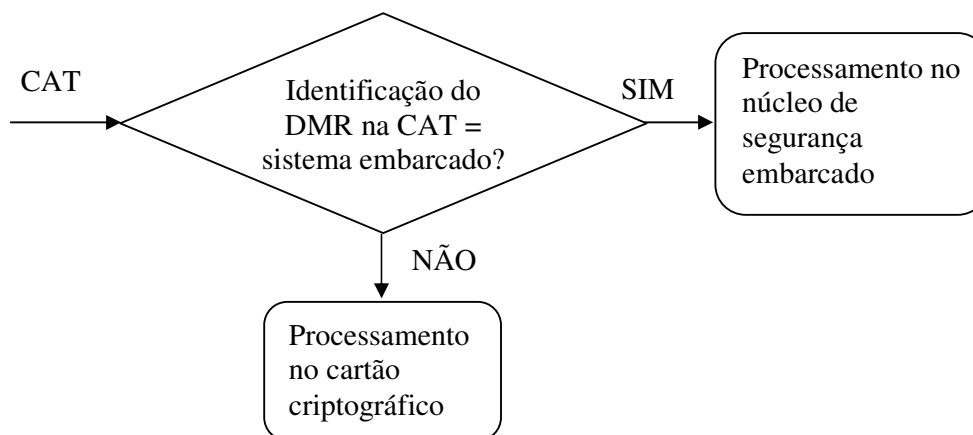


Figura 29. Decisão de processamento pelo módulo embarcado ou cartão criptográfico.

A Figura 30 mostra a integração entre o sistema embarcado e com cartão criptográfico. O demultiplexador recebe o TS contendo as mensagens ECM, EMM, os componentes de áudio e vídeo protegidos, além da tabela CAT junto às outras tabelas SI. O demultiplexador analisa o TS e determina com base nas informações da CAT se as mensagens ECM e EMM devem ser encaminhadas ao cartão criptográfico ou ao sistema embarcado.

Do processamento das mensagens ECM e EMM, são extraídas as chaves de cifra (Ks) e as regras de uso do conteúdo. As chaves de cifra são utilizadas em um bloco de decifração dos componentes protegidos. A saída deste bloco é o fluxo de áudio e vídeo claro.

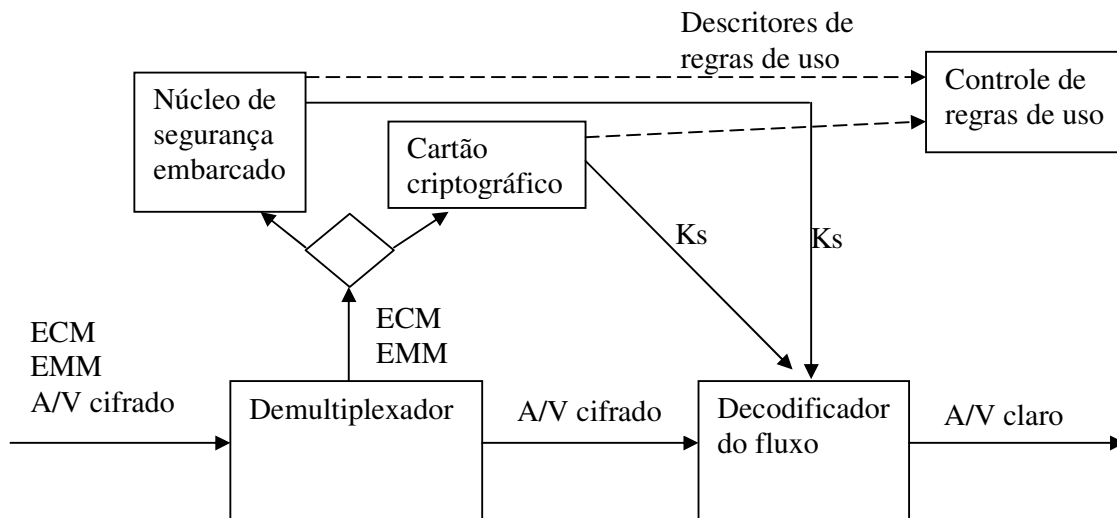


Figura 30. Integração entre processamento embarcado ou no cartão criptográfico.

3.2.3.5 Sumário do esquema de proteção do conteúdo

Esta seção apresentou uma análise dos sistemas de uso de chaves em relação a níveis hierárquicos e tipo de algoritmos criptográficos utilizados para fazer uma proposta ao sistema de acesso condicional do SPDA-BR. Foram propostos:

- Uso de hierarquia de chaves lógica, utilizando chaves de grupo, além das chaves mestra, de trabalho e de cifra.
- Chaves mestra, de grupo, de trabalho e de cifra, todas simétricas com operação centralizada.

Além disso, foi discutido o esquema de proteção do conteúdo para o Sistema Brasileiro de Televisão Digital, chegando-se à proposta de uso de criptografia do conteúdo no nível da área útil dos pacotes de *transport stream* com o uso de algoritmo AES 128 bits CBC. O *hardware* criptográfico proposto permite a operação com o sistema embarcado ou com inserção de um cartão criptográfico tipo *smartcard*.

3.3 Segurança em serviços

Esta seção trata da segunda área identificada para contribuições em segurança para televisão digital: segurança em serviços. Para a consolidação da proposta aqui apresentada foram considerados os casos de uso e os requisitos brasileiros e os sistemas no estado da arte, especialmente o sistema ETSI TS 102 543 (2008), que neste capítulo será referenciado como GEM.

A proposta resultante, denominada AUTV (AUtenticação de aplicativos para TV digital), é um sistema de autenticação de aplicativo para ser aplicado na segurança de serviços no âmbito do SBTVD.

As premissas utilizadas para realização da proposta apresentada foram:

- Utilização de padrões abertos, objetivando a interoperabilidade com ferramentas de outros sistemas;
- Gerar um sistema compatível com os requisitos e a infraestrutura brasileira;
- Unificação dos métodos empregados para os diferentes casos de uso identificados em segurança de serviços simplificando a infraestrutura de recepção e de transmissão.

Entre os casos de uso identificados para segurança em serviços, os casos de *serviço de engenharia*, *conexão de dispositivo* e *execução local de aplicativo interativo avançado*, têm necessidade tanto de verificação da integridade dos aplicativos recebidos como de verificação de permissão, que são cobertos pelo AUTV. A verificação de integridade garante que o pacote recebido seja o pacote enviado pela sua fonte nominal, e pode ser resolvido com o uso de assinatura digital. A verificação de permissão confirma que o remetente do pacote poderia produzir um aplicativo acessando os recursos solicitados.

O caso de uso *execução local de aplicativo interativo avançado* possui ainda um requisito de controle de acesso a funções e métodos do *middleware*. Como o controle de acesso pode ser considerado um tipo de permissão, o AUTV também atende este requisito, unificando o mecanismo de autenticação de aplicativos para estes casos.

Os outros dois casos de uso apresentados na seção de sistematização foram: *execução de aplicativo interativo com necessidade de canal de retorno* e *execução de aplicativo com*

necessidade de autenticação do usuário. Estes dois casos de uso não serão considerados parte do escopo deste trabalho, não por serem menos importantes, mas por estarem bastante associados às tecnologias utilizadas atualmente na Internet.

3.3.1 Autenticação de aplicativos para TV digital: AUTV

Considerando a complexidade de instalação de um serviço de certificação digital e a presença no Brasil de infraestrutura para certificação de identidade baseada em chaves públicas, a ICP Brasil, nesta seção será apresentada a proposta de um mecanismo de autenticação e permissão para aplicativos em ambiente de televisão digital terrestre utilizando assinatura digital de código de *software* com verificação por certificação de identidade ICP Brasil associada à certificação de atributos. Este sistema será denominado AUTV.

As especificações do GEM serão consideradas como estudo de caso para a proposta deste trabalho, dada a sua similaridade com o *middleware* adotado para o sistema brasileiro. O GEM especifica os detalhes de funcionamento de um sistema que utiliza assinatura digital com certificados de identidade específicos para TVD com foco nos casos de uso execução local de aplicativo interativo avançado e execução local de aplicativo interativo simples.

Como inovação é proposto no AUTV um incremento na especificação do GEM, acrescentando o uso de certificados de atributos, adaptando o esquema de segurança do GEM para o aproveitamento da infraestrutura de chaves públicas, já existente no Brasil. Esta infraestrutura de chaves públicas seria utilizada tanto para a assinatura dos aplicativos a serem autenticados, como para a assinatura dos certificados de atributos. Sem esta modificação seria necessário criar uma nova cadeia de chaves públicas, específica para TV Digital. Os certificados de atributos têm o papel de associar permissões às aplicações e entidades que assinam as aplicações. Com este mecanismo, o AUTV permite a expansão do sistema de autenticação de aplicações para os cenários de *serviço de engenharia* e *conexão de dispositivo*, além do caso de uso de *execução local de aplicativo interativo avançado*, que era o único o tratado na especificação do GEM.

Com o uso de certificados de atributos associados ao uso de certificados de identidade,

é possível garantir que apenas fontes confiáveis possuam permissões avançadas no receptor, utilizando a estrutura já estabelecida da ICP-Brasil para a emissão dos certificados de identidade.

3.3.1.1 Visão geral do modelo de operação do sistema AUTV

O sistema AUTV, realiza a autenticação de aplicativos através da assinatura digital do código do aplicativo. Para a realização desta assinatura são utilizadas cadeias de certificação de atributos e de identidade, o que separa os escopos destas infraestruturas: a infraestrutura de chaves públicas (ICP) e infraestrutura de gerenciamento de privilégios (IGP). Os certificados de identidade são responsáveis por garantir a associação correta entre chave pública e entidades, garantindo a correta validação das assinaturas digitais. Já os certificados de atributos determinam se o código transmitido tem privilégio (permissão) para executar ou utilizar recursos específicos do receptor de televisão digital.

As infraestruturas ICP e IGP formam uma cadeia de confiança, que permitem a operação do sistema a partir de uma entidade raiz, considerada confiável. Apesar desta similaridade, estas infraestruturas possuem requisitos de operação bastante distintos. Uma ICP requer custo de operação elevado, pois gera e armazena chaves que precisam ser mantidas em sigilo. Já a IGP utiliza os certificados e assinatura digital para associar informações a entidades. Por isso, pode-se afirmar que a complexidade de operação e manutenção da ICP é superior à IGP.

Com esta separação de escopos o AUTV mantém a infraestrutura ICP, utilizada para TV digital, sendo a ICP-Brasil e cria uma IGP própria para TV digital. O sistema AUTV utiliza o modelo de delegação para a IGP. O sistema de delegação descentraliza o gerenciamento dos certificados de atributos, permitindo a construção de cadeias de confiança para cada caso de uso.

Para isso, são propostos neste modelo, privilégios de delegação específica, ou seja, o detentor de certificado de atributo possui permissão de delegação da permissão X, não sendo capaz de delegar a permissão Y, mesmo que ele a possua. Quando a delegação de privilégios

é utilizada, é necessário que o **verificador de privilégios** cheque toda a cadeia de delegação, verificando se cada **Autoridade de Atributo** possuía o privilégio necessário para a delegação realizada até chegar à **Fonte de Autoridade (SOA)**, que deve estar na lista de confiança do verificador de privilégios.

No AUTV, os certificados de atributos podem ser emitidos para entidades ou para objetos. Quando emitidos para entidades, eles têm duração longa e são relacionados ao certificado de identidade ICP-Brasil da entidade. Neste caso eles atribuem privilégios à entidade. A emissão de certificados de atributos para objetos permite que privilégios sejam atribuídos a aplicativos específicos, não à entidade que o gerou. A integração da ICP e da IGP dá-se na verificação, quando os certificados de atributos apontam para um certificado de chave pública, tanto para o seu emissor como detentor. Por isso, a infraestrutura de chave pública é utilizada para autenticar a cadeia de confiança do emissor e para verificar a autenticidade do detentor do certificado.

3.3.1.2 Visão geral do funcionamento para o receptor

Considerando o uso dos dois tipos de certificados, é necessário que o receptor possua duas listas de entidades de confiança. Estas entidades serão utilizadas para validar a cadeia de certificados recebidos para verificação tanto de assinatura digital como para atribuição de privilégios, para os certificados de identidade e atributos respectivamente. São elas:

- Lista de certificados raiz de confiança: Esta lista define as **Autoridades Certificadoras (ACs)** de confiança;
- Lista de certificados de **Fonte de Autoridade (SOA – Source Of Authority)**, as autoridades de atributos de confiança.

Desta maneira, o software a ser carregado na plataforma que queira fazer uso de uma ação que requeira algum nível de privilégio, deve estar acompanhado da assinatura digital do pacote, da cadeia de certificados de identidades associada à assinatura até a raiz, cadeia de certificados de atributos até a SOA. Desta maneira, o receptor poderia verificar a integridade dos pacotes de dados recebidos, depois validar a sua origem e finalmente verificar se há

permissão para a realização da operação requisitada. As ações executadas pelo receptor para autenticação do pacote recebido seriam:

- Recebimento e verificação da integridade do pacote recebido (código *hash*);
- Recebimento do bloco de assinatura;
- Verificação da assinatura. Este processo é decomposto em:
 - Verificação do certificado do signatário e de todos os certificados da cadeia de certificação;
 - Verificação criptográfica da assinatura do pacote;
- Verificação da autorização para atualização:
 - Obter e verificar o certificado de atributo;
 - Verificação da assinatura do emissor do certificado de atributo;
 - Verificar se a autoridade emissora é uma das entidades autorizadas a delegar os respectivos privilégios;
 - Verificar se o certificado de atributos é relacionado ao objeto que requer os privilégios;
 - Verificar se a permissão corresponde ao tipo de atividade solicitada.

A seguir será apresentado o detalhamento do mecanismo de autenticação e permissão de aplicativos proposto. Alguns itens aqui apresentados foram tratados no capítulo de estado da arte, mas serão mais bem detalhados aqui, de modo a atingir uma proposta suficiente para ser aplicada.

3.3.1.3 Inclusão / Revogação de certificados de confiança

O sistema de gerenciamento de certificados de confiança para o AUTV considera mecanismo igual ao definido no GEM, fazendo uso de mensagens de gerenciamento de certificados de confiança. Porém no AUTV, a inclusão e revogação de certificados não se

aplicam apenas aos certificados de identidade raiz, mas também aos certificados de atributos da fonte de autoridade (SOA).

3.3.1.4 Revogação de certificados

A revogação de certificados no cenário de televisão digital não pode estar dependente do canal de retorno, por isso, o protocolo OCSP pode ser utilizado opcionalmente pelos receptores, mas o principal meio de verificação da validade de certificados deve ser feita por meio das listas de certificados revogados. Ou seja, na verificação da validade de um certificado, seja ele de identidade ou de atributos, faz-se necessário verificar também a LCR, além dos outros itens, como data de validade, assinatura, *etc.*

Caso a duração dos certificados utilizados no sistema fosse curta, não seria necessário utilizar as LCRs, mas como o sistema considera que os certificados pertencem a instituições (pessoas jurídicas), a validade destes certificados é de longo prazo. No AUTV também é possível associar os certificados de atributos a objetos, para algumas destas aplicações o certificado pode ter a validade bastante curta. Em exemplo seria para aplicações interativas sem persistência, que vai ser válida apenas para a duração exata do programa de TV. Apesar destes casos, o sistema deve suportar o uso de LCRs para dar cobertura a todos os demais casos.

O formato da LCR considerado no AUTV segue exatamente o definido por Housley ET AL (2002), na RFC3280. A transmissão dos certificados revogados deve ser realizada no interior do CMS que já possui capacidade para tal.

3.3.1.5 Cálculo da função *hash*

O código de um aplicativo pode ser representado por um diretório, composto por

arquivos e subdiretórios. Para geração de assinatura digital do código do aplicativo como um todo, é necessário criar um arquivo que represente o aplicativo para que a assinatura digital seja realizada sobre este arquivo.

No AUTV será utilizada a mesma solução utilizada no GEM para a geração deste arquivo de representação do aplicativo, que cria um arquivo denominado *hash.file* que sumariza o cálculo do código hash de todos os arquivos contidos no diretório. Desta maneira, com a assinatura do arquivo *hash.file*, é possível garantir a autenticidade de todo o aplicativo.

No AUTV é proposta uma modificação em relação ao sistema especificado pelo GEM para o cálculo da função *hash*, que se limita ao campo *digest_type*, onde o algoritmo MD-5 para cálculo de *hash* foi descartado por ser considerado obsoleto.

O arquivo contendo os valores do hash de cada arquivo da árvore de diretório recebida será denominado *hash.file* e seguirá a sintaxe definida na

Tabela 5. O *digest_type* define tipo de código hash aplicado, segundo a Tabela 10. Estas definições foram modificadas em relação ao GEM por não considerar o uso do algoritmo MD5.

Tabela 10. Interpretação do campo *digest_type*

digest_type	Comprimento do hash em bits	Algoritmo
0	0	Não autenticado
1	20	Cálculo sem prefixo utilizando SHA-1
2	20	Cálculo com prefixo utilizando SHA-1
Outros		Reservado para uso futuro

3.3.1.6 Assinatura digital

Para efetuar a assinatura digital do código do aplicativo, bastaria assinar digitalmente o arquivo *hash.file* no topo da uma árvore de diretórios que constitui o código que ela assina.

O GEM envia assinatura digital em um arquivo de formato proprietário, porém conforme a premissa de utilização de padrões abertos, a proposta deste trabalho é utilizar a CMS para dados assinados. A estrutura interna da CMS será detalhada em item posterior, mas aqui será apresentado o tipo *SignerInfo*, com considerações de uso no cenário de televisão digital sob o escopo desta proposta.

```

SignerInfo ::= SEQUENCE {
    version          CMSVersion,
    sid              SignerIdentifier,
    digestAlgorithm  DigestAlgorithmIdentifier,
    signedAttrs     [0] IMPLICIT SignedAttributes OPTIONAL,
    signatureAlgorithm SignatureAlgorithmIdentifier,
    signature        SignatureValue,
    unsignedAttrs   [1] IMPLICIT UnsignedAttributes OPTIONAL
}

```

version: o campo *version* identifica a sintaxe utilizada, quando o identificador do signatário for escolhido como o *subjectKeyIdentifier*, que é o caso nesta proposta, a versão deve ser igual a três (3).

sid: o campo *sid* identifica a entidade que está assinando o pacote, o remetente. Com esta identificação deve ser possível relacionar a assinatura ao certificado de identidade que possui a chave pública do remetente. Em Housley (2008) este campo pode ter dois valores para identificação do signatário: um número serial (*issuerAndSerialNumber*) ou a identificação da chave do detentor do certificado (*subjectKeyIdentifier*). Nesta proposta é considerado o uso apenas do *subjectKeyIdentifier*, identificador da chave do detentor, indicado para uso com certificados ITU-T X.509 (2005). Como os certificados de identidade e de atributos aqui propostos são compatíveis com certificados ITU-T X.509 (2005), esta opção foi realizada. O relacionamento entre o certificado de identidade e a assinatura é feita pelo campo *subjectKeyIdentifier* do CMS e campo *sid* do certificado de identidade, respectivamente, que devem ser idênticos.

```

SignerIdentifier ::= CHOICE {
    issuerAndSerialNumber IssuerAndSerialNumber,
    subjectKeyIdentifier [0] SubjectKeyIdentifier }

```

digestAlgorithm: identifica o algoritmo utilizado para cálculo do *hash* do pacote. Como apresentado no item anterior, cálculo da função *hash*, será utilizado o algoritmo SHA-1.

```
DigestAlgorithmIdentifier ::=
  sha-1 OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) oiw(14)
  secsig(3) algorithm(2) 26 }
```

signedAttrs: para a *CMS* de dado assinado (*Signed Data*) este campo deve ser composto de dois outros atributos, um indicando que se trata de dados assinados (*ContentType*) e outro com o valor do *hash* (*DigestMessage*, que é calculado utilizando o algoritmo definido em *digestAlgorithm* e é do tipo ASN.1).

```
SignedAttributes ::= SET SIZE (1..MAX) OF Attribute

Attribute ::= SEQUENCE {
  attrType      OBJECT IDENTIFIER,
  attrValues    SET OF AttributeValue }

ContentType ::= SEQUENCE {
  attrType      id-contentType OBJECT IDENTIFIER,
  attrValues    id-signedData OBJECT IDENTIFIER }

id-contentType OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs9(9) 3 }
id-signedData OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs7(7) 2 }

DigestMessage ::= SEQUENCE {
  attrType      id-messageDigest OBJECT IDENTIFIER,
  attrValues    MessageDigest }

id-messageDigest OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs9(9) 4 }
MessageDigest ::= OCTET STRING
```

signatureAlgorithm: este campo possui o identificador do algoritmo utilizado para a geração da assinatura digital. O algoritmo de assinatura digital selecionado pelo ITI no Brasil é o RSA, por isso será mantido este algoritmo como padrão para o SPDA-BR.

```
SignatureAlgorithmIdentifier ::= =
  sha1WithRSAEncryption OBJECT IDENTIFIER ::= { pkcs-1 5 }
```

signature: este campo contém a assinatura digital propriamente dita.

```
SignatureValue ::= OCTET STRING
```

unsignedAttrs: este é um campo opcional do CMS que não será utilizado no contexto

deste trabalho.

3.3.1.7 Certificado de identidade

No GEM o certificado de identidade é enviado em um arquivo à parte. Nesta proposta consideramos o envio do certificado de identidade na estrutura do CMS. O certificado é definido como sendo o definido na ICP-Brasil. Como no AUTV o certificado de identidade pode ser aplicado a entidades ou a objetos, serão utilizados os certificados de identidade definidos na ICP-Brasil para pessoa jurídica em Receita Federal (2002).

3.3.1.8 Certificado de atributos

O certificado de atributos é definido em ITU-T X.509 (2005). O perfil utilizado aqui é baseado no proposto por Farrel e Housley (2002), mas não é compatível com a especificação proposta por ser uma variante. A estrutura do certificado de atributos adotada será detalhada nesta seção. A cadeia de certificados de atributos é enviada também no pacote CMS.

A seguir está apresentada a estrutura da ITU-T X.509 (2005) com as variações em relação à Farrel e Housley (2002) propostas para o AUTV.

```
AttributeCertificate ::= SEQUENCE {
    acinfo                AttributeCertificateInfo,
    signatureAlgorithm    AlgorithmIdentifier,
    signatureValue        BIT STRING
}
```

acinfo: contém as informações do certificado de atributo, tais como emissor, detentor de direitos, atributos. Este campo é composto da maneira apresentada abaixo.

```
AttributeCertificateInfo ::= SEQUENCE {
```

```

version          AttCertVersion, -- deve ser = v2
holder           Holder,
issuer           AttCertIssuer,
signature        AlgorithmIdentifier,
serialNumber     CertificateSerialNumber,
attrCertValidityPeriod AttCertValidityPeriod,
attributes       SEQUENCE OF Attribute,
issuerUniqueID   UniqueIdentifier OPTIONAL,
extensions       Extensions OPTIONAL }

```

version: identifica a versão do certificado de atributos. Neste caso, o certificado aqui proposto é compatível com a v2 da ITU-T X.509 (2005), devendo este campo ser mantido e ter o valor abaixo.

```
AttCertVersion ::= INTEGER { v2(1) }
```

holder: este campo identifica a entidade à qual os atributos são relacionados. Apesar da norma ITU-T X.509 (2005) prever três tipos de identificação, Farrel e Housley (2002) recomendam o uso de apenas um tipo de identificação por vez, de maneira excludente às demais, ainda determinando o uso da opção de identificação por *baseCertificateID* para o caso da autenticação da entidade se dar por certificado de identidade ITU-T X.509 (2005). Desta maneira o relacionamento entre os certificados de atributo e de identidade torna-se direto, pela comparação com o campo *serialNumber* do certificado de identidade. Como a certificação da entidade que receberia atributos no AUTV é realizada com certificado de identidade ITU-T X.509 (2005), será considerado o uso do campo *baseCertificateID* em detrimento ao *entityName*. A desvantagem do uso do *baseCertificateID* é que a validade do certificado de atributos passa a ser atrelada à validade do certificado de identidade. Como a duração dos certificados de identidade é da ordem de grandeza de anos e normalmente eles são emitidos para uma finalidade específica, esta adoção não traria maior complexidade operacional ao sistema.

```

Holder ::= SEQUENCE {
    baseCertificateID  [0] IssuerSerial OPTIONAL,
    -- the issuer and serial number of the holder's PKC
    entityName        [1] GeneralNames OPTIONAL,
    -- the name of the claimant or role
    objectDigestInfo [2] ObjectDigestInfo OPTIONAL
    --used to directly authenticate the holder, ex: an executable
}

```

Já o campo *objectDigestInfo* tem como objetivo identificar, ao invés de uma entidade (empresa), um objeto, como um código executável, por exemplo. Para o caso de televisão

digital esta opção é muito útil para determinar não as permissões da instituição que gera um software, mas as permissões de um aplicativo propriamente dito. Neste caso, o certificado de atributos torna-se peça importante para limitar as permissões de aplicações interativas e para *softwares* homologados, permitindo um controle mais rígido de permissões de instalação de produtos em receptores.

```

ObjectDigestInfo ::= SEQUENCE {
    digestedObjectType  ENUMERATED {
        publicKey          (0),
        publicKeyCert      (1),
        otherObjectTypes   (2) },
    otherObjectTypeID   OBJECT IDENTIFIER OPTIONAL,
    digestAlgorithm     AlgorithmIdentifier,
    objectDigest        BIT STRING
}

```

digestedObjectTypes: Este campo identifica o tipo de arquivo ao qual o certificado de atributos estaria associado. Poderia ser a uma chave pública (*publicKey*) ou a um certificado de chave pública (*publicKeyCert*) diretamente, sendo desta maneira uma outra forma de associação de atributos a uma entidade. Já utilizando a opção outro tipo de objeto (*otherObjectTypes*), abre a possibilidade de associação do certificado de atributos a um objeto. Segundo Farrel e Housley (2002), não seria permitido o uso da opção *otherObjectTypes*, apenas a associação a chave pública ou a certificados de identidade. Para permitir a atribuição de permissões também por aplicativos, será considerada permitida a utilização deste campo, gerando uma não conformidade com a especificação de Farrel e Housley (2002). Para a utilização deste mecanismo, o *hash* deve ser calculado sobre o arquivo *hash.file* no mesmo nível em que será enviado o pacote *CMS Signed Data*.

otherObjectTypeID: campo opcional utilizado para identificar o tipo do objeto, não será utilizado nesta proposta.

digestAlgorithm: identifica o algoritmo utilizado para cálculo do *hash* do pacote. Como apresentado no item anterior, cálculo da função *hash*, será utilizado o algoritmo SHA-1.

```

DigestAlgorithmIdentifier::
sha-1 OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) oiw(14)

```

```
secsig(3) algorithm(2) 26 }
```

objectDigest: contém o valor do código *hash* do objeto que está recebendo os privilégios. O relacionamento é realizado pelo valor do *hash*.

issuer: voltando aos campos do *acinfo*, o *issuer* identifica o emissor do certificado de atributos. Segundo Farrel e Housley (2002), o certificado de atributos deve utilizar a opção *v2Form*, o qual deve conter apenas um nome no campo *GeneralName*. Os campos *baseCertificateID* e *objectDigestInfo* devem ser omitidos. Dessa forma, sem a utilização da identificação do certificado de identidade do emissor do certificado de atributos, pode haver várias opções de certificado de identidade do emissor, podendo ser formadas diferentes cadeias de confiança no verificador.

Além disso, a identificação do *issuer* deve ser desvinculada de um certificado de identidade específico, pois os certificados de identidade das entidades que receberam privilégios não podem estar vinculados ao certificado da autoridade de atributos no momento da emissão de seus certificados. Inclusive o detentor do certificado de atributos nem teria o controle da validade do certificado da sua autoridade de atributos.

```
AttCertIssuer ::= CHOICE {
  v1Form GeneralNames,
  v2Form [0] V2Form
}

V2Form ::= SEQUENCE {
  issuerName GeneralNames OPTIONAL,
  baseCertificateID [0] IssuerSerial OPTIONAL,
  objectDigestInfo [1] ObjectDigestInfo OPTIONAL
}
```

signature: contém o identificador do algoritmo a ser utilizado na assinatura digital do certificado de atributos. Este campo deve ser preenchido por identificadores definidos por Polk ET AL (2002) na RFC 3279. Nessa proposta será considerado o uso de RSA SHA-1 1024bits, como definido pela ICP Brasil atualmente para os tipos de certificados selecionados.

```
pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) 1}
sha1WithRSAEncryption OBJECT IDENTIFIER ::= { pkcs-1 5 }
```

serialNumber: número de identificação do certificado de atributos. Ele deve ser único para um dado emissor, tornando a concatenação *issuer/serialNumber* única. Farrel e Housley (2002) propõem o intervalo de valores para o número de série de certificados de 4 a 20 octetos. Será utilizada nesta proposta a mesma definição.

atrCertValidityPeriod: especifica o período de tempo para o qual os atributos delegados ao destinatário serão válidos. O tipo utilizado para tempo é o *GeneralizedTime*, definido pelo padrão ASN.1. Farrel e Housley (2002) propõem o preenchimento do campo *GeneralizedTime* com padrão UTC (*Coordinated Universal Time*), ou seja, com o horário de *Greenwich* e deve incluir segundos (formato: YYYYMMDDHHMMSSZ). Não é proposta nenhuma alteração neste item.

```
AttCertValidityPeriod ::= SEQUENCE {
  notBeforeTime GeneralizedTime,
  notAfterTime GeneralizedTime
}
```

attributes: este campo possui os atributos que determinarão os privilégios do *holder*. Farrel e Housley (2002) determinam as seguintes regras que também serão utilizadas nesta proposta: cada certificado de atributo não pode possuir duas entradas do mesmo tipo de atributo, mas para um dado tipo, pode ser alocado mais de um valor e deve haver pelo menos um atributo definido no certificado. Os atributos para TV digital serão apresentados no item 3.3.1.10.

```
Attribute ::= SEQUENCE {
  type AttributeType,
  values SET OF AttributeValue
  -- at least one value is required
}

AttributeType ::= OBJECT IDENTIFIER
AttributeValue ::= ANY DEFINED BY AttributeType

IetfAttrSyntax ::= SEQUENCE {
  policyAuthority [0] GeneralNames OPTIONAL,
  values SEQUENCE OF CHOICE {
    octets OCTET STRING,
    oid OBJECT IDENTIFIER,
    string UTF8String
  }
}
```

extensions: as extensões são utilizadas para adicionar informações sobre o certificado de atributos propriamente dito, não sobre a entidade a qual ele se refere. As extensões serão as mesmas propostas por Farrel e Housley (2002). As extensões lá definidas são: *Audit Identity*, *AC Targeting*, *Authority Key Identifier*, *Authority Information Access*, *CRL Distribution Points*, *No Revocation Available*. Neste trabalho será explorada a extensão *AC Targeting*, considerando a sua aplicação ao cenário brasileiro.

Audit Identity: esta extensão é utilizada para permitir auditoria sobre o detentor do certificado de atributos. Ela é utilizada para registro de transações efetuadas, não identificando o detentor diretamente, mas um número de registro. O emissor do certificado de atributos, e somente ele, pode identificar o detentor com este valor de registro, caso seja identificada uma ação maliciosa deste detentor. Esta é uma extensão crítica (deve ser interpretada pelo leitor do certificado de atributos).

```

name id-pe-ac-auditIdentity
OID { id-pe 4 }
syntax OCTET STRING -- MUST be longer than zero octets. MUST NOT be
longer than 20 octets.
criticality MUST be TRUE

```

AC Targeting: Esta extensão é utilizada para delimitar o grupo de receptores que deve interpretar o certificado de atributos. Ela contém uma lista dos receptores que devem ler o certificado e caso o receptor atual não faça parte desta lista o certificado deve ser descartado. Caso a extensão não exista, todos os receptores devem interpretar o certificado. Sintaxe a ser utilizada:

```

Targets ::= SEQUENCE OF Target

Target ::= CHOICE {
targetName [0] GeneralName,
targetGroup [1] GeneralName,
targetCert [2] TargetCert
}

TargetCert ::= SEQUENCE {
targetCertificate IssuerSerial,
targetName GeneralName OPTIONAL,
certDigestInfo ObjectDigestInfo OPTIONAL
}

```

A opção `targetCert` na estrutura `Target` não deve ser utilizada nesta proposta, sendo suficiente que o tipo do receptor seja coincidente com algum dos campos `targetName` ou `targetGroup`.

```
name id-ce-targetInformation
OID { id-ce 55 }
syntax SEQUENCE OF Targets
criticality MUST be TRUE
```

Para esta proposta serão definidos grupos e nomes para seleção dos receptores alvo. Os nomes identificam o receptor propriamente dito, enquanto grupo identifica a categoria do receptor. Para atribuição do *nome* foi considerada uma identificação definida pelo SBTVD para atualização de *software*, ABNT NBR 15603-2 (2007). São conjuntos de bits que definem unicamente o fabricante e outro conjunto que define unicamente o modelo do receptor para um dado fabricante (campos *maker_id* e *model_id*, utilizados na atualização de *software*).

Já os grupos foram divididos de acordo com as características mais importantes para receptores levando-se em consideração a execução de aplicativos: se são fixos ou móveis, se possuem canal de retorno ou não e se há suporte a aplicativos interativos ou não (presença do *middleware* Ginga).

Grupos:

```
Receptores SBTVD interativos one-seg com suporte a canal de retorno
(com suporte a Ginga)
Receptores SBTVD interativos full-seg com suporte a canal de retorno
(com suporte a Ginga)
Receptores SBTVD interativos one-seg (com suporte a Ginga)
Receptores SBTVD interativos full-seg (com suporte a Ginga)
Receptores SBTVD não interativos one-seg (sem suporte a Ginga)
Receptores SBTVD não interativos full-seg (sem suporte a Ginga)
```

Nomes:

```
Concatenação: Maker_id + Flag Model_id + Model_id (caso o flag de
model_id seja 1 o campo Model_id é considerado, caso contrário, não).
```

Authority Key Identifier: conforme definido por Housley ET AL (2002) na RFC 3280, esta extensão auxilia a verificação da assinatura do emissor do certificado de atributos. Suporte opcional.

```
name id-ce-authorityKeyIdentifier
OID { id-ce 35 }
syntax AuthorityKeyIdentifier
criticality MUST be FALSE
```

Authority Information Access: conforme definido por Housley ET AL (2002). Auxilia na verificação do status de revogação do certificado de atributos. Suporte opcional.

```
[OCSP]:
id-ad-ocsp OBJECT IDENTIFIER ::= { id-ad 1 }
name id-ce-authorityInfoAccess
OID { id-pe 1 }
syntax AuthorityInfoAccessSyntax
criticality MUST be FALSE
```

CRL Distribution Points: conforme definido por Housley ET AL (2002). Auxilia na verificação do status de revogação do certificado de atributos por acesso a um ponto de distribuição na Internet. Suporte opcional.

```
name id-ce-cRLDistributionPoints
OID { id-ce 31 }
syntax CRLDistPointsSyntax
criticality MUST be FALSE

--MUST use the DistributionPointName option;
--MUST contain a fullName, which MUST contain a single name form;
--MUST contain either a distinguished name or a URI;
--The URI MUST be either an HTTP URL or an LDAP URL [URL].
```

No Revocation Available: Definido na ITU-T X.509 (2005), indica que não há informação de revogação para este certificado.

```
name id-ce-noRevAvail
OID { id-ce 56 }
syntax NULL (i.e. '0500'H is the DER encoding)
criticality MUST be FALSE
```

signatureAlgorithm: voltando aos campos diretos do certificado de atributos, o *signatureAlgorithm* contém o identificador do algoritmo a ser utilizado na assinatura digital do certificado de atributos. Este campo deve ser preenchido por identificadores definidos por Polk ET AL (2002). Nessa proposta será considerado o uso de RSA SHA-1 1024bits, como definido pela ICP Brasil atualmente para os tipos de certificados aplicáveis à proposta.

```
pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) 1}
rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1}
sha1WithRSAEncryption OBJECT IDENTIFIER ::= { pkcs-1 5 }
```

signatureValue: contém a assinatura digital do certificado de atributos, identificando o seu emissor. O emissor do certificado de atributos deve ter permissão para delegar privilégios e deve ter a sua assinatura autenticada por uma cadeia de certificados de identidade.

3.3.1.9 CMS Signed Data

Conforme a premissa de utilização de padrões abertos, a proposta deste trabalho é utilizar a estrutura definida pela RFC3852, *Cryptographic Message Syntax – Signed Data*, proposta por Housley (2008). Esta estrutura permite o armazenamento de certificados digitais, lista de certificados revogados, assinaturas digitais e dados assinados. Apesar de ser possível enviar o arquivo assinado internamente à estrutura *CMS Signed Data*, o arquivo a ser assinado, *hash.file*, será mantido externo a esta estrutura conforme definido anteriormente em **cálculo da função hash**. Os detalhes de uso desta estrutura estão apresentados a seguir.

Um diretório de objetos contém um pacote CMS no seu topo. Estes arquivos devem ser nomeados *CMS.SignedData*, e possuem as informações relacionadas à assinatura do arquivo *hash.file* que está no mesmo nível que ele.

O arquivo *CMS.SignedData* possui a seguinte estrutura (notação ASN.1):

```
SignedData ::= SEQUENCE {
    version CMSVersion,
    digestAlgorithms DigestAlgorithmIdentifiers,
    encapContentInfo EncapsulatedContentInfo,
    certificates [0] IMPLICIT CertificateSet OPTIONAL,
    crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
    signerInfos SignerInfos
}
```

Version: indica o conteúdo e a sintaxe do *CMS Signed Data* de acordo com o seu conteúdo. Para o uso em TV Digital proposto, a versão seria 4.

```
IF ((certificates is present) AND (any certificates with a type of
other are present)) OR ((crls is present) AND (any crls with a type of other
are present))
```

```

THEN version MUST be 5
ELSE
  IF (certificates is present) AND (any version 2 attribute
certificates are present)
THEN version MUST be 4
ELSE
  IF ((certificates is present) AND (any version 1 attribute
certificates are present)) OR (any SignerInfo structures are version 3)
OR (encapContentInfo eContentType is other than id-data)
THEN version MUST be 3
ELSE
  version MUST be 1

```

digestAlgorithms: este campo possui uma lista de algoritmos para cálculo de códigos *hash* utilizados para as diferentes assinaturas do conteúdo assinado. Pode ter qualquer tamanho, inclusive zero. Caso o algoritmo utilizado não esteja nesta lista, a verificação da assinatura digital pode falhar, segundo Housley (2008). Nesta proposta será aceito o algoritmo SHA-1:

```

DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier
sha-1 OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) oiw(14)
secsig(3) algorithm(2) 26 }

```

encapContentInfo é o conteúdo assinado. Possui um identificador de tipo e o conteúdo propriamente dito.

```

EncapsulatedContentInfo ::= SEQUENCE {
eContentType ContentType,
eContent [0] EXPLICIT OCTET STRING OPTIONAL }

```

eContentType: identificador do tipo de conteúdo, que deve indicar *CMS SignedData*, conforme abaixo:

```

ContentType ::= OBJECT IDENTIFIER
id-signedData OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs7(7) 2 }

```

eContent: possui o conteúdo propriamente dito. Segundo Housley (2008) pode ser omitido para permitir a assinatura de conteúdos externos. Como o CMS contém a assinatura sobre o arquivo *hash.file*, o *eContent* deve ser omitido. Neste caso os campos *signatureValue* e *eContentType* são preenchidos como se o *eContent* estivesse presente.

Certificates: possui as cadeias de certificados, tanto de identidade como de atributos. Pode haver mais de uma cadeia de certificados, independentemente dos tipos. Os tipos de certificados que podem ser selecionados no *CMS Signed Data* são: PKCS #6 estendido, certificado de identidade ITU-T X.509 (2005), versão 1 do certificado de atributos ITU-T X.509 (1997), versão 2 do certificado de atributos ITU-T X.509 (2000), ou outro tipo genérico de certificado. Os certificados utilizados para o ambiente de televisão digital devem ser certificado de identidade ITU-T X.509 (2005), ICP Brasil, e versão 2 do certificado de atributos ITU-T X.509 (2005).

```
CertificateSet ::= SET OF CertificateChoices

CertificateChoices ::= CHOICE {
    certificate          Certificate,
    -- certificado de identidade X.509
    extendedCertificate  [0] IMPLICIT ExtendedCertificate,
    -- Obsoleto, não deve ser utilizado
    v1AttrCert          [1] IMPLICIT AttributeCertificateV1,
    -- Obsoleto, não deve ser utilizado
    v2AttrCert          [2] IMPLICIT AttributeCertificateV2,
    -- certificado de atributo X.509
    other                [3] IMPLICIT OtherCertificateFormat
    -- não deve ser utilizado
}

AttributeCertificateV2 ::= AttributeCertificate
```

CRLs (*Certificate revocation lists*): possui a lista de certificados revogados. Este lista pode conter uma lista de certificados de identidade ou de certificados de atributos revogados; já que ambos possuem a mesma sintaxe. Caso um certificado seja considerado revogado, ele deve ser descartado nas verificações.

```
RevocationInfoChoices ::= SET OF RevocationInfoChoice

RevocationInfoChoice ::= CHOICE {
    crl CertificateList,
    other [1] IMPLICIT OtherRevocationInfoFormat
    -- não sera utilizado
}
```

signerInfos: é um pacote de informações sobre uma assinatura digital. O *CMS Signed Data* pode possuir mais de um pacote deste tipo, para o caso de haver uma série de assinaturas

sobre o mesmo pacote. O item assinatura digital deste capítulo contém o detalhamento deste pacote de informações.

```
SignerInfos ::= SET OF SignerInfo
```

3.3.1.10 Atributos para TV digital

Para aplicação da proposta apresentada para a autenticação de aplicativos, foram identificados os seguintes privilégios, aplicados aos casos de uso identificados neste trabalho. Exemplos da aplicação destes privilégios nos casos de uso identificados estão descritos nos itens: 3.3.2. São eles:

- privilégio de alteração do software residente;
- privilégio delegação de alteração do software residente;
- privilégio para rodar executável;
- privilégio para delegação para rodar executável;
- privilégio de construção de aplicativo Ginga;
- delegação do privilégio de construção de aplicativo Ginga;
- privilégio de aplicação Ginga;

Cada um destes privilégios deve receber um nome em inglês e serão empregados em estrutura como a apresentada a seguir:

```
attributeType:
id-sbtvd-entity-allowed OBJECT IDENTIFIER ::= {definir}
attributeValue
SbtvdEntityAllowed ENUMERATED {
ReceiverSoftwareUpdate (0),
ReceiverExecLoading (1),
interactiveTVContentProduction (2),
}
```

Os privilégios de aplicativos Ginga referem-se às permissões de aplicativo interativo

com execução sobre o *middleware* Ginga do SBTVD, que requerem acesso a recursos críticos e precisam ter um arquivo associado que determinam quais chamadas de softwares (APIs) podem ser utilizadas pelo aplicativo. No GEM é utilizado um arquivo em formato XML para fazer requisição de uso de APIs protegidas. No caso desta proposta será utilizado também um arquivo XML, que será inserido no certificado de atributos do objeto (aplicativo interativo). Como a definição das APIs do *middleware* não está no escopo deste trabalho, o arquivo de solicitação de acesso aos métodos e funções do *middleware* não será detalhado aqui. Um exemplo da estrutura do arquivo segue abaixo:

```
xmlPrivilegeInfo ATTRIBUTE ::= {
  WITH SYNTAX UTF8String -- contains XML-encoded privilege information
  ID id-at-xMLPrivilegeInfo }
```

Exemplo de uso de schema para atributos::

```
<schema xmlns="http://www.w3.org/2000/08/XMLSchema">
<element name="role">
  <attribute name="id" type="ID"/>
  <complexType>
<sequence>
<element name="authorities">
<complexType>
<sequence>
  <element name="authority" type="string" minOccurs="1"
maxOccurs="*" />
</sequence>
</complexType>
</element>
<element name="name" type="string"/>
</sequence>
</complexType>
</element>
</schema>
```

3.3.1.11 Mecanismo de autenticação de aplicativos

Para a realização da autenticação de aplicativos os seguintes passos devem ser seguidos pelo sistema:

- Verificação das requisições de permissões que o pacote está realizando para decidir se há necessidade de autenticação
- Recebimento e verificação da integridade do pacote recebido
- Identificação do pacote *CMS.SignedData*.
- Verificação se há subdiretórios no local onde se encontra este pacote.
- Em caso afirmativo, para cada arquivo a partir da base da estrutura de diretórios:
 - Verificar se o arquivo está listado no *hash.file*.
 - Verificar se o valor do *hash* do arquivo corresponde ao informado no *hash.file*.
 - Checar o *hash* de cada arquivo indo da base para o topo da árvore de diretórios até chegar a um nível com o CMS.
 - Comparar o valor de *hash* do arquivo *hash.file* no mesmo nível que o *CMS.SignedData* com o atributo *DigestMessage* no campo *SignerInfo* no CMS.
- Verificação da assinatura do pacote
 - Leitura do SID do emissor (identifica quem assinou o pacote).
 - Recuperação do certificado de identidade do emissor do pacote e da sua cadeia de certificados de identidade.
 - Verificação se o certificado raiz da cadeia de certificados faz parte dos certificados de confiança do receptor.
 - Verificação da validade temporal do certificado (data de início de validade e de expiração).
 - Recuperação da lista de certificados revogados e verificação da validade do certificado. – caso tenha canal de retorno, verificação da lista de certificados revogados por URI caso seja informado

- Verificação criptográfica da assinatura do pacote;
- Verificação criptográfica da cadeia de certificados raiz (autenticação).
- Caso a verificação da assinatura do pacote não tenha sucesso, será necessário procurar outra assinatura digital válida para o pacote.
- Verificação da autorização para uso dos recursos:
 - Obter o certificado de atributo da área de certificados;
 - Verificação da estrutura do certificado de atributos:
 - Verificação da existência de extensões críticas não suportadas.
 - Verificação se o receptor encontra-se no grupo-alvo do certificado de atributo.
 - Verificação da validade temporal do certificado de atributos (data de início de validade e de expiração);
 - Recuperação da lista de certificados revogados e verificação da validade do certificado – caso tenha canal de retorno, verificação da lista de certificados revogados por URI caso seja informado;
 - Verificação da assinatura do certificado de atributo. Isto corresponde a realizar a verificação do certificado de identidade da entidade signatária e da sua cadeia de certificação – que deve fazer parte da cadeia de confiança do receptor, a verificação criptográfica, a verificação da validade do certificado de identidade;
 - Verificar se a autoridade emissora (*issuer*) é uma das entidades autorizadas a emitir o certificado com os atributos que o certificado apresenta. Verificar a cadeia de certificados de atributos para verificar a delegação a partir das autoridades de atributos de confiança.
 - Caso o campo *holder* indique uma entidade: Obter o valor contido no atributo “*holder*” e verificar se corresponde à mesma entidade signatária do pacote de atualização;
 - Caso o campo *holder* indique um objeto: Obter o valor contido no atributo “*holder*” e verificar se corresponde ao código *hash* do arquivo *hash.file* no mesmo nível que o CMS;

- Obter o valor contido no atributo e verificar se a permissão corresponde ao tipo de permissão solicitada.
- Caso a verificação do certificado de atributos não tenha sucesso, será necessário procurar outra cadeia de certificados de atributo válida para o pacote.

Caso todos os passos sejam executados com sucesso, o objeto que requer a permissão solicitada pode realizar a operação, caso contrário, a operação não é executada e os arquivos relacionados são eliminados.

3.3.2 O sistema AUTV aplicado a casos de uso

Nesta seção será apresentado como o sistema AUTV poderia ser aplicado aos casos de uso de segurança em serviços de TV digital, além disso, para cada caso de uso serão feitas considerações em relação às conseqüências na falha de autenticação dos aplicativos para o sistema.

3.3.2.1 Caso de uso: Serviço de engenharia

O caso de uso de serviço de engenharia trata da atualização do software do receptor, que pode ser determinada como a substituição da região de memória do receptor com o sistema de arquivos, incluindo sistema operacional e software residente, excluindo-se a região de memória com os dados de usuário (configurações e base de dados). A falha de autenticação de um pacote de atualização para o receptor poderia resultar no descarte do pacote de atualização ou à consulta ao usuário final em relação à ação a ser tomada.

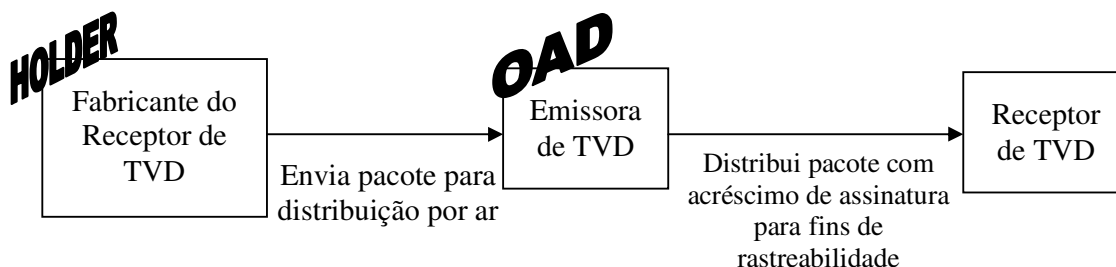


Figura 31. Estudo de caso: atualização do software residente de um receptor.

Legenda:

OAD é o mecanismo de *ON AIR DOWNLOAD* que trata do envio de pacotes de dados para atualização juntamente ao TS pelas emissoras de TV.

HOLDER: Não tem privilégio de delegação, apenas requer seus privilégios pela apresentação do seu certificado de atributo.

O cenário mais simples para o serviço de engenharia é aquele que envolve o Fabricante do Receptor de TVD, a Emissora de TVD e o Receptor de TVD. Neste caso, o Fabricante do Receptor de TVD agiria como detentor de privilégio e a permissão que ele utilizaria seria a de **privilégio de alteração do software residente**. O Fabricante do Receptor de TVD envia para o Receptor de TVD, por intermédio da Emissora de TVD, os pacotes de atualização assinados com os dados associados para autenticação (arquivos de *hash* e arquivo contendo o CMS com certificados e assinaturas). A Emissora de TVD envia os pacotes ao Receptor de TVD por meio de mecanismo denominado OAD (*On Air Download*), que é o envio de pacotes de atualização por meio do carrossel de dados do DSM CC, junto ao seu TS. Para fins de rastreabilidade, a Emissora de TVD pode inserir a sua assinatura no CMS, permitindo posteriormente atestar por qual emissora foi enviado o pacote. Este caso está representado na Figura 31.

Pode ser delineada uma variante a este caso de uso, considerando o serviço de um terceiro para a geração dos pacotes de atualização de *software*. Neste caso o Fabricante de Receptor de TVD possuiria o **privilégio de delegação de alteração do software residente**, o que lhe permitiria delegar o privilégio de alteração de software residente ao Terceiro. Esta delegação de privilégios pode ser realizada para a entidade, pelo seu nome definido no campo *holder*, com controle de tempo pelo campo de validade do certificado de atributos, ou vinculando a delegação de privilégio a um dado **objeto**, através da determinação de um

ObjectDigestInfo, no campo *holder* do certificado de atributos.

Neste caso, como o Fabricante do Receptor de TVD emite um certificado de atributos para o Terceiro ou para o pacote de atualização gerado pelo Terceiro, o Fabricante do Receptor de TVD age como uma Autoridade de Atributos (AA). Esta AA será responsável por gerar os certificados de atributos que devem ser anexados às assinaturas dos pacotes de atualização de *software*.

Para realizar a atualização por um terceiro, o Fabricante do Receptor de TVD gera um certificado de atributos para o Terceiro com o **privilegio de alteração do software residente**. O terceiro gera o pacote de atualização e o envia com os arquivos *CMS.SignedData* e *hash.file*, contendo a assinatura do pacote, os certificados de atributo e de identidade associados além da lista de certificados revogados associada. A **emissora de TVD** recebe o conjunto, insere a sua assinatura no arquivo *CMS.SignedData* para fins de rastreabilidade e os transmite pelo ar. O **receptor de TVD** recebe o pacote e realiza a atualização.

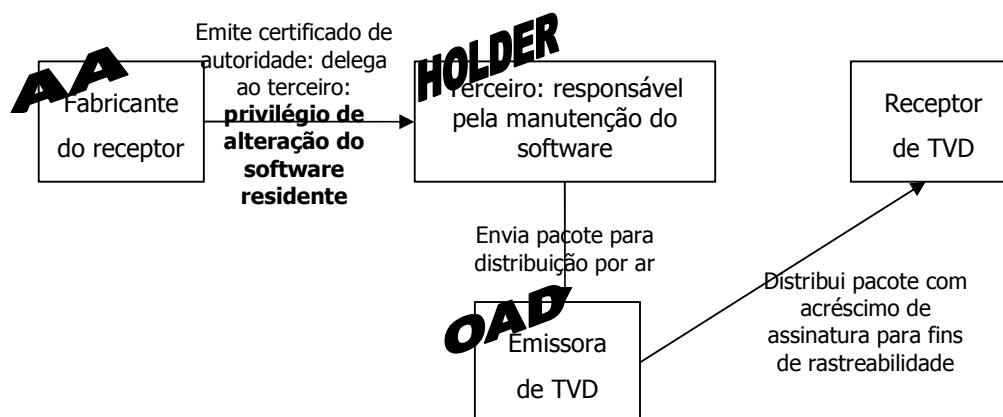


Figura 32. Estudo de caso: atualização do software residente de um receptor.

Legenda:

AA é a Autoridade de atributos. Pode gerar certificados de atributos ou apenas requerer um dado privilégio, agindo como HOLDER.

OAD é o mecanismo de ON AIR DOWNLOAD que trata do envio de pacotes de dados para atualização juntamente ao TS pelas emissoras de TV.

HOLDER: Não tem privilégio de delegação, apenas requer seus privilégios pela apresentação do seu certificado de atributo.

Para realizar a atualização por um terceiro, limitando o privilégio apenas para um pacote de atualização específico, o Fabricante de Receptor de TVD deve gerar um certificado de atributos para o **pacote de atualização** utilizando o código *hash* do pacote, ao invés de para o Terceiro. O pacote de atualização deve possuir o **privilégio de alteração do software residente**. O Terceiro envia à Emissora de TVD o pacote com os arquivos *CMS.SignedData* e *hash.file*, contendo a assinatura do pacote, os certificados de atributo e de identidade associados, além da lista de certificados revogados associada. A **emissora de TVD** recebe o conjunto, insere a sua assinatura no arquivo *CMS.SignedData* para fins de rastreabilidade e os transmite pelo ar. O **receptor de TVD** recebe o pacote e realiza a atualização.

Outra maneira de limitar o privilégio do terceiro seria limitar a validade do certificado de atributo apenas para as datas programadas para a difusão do pacote de atualização.

3.3.2.2 Caso de uso: Conexão de um dispositivo

O Sistema Brasileiro de Televisão Digital considera o uso de uma interface genérica para conexão de dispositivos, segundo ABNT NBR 15604 (2007). Na primeira fase do projeto SBTVD, de pesquisa e desenvolvimento, foi elencada a porta USB para esta finalidade, inclusive para conexão de *modems*. O emprego de uma única porta para a conexão de diversos aplicativos melhora a usabilidade do sistema, como apresentado em LSI-TEC (2006) e simplifica o projeto de *hardware*, mas traz a necessidade de instalação de *drivers*.

A interface USB possui *drivers* genéricos e permite a importação de *drivers* do próprio dispositivo para o receptor. Por outro lado, a recepção livre de arquivos executáveis pela interface USB seria um ponto de grande vulnerabilidade no sistema. Por isso, torna-se importante a autenticação dos aplicativos recebidos pela interface genérica, evitando a instalação de aplicativos maliciosos ou a danificação do sistema por aplicativos inadequados.

Caso a autenticação do *driver* não seja executada com sucesso, o *driver* poderia ser desconsiderado pelo sistema, impedindo a sua instalação no receptor, ou o receptor poderia solicitar ao usuário final decidir quanto à instalação do *driver*. Este tratamento para falha de autenticação é o mesmo do caso de uso de serviço de engenharia.

O AUTV permite que o fabricante de dispositivo que fará uso de porta genérica e não possua um *driver* padrão, homologue os *drivers* ou os fabricantes de *drivers*, disponibilizando para os mesmos um certificado de atributos contendo o **privilégio de rodar executável** e utilizando a extensão de definição de grupo alvo para determinar para quais receptores cada *driver* seria relacionado.

A Figura 33 apresenta um exemplo deste caso de uso com a realização de homologação do fabricante de *drivers*. As entidades que fariam parte deste caso de uso são: o Fabricante do Receptor de TVD, Fabricante de Dispositivo Externo e Receptor de TVD.

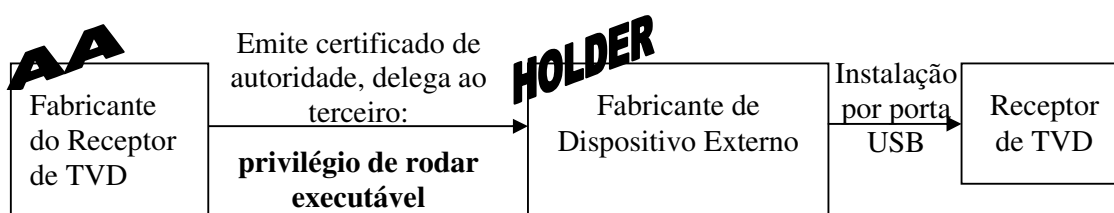


Figura 33. Estudo de caso: instalação de dispositivo externo.

O Fabricante do Receptor de TVD age como Autoridade de Atributos, possui **privilégio de delegação para rodar executável**.

O Fabricante de Dispositivo Externo passa por um processo homologatório com um ou mais entidades que tenham o papel de Fabricante de Receptor de TVD e recebe de cada um, um certificado de atributos lhe dando **privilégio de rodar executável** no receptor, limitando o grupo alvo para os receptores adequados, de acordo com modelo e fabricante.

O Fabricante de Dispositivo Externo gera o pacote de atualização e o envia com os arquivos *CMS.SignedData* e *hash.file*, contendo a assinatura do pacote, os certificados de atributos, recebidos de um ou mais Fabricantes de Receptores de TVD, e certificados de identidade, além da lista de certificados revogados associados. O pacote é inserido na memória interna do dispositivo externo junto aos *drivers* de instalação.

Quando o usuário final conecta o dispositivo externo, o receptor deve verificar se há privilégio para fazer a instalação naquele receptor e a autenticidade dos arquivos, depois disso a instalação poderia ser feita de maneira automática e transparente.

Este caso de uso poderia ser estendido para que fosse realizada homologação sobre o *driver*, neste caso o certificado de atributos seria gerado para o *driver* propriamente dito.

3.3.2.3 Caso de uso Execução local de aplicativo interativo com uso de recursos críticos

Os aplicativos interativos são executados utilizando as APIs definidas na especificação de um *middleware* de TV digital. Algumas destas APIs são consideradas inofensivas, outras podem permitir que aplicativos maliciosos prejudiquem o modelo de negócios da televisão digital e a experiência, ou até mesmo a privacidade, do usuário. Os aplicativos que fazem uso destas APIs que trazem algum risco são denominados aplicativos interativos com uso de recursos críticos.

Por isso, é necessário definir uma política de segurança para aplicativos interativos, que classifique as APIs do *middleware* em nível de periculosidade e que determine como liberar os recursos aos aplicativos que necessitem destas APIs. O GEM utiliza o conceito de caixa de areia, que determina um conjunto de APIs inofensivas, às quais todos os aplicativos interativos podem utilizar sem ser necessário ter nenhum privilégio. No GEM, para as demais APIs, é necessário ter privilégios especiais e ter a aceitação do usuário. Nesta proposta será aproveitado o conceito de caixa de areia, fazendo uma proposta diferenciada no mecanismo de atribuição de privilégios.

Como exemplo, os privilégios de acesso poderiam ser delegados pela divisão das APIs do *middleware* nos seguintes conjuntos:

- Controle de outros aplicativos
- Persistência da aplicação
- Acesso a arquivos
- Acesso ao canal de interatividade
- Acesso às preferências de usuário
- Controle do *front-end*
- Controle de seleção de serviço
- Controle de multimídia

A categorização destes grupos de APIs para determinar se elas estão dentro ou fora da caixa de areia é realizada considerando se elas dão acesso a recursos escassos do receptor

(como ao canal de retorno ou à memória persistente, por exemplo), que pudesse ser considerado de risco para a privacidade do usuário ou ainda que permita tomar o controle do receptor (uma aplicação com controle ao *front-end* pode impedir a troca de canais, por exemplo).

Para que um aplicativo possa fazer uso de um método que requer privilégio, é necessário que o usuário do receptor de TV tenha liberado este uso. No GEM a solicitação de permissões para os aplicativos é realizada por um XML enviado na estrutura de diretórios do carrossel de objetos. Um aplicativo assinado, com um pedido de privilégios já estaria apto a receber as permissões solicitadas, dependendo apenas de uma autorização do usuário. No AUTV, será considerado o uso do conceito de caixa de areia e é o certificado de atributos que carrega os privilégios do aplicativo interativo, podendo também haver a necessidade da autorização/configuração do usuário para liberar o acesso de fato do aplicativo.

Os objetos, ou seja, as aplicações interativas recebem privilégios por meio de um atributo XML, denominado **privilégio de aplicação Ginga**, que agrupa os métodos disponibilizados pela API do *middleware*, estabelecendo as permissões deste aplicativo. O aplicativo pode receber o **privilégio de aplicação Ginga** por delegação de uma instituição que tenha **privilégio de construção de aplicativo Ginga**.

A fonte de autoridade do receptor de TV digital no que tange aplicativo interativo deve ser de uma instituição de confiança do SBTVD. Esta entidade será denominada Entidade de Confiança do SBTVD e delega os atributos **delegação de privilégio de construção de aplicativo Ginga** e **construção de aplicativo Ginga**.

A atribuição dos privilégios **construção de aplicativo Ginga** e **delegação do privilégio de construção de aplicativo Ginga** são aplicáveis a entidades, pelo seu nome definido no campo *holder*, com controle de tempo pelo campo de validade do certificado de atributos. Já a atribuição do privilégio de **aplicação Ginga** é vinculado a um dado objeto, através da determinação de um *ObjectDigestInfo*, no campo *holder* do certificado de atributos. Uma vez que a entidade detenha o privilégio **construção de aplicativo Ginga**, ela pode emitir um certificado de atributos para objeto, delegando a ele o privilégio de **aplicação Ginga**.

Neste caso, a Entidade de Confiança do SBTVD está representando uma fonte de autoridade (Source Of Authority). Ele será responsável por gerar os certificados de atributo que darão às emissoras de TV o privilégio de produzirem aplicativos interativos e de tornarem-se autoridades de atributos (AA). Como AA, as emissoras podem delegar a um

objeto um conjunto de privilégios ou permitir que um terceiro produza aplicativos interativos, tornando-o uma AA para que por sua vez possa gerar certificado de atributo com **privilégio de aplicação Ginga**.

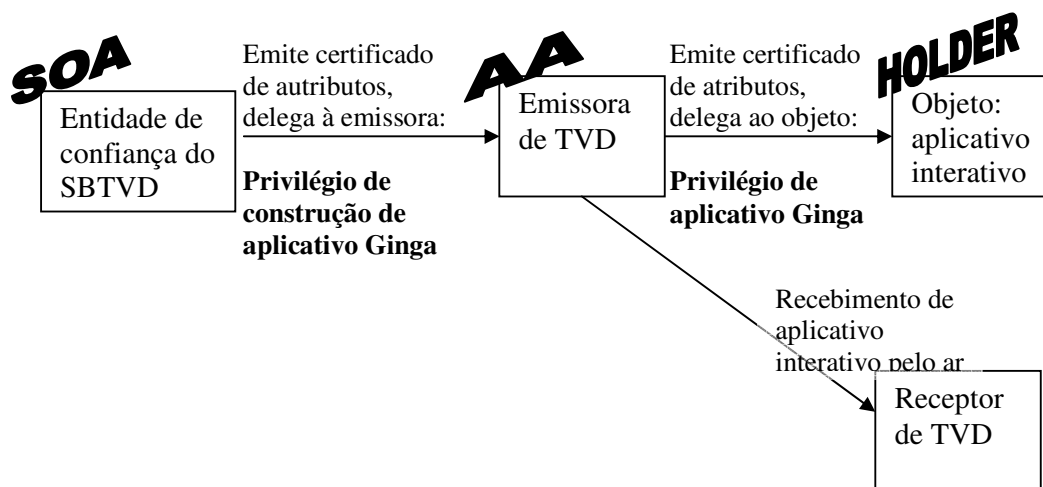


Figura 34. Estudo de caso: execução local de aplicativo interativo.

Os aplicativos interativos Ginga podem ser enviados por uma emissora de TV ou por alguma fonte alternativa, como pela Internet, por exemplo. Nos casos aqui apresentados, o aplicativo será enviado por uma emissora de TV.

A Emissora de TV possui a flexibilidade de delegar o privilégio de construção do aplicativo interativo a um terceiro ou ele pode assiná-lo ele mesmo. Mesmo com o uso de um terceiro para a construção do aplicativo, a emissora poderia ainda assinar o pacote para possibilitar a rastreabilidade da aplicação (identificação da emissora responsável pela sua transmissão).

A Figura 34 apresenta o caso em que a Emissora de TV desenvolve a aplicação interativa por conta própria. Neste caso a Emissora de TV possui um certificado de atributos, emitido pela Entidade de Confiança do SBTVD, com o privilégio **construção de aplicativo Ginga**. Desta maneira, a Emissora de TV gera o aplicativo interativo e um certificado de atributos destinado a ele (aplicativo interativo) com o atributo **privilégio de aplicação Ginga** (contendo a especificação de privilégios em XML para a execução deste aplicativo). A Emissora de TV envia por radiodifusão o aplicativo interativo e os pacotes com os arquivos

CMS.SignedData e *hash.file*. O receptor de TVD recebe o pacote e, caso as preferências do usuário o permitam, executa o aplicativo.

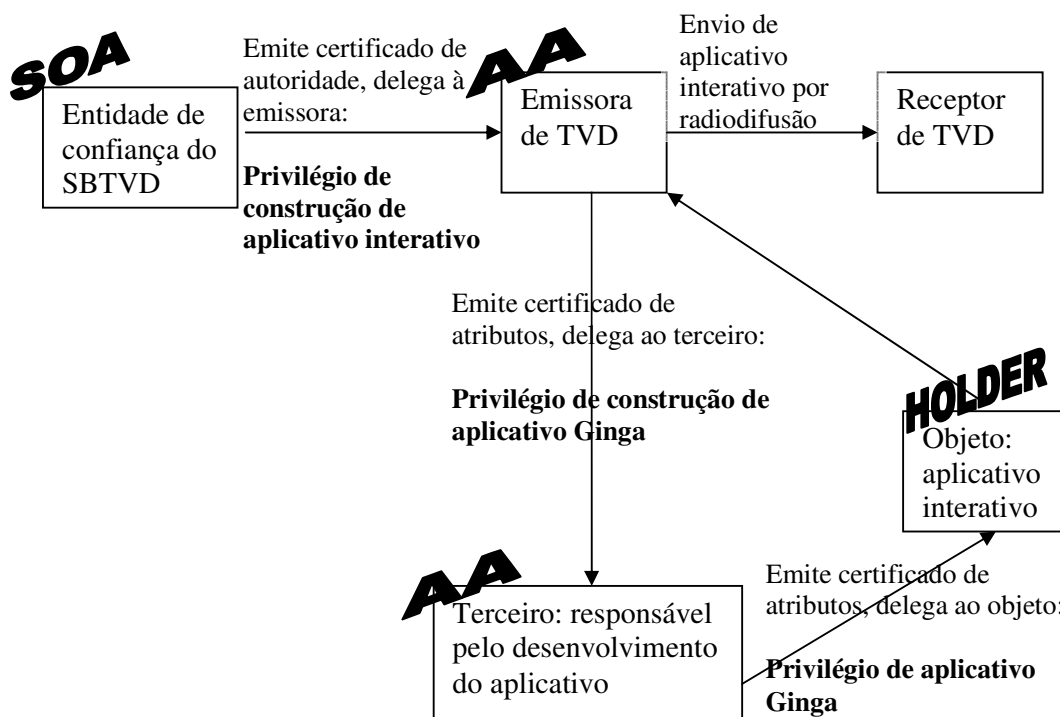


Figura 35. Estudo de caso: execução local de aplicativo interativo com Terceiro.

Para que o desenvolvimento seja de responsabilidade de um terceiro, como representado na Figura 35, a Emissora de TVD deve possuir um certificado de atributos com privilégio **delegação do privilégio de construção de aplicativo Ginga** e agir como autoridade de atributos gerando um certificado de atributos para o Terceiro com o **privilégio construção de aplicativo Ginga**. O terceiro gera o aplicativo e um certificado de atributos com **privilégio de aplicação Ginga**, determinando no atributo com formato XML as permissões necessárias para a execução do aplicativo. O Terceiro repassa para a Emissora de TVD o aplicativo e os arquivos *CMS.SignedData* e *hash.file*. A Emissora de TVD recebe o conjunto, insere a sua assinatura no arquivo *CMS.SignedData* para fins de rastreabilidade e os transmite pelo ar. O Receptor de TVD recebe o pacote e, com a anuência do usuário final, executa o aplicativo liberando os métodos críticos.

No caso de falha na autenticação do aplicativo, os privilégios do aplicativo interativo

devem ser limitados às APIs internas à caixa de areia. Desta maneira, o aplicativo poderia ser executado, mas de maneira parcial. Outra opção de tratamento de erro no caso de falha de autenticação do aplicativo seria o descarte deste aplicativo. Neste caso, o receptor apresentaria o áudio e vídeo do programa mas não apresentaria a opção de interagir com o programa pelo aplicativo Ginga.

3.4 Conclusão

Este capítulo apresentou a sistematização da segurança para televisão digital e as propostas das duas contribuições para o sistema de segurança do SBTVD, no caso uma contribuição para a proteção dos direitos autorais denominada SPDA-BR (Sistema de Proteção de Direitos Autorais Brasileiro) e a contribuição na área de autenticação de aplicativos denominada AUTV (AUtenticação de aplicativos para TV digital). Nos próximos parágrafos apresentaremos algumas conclusões acerca destas contribuições.

Na seção 3.2 foi apresentada a arquitetura de Proteção de Direitos Autorais do SPDA-BR, tendo por base a análise nos sistema de DRM atuais, em especial do ISDB-T. Foram propostas as seguintes contribuições ao sistema ISDB-T:

- Inclusão dos descritores que informam as regras de uso do conteúdo nas mensagens ECM utilizadas para envio de chaves;
- Inclusão de um **descritor de rastreamento** também enviado no interior das mensagens ECM;
- Inserção da chave de grupo, permitindo o uso de hierarquia de chaves;
- Uso conjunto da solução de cartão criptográfico e de uma solução embarcada, reduzindo o custo da lista de materiais inicial, mas permitindo flexibilidade ao sistema;
- Substituição do algoritmo MULTI-2 pelo AES.

As demais áreas do sistema de proteção de direitos autorais, que não receberam contribuições mantiveram-se conforme o sistema ISDB. As áreas de robustez e conformidade

de dispositivos são muito ligadas a produtos e aspectos legais de verificação de conformidade, não tendo sido abordadas no texto. Já em relação às ferramentas de descrição, apesar de existirem vários avanços na área, como nos padrões MPEG-7 e MPEG-21, no sistema de televisão digital terrestre, a descrição de conteúdo está intimamente relacionada aos multiplexadores. No Brasil, para minimização de custos, as alterações em norma não podem impactar os transmissores e multiplexadores. Por isso, a descrição do conteúdo segue de maneira geral a norma ARIB STD B10 (2002), conforme ABNT NBR 15606-3 (2007). Em relação às interfaces de saída, como há necessidade de interoperabilidade entre os produtos de mercado, não foram exploradas outras opções, já que o sistema ARIB contempla as interfaces utilizadas no mercado de eletrônicos de consumo.

Desta maneira, o sistema SPDA-BR possui as seguintes características:

- Linguagem de Definição de Direitos: descritores: controle de cópias, disponibilidade de conteúdo e descritor de rastreamento com envio não apenas no *transport stream*, mas também no interior das mensagens ECM.
- Esquema de proteção do conteúdo: uso de criptografia do conteúdo no nível da área útil dos pacotes de *transport stream* com algoritmo AES 128 bits CBC. Emprego de *hardware* criptográfico flexível, permitindo operação com o sistema embarcado ou com inserção de um cartão criptográfico tipo *smartcard*.
- Ferramentas de descrição – mecanismo conforme ao ARIB. Utiliza tabelas SI com informações do programa, contendo: gênero, classificação indicativa, sinopse, formato e codificação.
- Conformidade e robustez de dispositivos – não tratados neste trabalho, relacionados à produção e operação do sistema.
- Mecanismos de controle de conteúdo exportado pelas interfaces – mantido como no sistema ARIB, CGMS-A para vídeo componente, APS Macrovision para vídeo composto, HDCP para HDMI, DTCP para interfaces de TS e SCMS para SPDIF.

Outra contribuição deste capítulo foi na área de segurança de serviços, o AUTV, apresentado na seção 3.3, utilizado para a autenticação de aplicativos. Esta autenticação de aplicativos é interessante para os casos de uso de serviço de engenharia, conexão de dispositivo e execução local de aplicativo interativo com uso de recursos críticos. No AUTV foi desenvolvido um mecanismo de autenticação e delegação de privilégios compatível com a

infraestrutura brasileira de chaves públicas, a ICP-Brasil. Os casos de uso execução de aplicativo interativo com necessidade de canal de retorno e execução de aplicativo com necessidade de autenticação do usuário não foram considerados parte do escopo deste trabalho e devem ser considerados em trabalhos futuros decorrentes desta dissertação.

O mecanismo adotado para autenticação e delegação de privilégios faz uso conjunto do certificado de identidade compatível com a ICP-Brasil e de certificado de atributos com um perfil proposto especificamente para o cenário de televisão digital no Brasil. Este perfil difere do perfil adotado para a Internet, a sua principal diferença é a possibilidade de atribuir privilégios para aplicativos e enviar atributos por meio de formatação XML, o que é muito conveniente para o caso de uso de execução de aplicativo interativo avançado.

Em um esforço de avaliação da viabilidade das propostas apresentadas, no próximo capítulo será realizada a avaliação da eficiência do sistema SPDA-BR e será apresentada a implementação da prova de conceito do sistema AUTV.

4 Viabilidade Funcional do AUTV e Análise de Eficiência do SPDA-BR

Este capítulo tem por objetivo apresentar evidências de viabilidade das contribuições apresentadas no capítulo 3, através de uma abordagem experimental. Na contribuição de direitos autorais SPDA-BR foi realizada uma análise de eficiência baseada na avaliação teórica do uso de banda para diferentes hierarquias de chaves criptográficas. Na contribuição em autenticação de aplicativos AUTV foi realizada uma comprovação de viabilidade funcional analisando uma implementação de prova de conceito utilizando certificados de atributos. Estas questões são detalhadas de forma pormenorizada ao longo do capítulo.

4.1 Análise de eficiência do SPDA-BR

A análise de eficiência do SPDA-BR foi realizada considerando-se a análise de desempenho do *smartcard* para tratamento das EMMs e a diferença de ocupação de banda para um tempo determinado de atualização de chaves do sistema.

O uso da criptografia simétrica, tanto por meio do MULTI-2 como utilizando o AES, o tamanho dos pacotes mantém-se o mesmo, estando ele claro ou cifrado. Desta maneira, a diferença de ocupação de banda e tempo de atualização de chaves entre o SPDA-BR e o sistema ISDB-T, não está relacionado diretamente ao tipo de criptografia.

Em relação ao tamanho das mensagens ECM e EMM, o SPDA-BR aumenta o tamanho dos pacotes pelo aumento do tamanho das chaves criptográficas e pela possibilidade de inclusão de descritores nas mensagens ECM. A chave AES proposta, possui 128 bits *versus* os 64 bits da chave do MULTI-2. Já em relação ao tamanho dos descritores, segundo a ABNT NBR 15603-2 (2007), o de controle de cópias possui 64 bits, o de disponibilidade de conteúdo possui 24 bits. Considerando que o de rastreamento possuísse 56 bits (18 bits de cabeçalho, 24 bits de posicionamento, mais 3 bits de modo e mais 12 bits para a duração).

Desta maneira as mensagens ECM têm com um acréscimo, no pior caso, de 208 bits por mensagem ECM.

Com o objetivo de estimar o tamanho das mensagens ECM e EMM, pode-se utilizar o tamanho das mensagens definidas no ARIB. Segundo a ARIB STD-B25 (2006), as mensagens ECM têm 42 bytes e as EMM têm 12 bytes de cabeçalho e a possibilidade de transmissão de vários *payloads* com 17 bytes cada, a estes 17 bytes deve-se ainda adicionar os bytes da chave, da identificação da chave e a identificação da sua localização na hierarquia. Com os bytes adicionais totalizaria 39 bytes (16 bytes + 3 bytes + 3 bytes). O número de *payloads* de EMMs pode ser colocado até ocupar uma seção inteira (184 bytes). Desta maneira, para o SPDA-BR pode ser considerado o pior caso, com ECMs de 68 bytes (208 bits + 42 bytes) e o envio de quatro $((184-12) / 39)$ EMMs em 184 bytes, ocupando cerca de 46 bytes cada uma.

Pode-se estimar o parque instalado de receptores de televisão digital para o sistema já em regime, como sendo de cerca de 60 milhões de dispositivos. Atualmente o parque de televisores no Brasil, segundo o IBGE, é de aproximadamente 54 milhões de aparelhos, considerando que este parque seja todo digitalizado e que sejam incorporados alguns usos adicionais ao televisor digital, como por exemplo, a integração a computadores pessoais, automóveis, entre outros; levando a um aumento estimado de 10% no parque atual. Com este aumento o parque total com o sistema em regime seria de 60 milhões de unidades.

Outro parâmetro importante a ser definido é o tempo que um usuário poderia esperar o recebimento de uma chave. Segundo BBC (2002), o tempo máximo que usuários de televisão digital esperam antes de se desinteressar é de 8s. Por isso, será utilizado este valor como tempo máximo de espera para o recebimento de chaves.

Para determinar o quanto a quantidade de dados disponíveis para mensagens estaria refletindo em custo de banda de transmissão para as emissoras, a taxa de bits que pode ser transmitida pelas emissoras depende das configurações adotadas para o modulador das emissoras. Em medida realizada em dezembro de 2008 em São Paulo (Tabela 11) utilizando uma plataforma de desenvolvimento de um *front-end* ISDB-T_B (FUJITSU MB86A20S), foi identificada a modulação 64QAM, com código convolucional de $\frac{3}{4}$ e intervalo de guarda de 1/16 como a configuração empregada na prática no Brasil. Segundo ARIB STD-B31 (2003), a taxa de bits que pode ser transmitida pelo canal de radiodifusão pode chegar até 23Mbps, ainda segundo esta especificação, na configuração de 64QAM, intervalo de guarda de 1/16 e código convolucional de $\frac{3}{4}$, a taxa disponível seria de 19,33Mbps. Neste trabalho será

considerada a taxa aproximada de 20Mbps.

Tabela 11. Medida de taxa disponível para as emissoras de TV no SBTVD.

<i>Canal</i>	<i>Frequência (MHz)</i>	<i>Intervalo de Guarda</i>	<i>Modulação</i>	<i>Código Convolutional</i>
15	479,143	1/16	64QAM	3/4
18	497,143	1/16	64QAM	3/4
20	509,143	1/16	64QAM	3/4
22	521,143	1/16	16QAM	3/4
23	527,143	1/16	16QAM	3/4
24	533,143	1/16	64QAM	3/4
28	557,143	1/16	64QAM	3/4
29	563,143	1/16	64QAM	3/4
31	575,143	1/8	64QAM	3/4
63	767,143	1/16	64QAM	5/6

Outro fator que deve ser definido é o número de níveis hierárquicos considerado. O número de níveis hierárquicos impacta tanto na flexibilidade do sistema e no número de mensagens necessárias para o gerenciamento do sistema do lado do transmissor, como na quantidade de memória necessária aos receptores para gerenciamento das mensagens no receptor. Para efeito de comparação, foram considerados neste trabalho cinco níveis hierárquicos de chaves.

Considerando a entrada de um novo dispositivo no sistema, o número de mensagens necessárias para incluí-lo depende exclusivamente do número de níveis hierárquicos considerado, é necessária uma mensagem para cada nível. Como neste caso são considerados cinco níveis, a entrada de um dispositivo requereria o envio de cinco mensagens. Já para o caso de não utilizar a hierarquia de chaves, seria necessária apenas uma nova mensagem. Como o tamanho da mensagem é pequeno, a situação de entrada de um novo dispositivo pode ser considerada desprezível no sistema para as duas situações ($46B * 5 \text{ mensagens} * 8\text{bits}/1B * 1/8s * 100\% / (20\text{Mb/s}) = \sim 0\%$ de consumo da banda de transmissão).

4.1.1 Estratégias de distribuição de chaves

As estratégias de distribuição de chaves consideradas neste trabalho são: divisão por fabricantes, divisão geográfica e divisão por ordem de requisição de chaves mestras. As estratégias de distribuição de chaves envolvem questões não apenas técnicas, mas também operacionais, conforme será apresentado a seguir.

4.1.1.1 A Estratégia de Distribuição de Chaves por Fabricante

A estratégia de distribuição de chaves por Fabricante é adequada para a proteção de direitos autorais para a televisão digital aberta, pois as chaves mestras são concedidas a receptores e a única condição para esta concessão é a declaração de conformidade dos receptores aos sistemas de proteção de direitos autorais. Desta maneira, organizando os receptores por fabricantes, modelos, lotes e subgrupos, em caso de irregularidade ou vazamento de chaves de um dado conjunto de receptores, a atualização de chaves deste ramo da hierarquia de chaves em árvore ficaria mais simples.

Foram considerados cinco níveis hierárquicos, organizados conforme a Figura 36. O primeiro nível é formado por um conjunto de até sessenta mil grupos, contendo cada um até mil receptores. O segundo nível é formado por até 600 grupos, cada um destes 600 grupos é formado pelo agrupamento de até 100 grupos do primeiro nível (contendo conseqüentemente até 100 mil receptores cada).

O terceiro nível é agrupado a partir dos modelos de receptores de um dado fabricante. Como o número de unidades de cada modelo não é uniforme, os grupos do segundo nível poderiam ser agrupados em uma variação desde um modelo possuindo os 600 grupos existentes no nível dois até 600 modelos, cada um possuindo apenas um grupo do nível dois.

O quarto nível é agrupado a partir dos fabricantes de receptores. Como o número de fabricante e de modelos produzidos por cada fabricante não é uniforme, os grupos do segundo

nível poderiam ser agrupados em uma variação de um único fabricante presente no mercado nacional possuindo os 600 modelos existentes (no máximo) ou este fabricante possuindo apenas um único modelo. O outro extremo seriam 600 fabricantes, cada um com um único modelo cada.

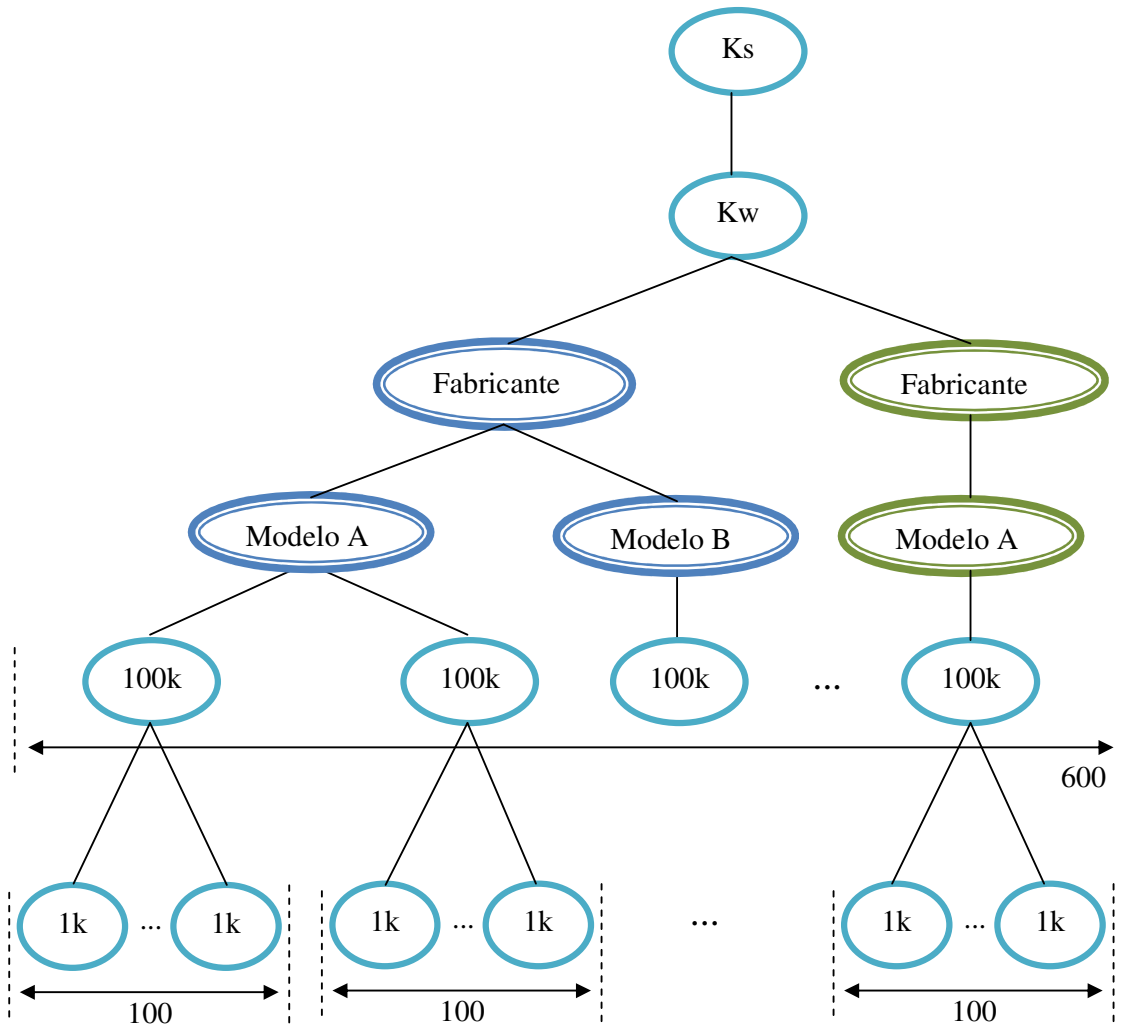


Figura 36. Organização de hierarquia lógica de chaves segundo modelo e fabricante.

A quantidade de mensagens necessárias para realizar a revogação de uma unidade receptora de TV no cenário apresentado na Figura 37 seria de cerca de 1.700 mensagens $((1000-1) + 100 + 600 + 1 + 1)$. Considerando que cada EMM ocupa 46 bytes; no pior caso, seriam distribuídos 78.246 bytes em 8 segundos, para a revogação de uma unidade receptora específica no sistema. O que resultaria em uma taxa transmissão para atualização de cerca de 1,2 kbps $(78.246 / 8 / 8 / 1000 = 1,222)$, para o pior caso.

Já no cenário apresentado na Figura 38, seriam necessárias 1.102 mensagens ($1.102=(1.000-1)+100+1+1+1$). Considerando novamente que cada EMM ocupa 46 bytes, no melhor caso, teriam que ser distribuídos 50.692 bytes em 8 segundos, para a revogação de uma unidade receptora específica no sistema. O que resultaria em uma taxa transmissão para atualização de cerca de 0,8 kbps ($50.692 / 8 / 8 / 1000 = 0,792$), para o melhor caso.

Como a taxa de transmissão disponível para as emissoras é de cerca de 20Mbps, em ambos os casos, a ocupação é desprezível, de aproximadamente 0% da banda disponível.

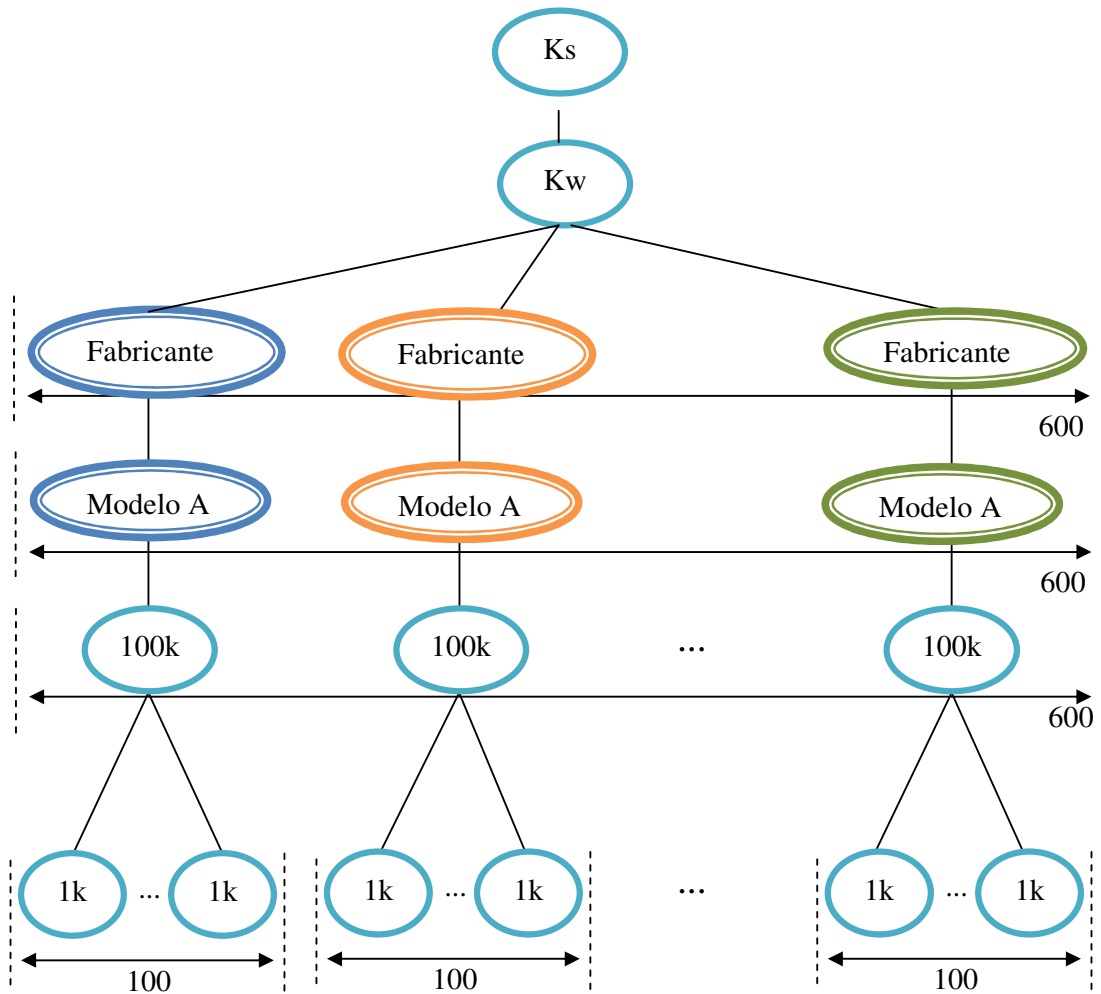


Figura 37. Organização de hierarquia de chaves segundo modelo e fabricante – pior caso.

Além disso, no caso de revogar um determinado modelo ou fabricante, esta disposição é especialmente favorável. Caso seja provado que um fabricante que estivesse produzindo equipamentos de determinado modelo em desacordo com as regras de proteção de direitos

autorais, para o pior caso teriam que ser enviadas 600 mensagens, por outro lado, no melhor caso seria necessário o envio de apenas duas mensagens.

Já para a atualização da chave de trabalho, esta estratégia de hierarquia demanda entre 600 a 1 mensagens.

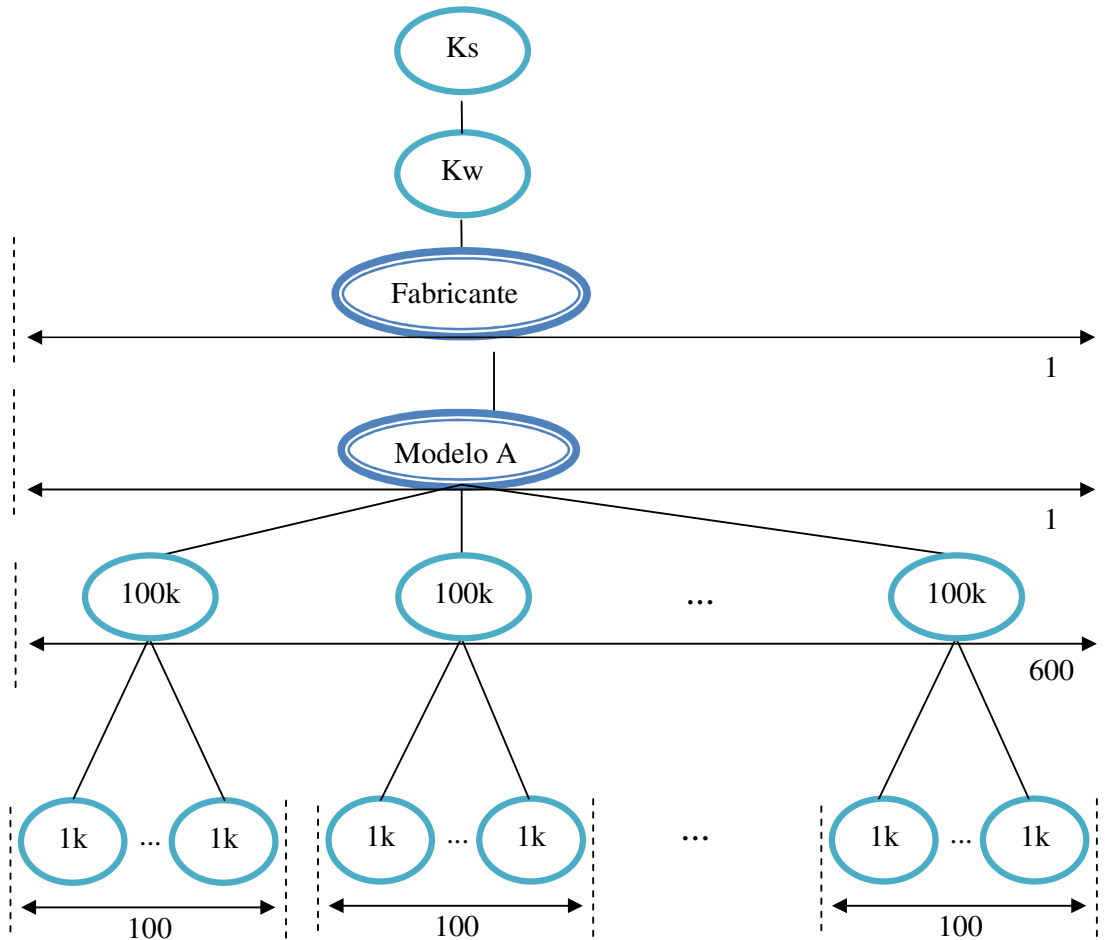


Figura 38 Organização de hierarquia de chaves segundo modelo e fabricante – melhor caso

4.1.1.2 A Estratégia de Distribuição de Chaves por Localização Geográfica

A estratégia de distribuição de chaves pelo agrupamento de receptores de acordo com a localização geográfica pode ser utilizada para diminuir o número de mensagens a serem enviadas no processo de atualização de chaves. O inconveniente deste modelo é a necessidade

de cadastrar o aparelho para a sua área de operação junto ao órgão de gerenciamento, devendo este estar sempre atualizado. Como em áreas com alta densidade demográficas um único transmissor de TV cobre uma grande quantidade de receptores, é necessária uma divisão em áreas menores do que a de cobertura dos transmissores. Em São Paulo, por exemplo, a cidade é coberta em sua maior parte por uma única transmissora, cobrindo milhões de aparelhos receptores.

No caso desta distribuição, o nível mais baixo da hierarquia de chaves é igual ao número de receptores de uma dada localidade. A Figura 39 apresenta a árvore para o pior caso, o da cidade mais populosa do Brasil, São Paulo. Segundo o PNAD 2007, existem na região metropolitana de São Paulo, cerca de 5.812.784 domicílios. Como a média de televisores por domicílio no Brasil é de 1,41, podemos considerar que São Paulo possui um total de 8.196.025 televisores, será considerado o valor aproximado de nove milhões de receptores de TVD.

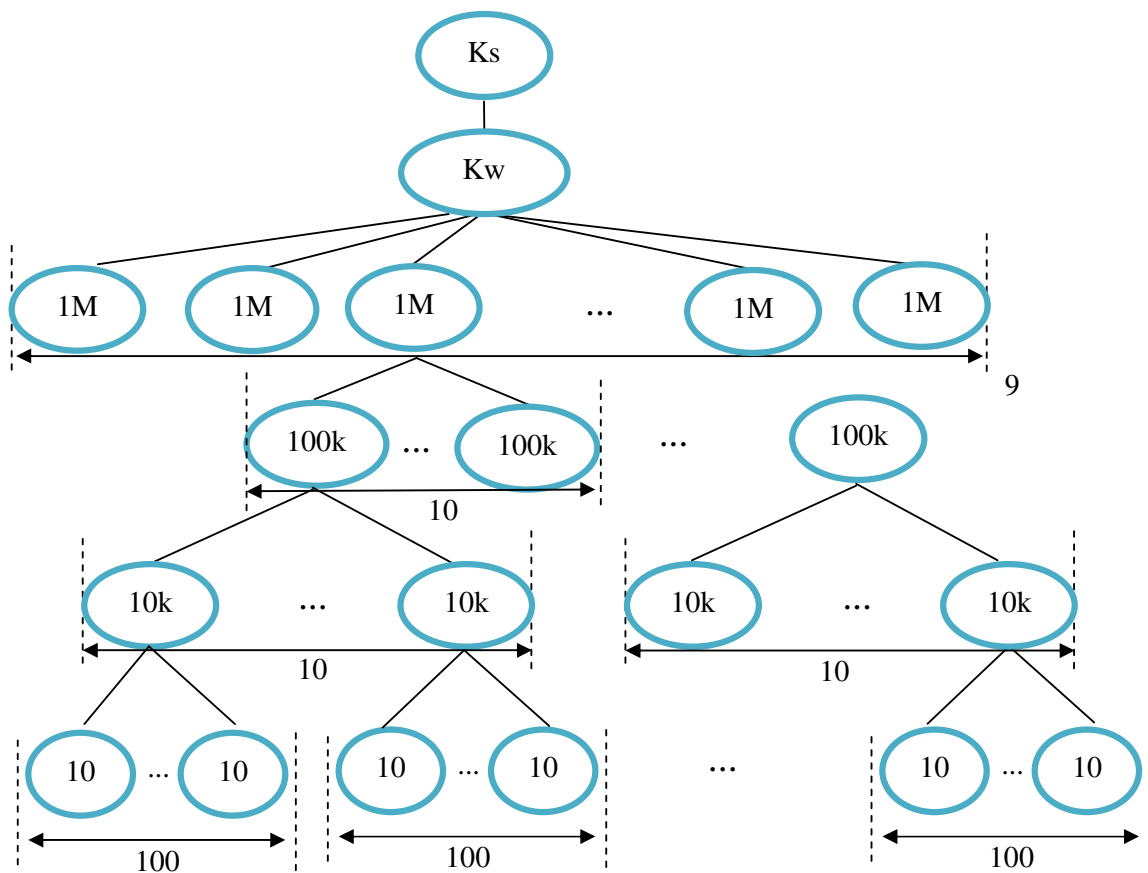


Figura 39. Organização de hierarquia lógica de chaves segundo localidade.

Foram considerados, também para este caso, cinco níveis hierárquicos. O primeiro nível é formado por grupos de cem receptores. O segundo nível agrupa 100 grupos do primeiro nível, resultando em até dez mil receptores. O terceiro nível agrupa 10 grupos do nível inferior, resultando em um total de até cem mil receptores. O quarto nível um agrupa dez grupos do nível inferior, resultando em um agrupamento de até um milhão de unidades. Já o quinto nível agrupa até nove grupos do nível inferior, contendo a totalidade do parque de receptores, 9 milhões.

A quantidade de mensagens necessárias para realizar a revogação de uma unidade receptora de TV no cenário apresentado na Figura 39 seria de cerca de 228 mensagens ($(100-1) + (100) + (10) + 10 + 9 = 228$). Considerando que cada EMM ocupa 46 bytes, no pior caso, teriam que ser distribuídos 10.488 bytes em 8 segundos, para a revogação de uma unidade receptora específica no sistema. O que resultaria em uma taxa transmissão para atualização de cerca de 0,16kbps ($10.488 / 8 / 8 / 1024 = 0,1639$), o que equivale a aproximadamente 0% da banda disponível para as emissoras.

Já para a atualização da chave de trabalho nesta distribuição, seria necessário o envio de até nove mensagens, uma para cada grupo superior da hierarquia. Como visto, este valor é desprezível frente à banda disponível pela emissora.

4.1.1.3 A Estratégia de Distribuição de Chaves por Ordem de Requisição

Esta estratégia de agrupamento de receptores é utilizada pensando-se apenas na formação da hierarquia de chaves de maneira eficiente.

Foram considerados, também para este caso, cinco níveis hierárquicos, organizados conforme a Figura 40. O primeiro nível é formado por grupos de cem receptores. O segundo nível agrupa 100 grupos do primeiro nível, resultando em até dez mil receptores. O terceiro nível agrupa 100 grupos do nível inferior, resultando em um total de até um milhão de receptores. O quarto nível um agrupa dez grupos do nível inferior, resultando em um agrupamento de até dez milhões de unidades. Já o quinto nível agrupa até seis grupos do nível inferior, contendo a totalidade do parque de receptores considerada, 60 milhões.

A quantidade de mensagens necessárias para realizar a revogação de uma unidade receptora de TV no cenário apresentado na Figura 40 seria de cerca de 315 mensagens ($(100-1) + (100) + 100 + (10) + 6 = 315$). Considerando que cada EMM ocupa 46 bytes, no pior caso, teriam que ser distribuídos 14.490 bytes em 8 segundos, para a revogação de uma unidade receptora específica no sistema. O que resultaria em uma taxa transmissão para atualização de cerca de 0,2kbps ($14.490 / 8 / 8 / 1000 = 0,2264$), o que equivale a aproximadamente 0% da banda disponível para as emissoras.

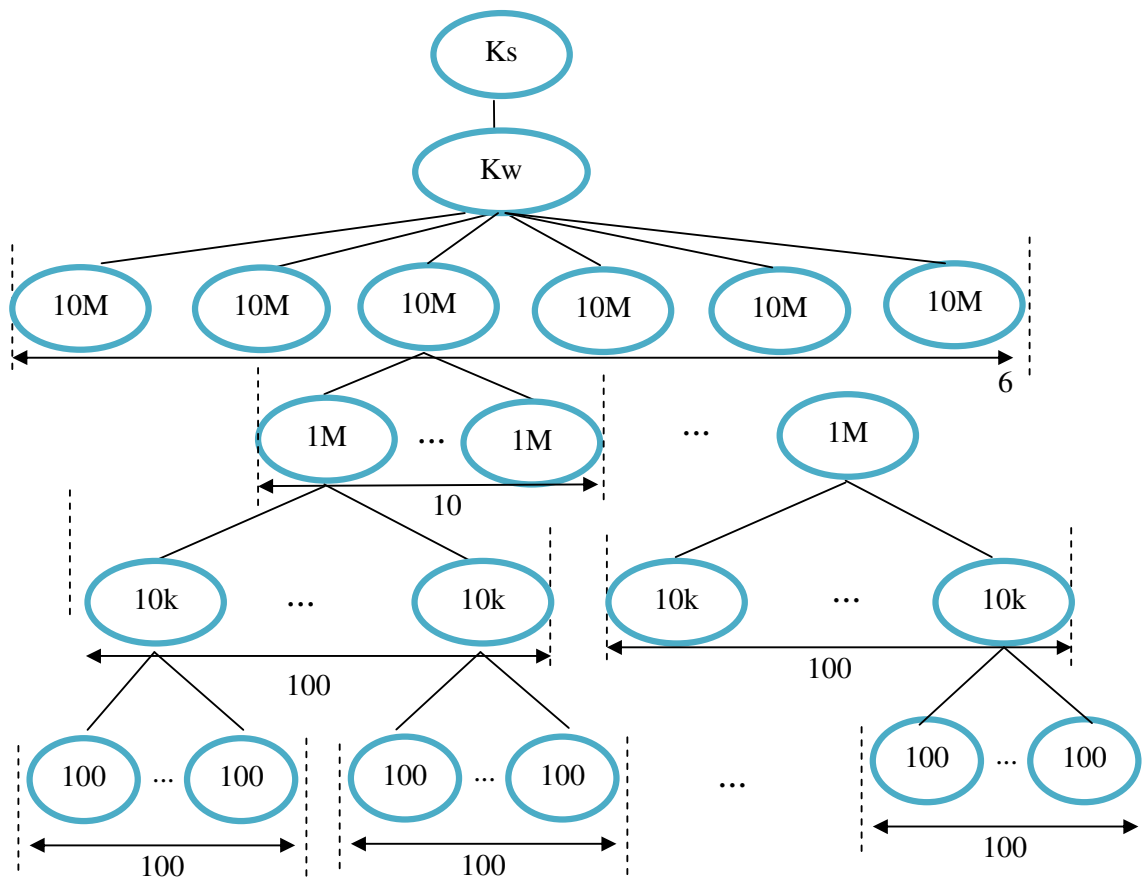


Figura 40. Organização de hierarquia lógica de chaves segundo ordem de requisição.

4.1.1.4 A Estratégia de Distribuição de Chaves sem Hierarquia Lógica de Chaves

A estratégia de distribuição de chaves sem hierarquia lógica de chaves é a estratégia adotada pelo ISDB-T, portanto a comparação desta estratégia com as anteriormente propostas

neste capítulo é pertinente. Para compararmos as estratégias propostas com a estrutura sem uso da hierarquia lógica de chaves, será apresentado neste item o consumo de banda para o caso sem hierarquia de chaves. O número de mensagens necessárias para a alteração da chave Kw é igual ao tamanho do parque de receptores considerado. Além disso, a revogação da licença de um receptor consiste na atualização da chave Kw do sistema, sendo necessário o envio de mensagens para todo o parque de receptores também neste caso. Já para a inclusão de uma nova unidade no sistema, basta que ela receba uma mensagem informando qual a chave de trabalho em uso. A Tabela 12 apresenta a necessidade de consumo de banda para cada uma destas operações.

Tabela 12. Custo de distribuição de mensagens EMM sem uso de hierarquia de chaves.

Operação	Custo em Mensagens	Número de bytes	Banda ocupada
Revogação	60.000.000	2.760.000.000	215%
Inclusão	1	46	0%
Atualização de Kw	60.000.000	2.760.000.000	215%

4.1.1.5 Sumário Comparativo das Estratégias de Distribuição de Chaves

A Tabela 13 apresenta um quadro comparativo de consumo de banda das emissoras considerando as diferentes estratégias propostas em relação à formação de grupos de chaves para o acesso condicional do SPDA-BR. Analisando a tabela, pode-se afirmar que do ponto de vista de economia de banda, a melhor solução seria a de transmissão de mensagens específicas para os receptores que estão em uma determinada região. Além disso, percebe-se que a não utilização de hierarquia de chaves torna o consumo de banda muito alto, inviabilizando a atualização de chaves Kw no sistema para a disponibilidade especificada (máximo de 8 segundos sem sinal de TV aberta devido ao sistema de proteção de direitos autorais).

Tabela 13. Consumo de banda para diferentes estratégias de gerenciamento de receptores.

Operações Estratégias	Revogação		Atualização periódica de Kw		Observações
Fabricante	1,22kbps – 0,79kbps	0%	0,43kpbs - 0,00kbps	0%	Facilidade de localização de dispositivos e revogação por modelos ou fabricantes.
Localização Geográfica	0,16kbps	0%	0,01kbps	0%	Necessidade de cadastro da localização do dispositivo pelo usuário.
Ordem de requisição	0,23kbps	0%	0,00kbps	0%	Facilidade de revogação de dispositivos por lotes de fabricação.
Sem uso da hierarquia lógica de chaves	43.125kbps	>100%	43.125kbps	>100%	Gerenciamento mais simples.

4.1.2 Análise de desempenho para o uso de cartões criptográficos

Quanto ao uso de cartões criptográficos para implementação do SPDA-BR, a análise realizada foi feita com base no trabalho de Yang (2001) e na análise das especificações de alguns componentes atuais para cartões criptográficos. No trabalho de Yang (2001), foram testados algoritmos criptográficos, entre eles o AES, em dois cartões criptográficos com processadores distintos, com suas características sumarizadas na

Tabela 14. Devem ser considerados dois pontos para a análise de viabilidade da aplicação do SPDA-BR a cartões criptográficos, a primeira seria a disponibilidade de memória interna para gerenciamento da hierarquia de chaves empregada e a segunda seria a capacidade de processamento do algoritmo de criptografia das mensagens ECM e EMM (AES CBC 128 bits).

Tabela 14. Características técnicas de processadores para cartões criptográficos. Fonte: Yang (2001)

	MC68HC705B16	H8/3113
Processador	8 bits, 2,1MHz	8 bits, 5MHz
ROM	15k	32k
EEPROM	256Bytes	16kBytes
RAM	352Bytes	2,5kBytes
Gerador de números aleatórios	Não	Sim
Coprocessador embarcado	Não	Sim, um multiplicador.

Em relação à suficiência de quantidade de memória disponível para o armazenamento das chaves da hierarquia, devemos analisar o tamanho da memória EEPROM que foi destinada a esta finalidade no desenvolvimento utilizado como base. Considerando os cinco níveis hierárquicos de chaves propostos nas estratégias descritas no item 4.1.1, deveríamos ter na EEPROM espaço para armazenamento de pelo menos cinco chaves e suas identificações. Cada chave possui 128 bits e a quantidade de chaves que precisam ser identificada está por volta de 60 milhões de unidades, o que requereria no mínimo 26 bits de endereçamento. Sendo assim, seriam necessários 100 bytes para o armazenamento das chaves da hierarquia do sistema, 20 bytes por chave. Em relação à memória, pudemos perceber que os dois processadores em análise suportam as contribuições propostas ao SPDA-BR.

Já em relação à capacidade de processamento do AES nos dois processadores testados, conforme apresentado na Tabela 15, para o pior caso a capacidade de processamento dos processadores analisados é de 30kbps. No item 4.1.1, considerou-se a entrega de mensagens EMM de 46 bytes em um intervalo de tempo de 8s, o que resultaria em uma taxa de bits de 46bps, o que se encontra dentro da capacidade de processamento obtida.

Com o objetivo de completar esta análise foram levantados alguns dos processadores para cartões criptográficos atualmente disponíveis no mercado, para que possa ser confirmado que as características de processadores analisadas anteriormente foram superadas ou

mantidas. Segundo STM (2008), a família ST19 da empresa *ST Microelectronics* apresenta uma linha nova de produtos para cartões criptográficos. A memória ROM varia de 128k a 210k e a EEPROM de 18kB a 66kB. Já a memória RAM vai de 4kB a 6kB. É suportada a criptografia AES CBC de 128 bits por toda a família, que possui processadores de 8 ou 16 bits, com 10MHz. Desta maneira, foi constatado que as famílias de componentes para smartcards atuais são capazes de realizar os processamentos demandados no sistema AUTV.

Tabela 15. Comparação de processamento do AES para modelos de cartões criptográficos. Fonte: Yang (2001)

Modelo	MC68HC705B16	H8/3113
Parâmetro		
Tempo de processamento por bloco	4,3ms	1,67ms
Número de ciclos de processador consumidos	9000	4180
Taxa de criptografia de dados	30kbps	78kbps

4.2 Viabilidade Funcional do AUTV

Nesta seção descreveremos a análise de viabilidade funcional do sistema de autenticação de aplicativos AUTV. Para tanto foi proposta a especificação e desenvolvimento de uma prova de conceito do AUTV baseada numa implementação em software utilizando a linguagem Java e um computador pessoal como ambiente de execução. A etapa de construção da prova de conceito do modelo proposto foi definida pela criação de dois aplicativos, um para realizar a geração dos pacotes de atualização e outro para fazer a verificação de autenticação. Para ambos os protótipos, as seguintes restrições da implementação podem ser observadas:

- O processo de recebimento de dados foi desconsiderado. O aplicativo de verificação

de autenticação considera o sistema de arquivos do aplicativo já montado em diretório especificado e o de geração do pacote de autenticação gera o pacote a ser transmitido em diretório.

- A aplicação foi representada por uma estrutura de diretórios e arquivos. Os aplicativos interativos são compostos de uma estrutura de diretórios e arquivos, mas na prova de conceito, esta estrutura continha apenas arquivos de texto.
- Todos os arquivos do diretório foram autenticados. No sistema AUTV seria possível incluir no arquivo *hash.file* um identificador para arquivos não autenticados, que seriam os considerados inofensivos, como de imagens, por exemplo.
- Os testes foram realizados em computador pessoal comum. A prova de conceito não foi exercitada em ambiente embarcado de eletrônica de consumo.

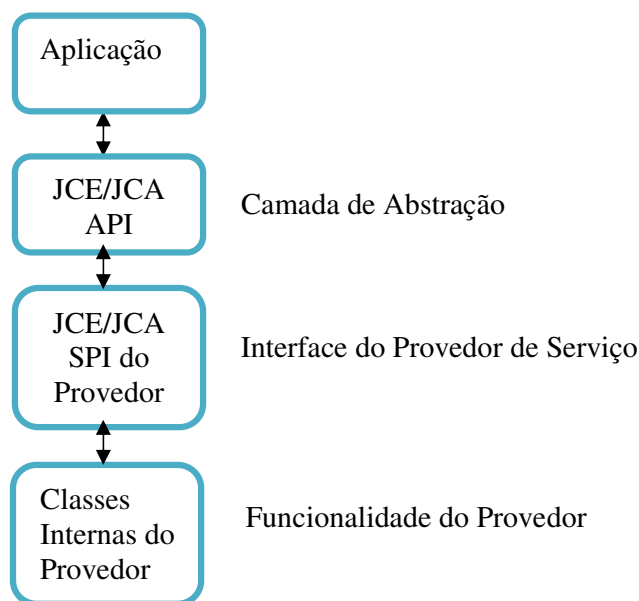


Figura 41. Funcionamento JCA/JCE.

Os protótipos foram construídos utilizando a linguagem de programação Java, com o auxílio das bibliotecas criptográficas BouncyCastle. Segundo Hooks (2005), o Java possui uma infraestrutura de segurança composta pela JCA (*Java Cryptography Architecture*) e JCE (*Java Cryptography Extension*). A arquitetura do JCA/JCE é baseada em provedores, o que significa que ao invés de prover as classes para uso das funcionalidades de segurança, são definidas as APIs, como classes abstratas, que são implementadas por provedores, como

ilustrado na Figura 41. As bibliotecas de provedores para funcionalidades de criptografia devem ser assinadas por uma ICP com um dos certificados raiz presentes na máquina virtual Java utilizada. A *BouncyCastle* é uma biblioteca de código aberto desenvolvida para uso em dispositivos embarcados que pode ser utilizada como provedor criptográfico, além disso, ela propõe algumas interfaces para tratamento de certificados de atributos.

No desenvolvimento, foram utilizados o JDK1.6 e o IDE NetBeans 6.0, que podem ser obtidos em SDN (2008) e *NetBeans Project* (2008), respectivamente. Para o tratamento dos atributos XML, utilizou-se a biblioteca *XStream*, que pode ser obtida em *Xstream Project* (2008).

4.2.1 O aplicativo Autenticador

O primeiro aplicativo prototipado foi o Autenticador, que é responsável por gerar os arquivos de autenticação do diretório do aplicativo. Ele possui uma interface gráfica, apresentada na Figura 43, permitindo a configuração dos diferentes casos de uso para a realização dos testes funcionais da prova de conceito. A Figura 42 apresenta as entradas e saídas do autenticador e a Figura 44 apresenta o diagrama IDEF0 (*Integration Definition for Function Modeling*) do autenticador. As diretrizes para a construção deste diagrama foram extraídas de Waltman e Presley (1993) e Bider (2002).

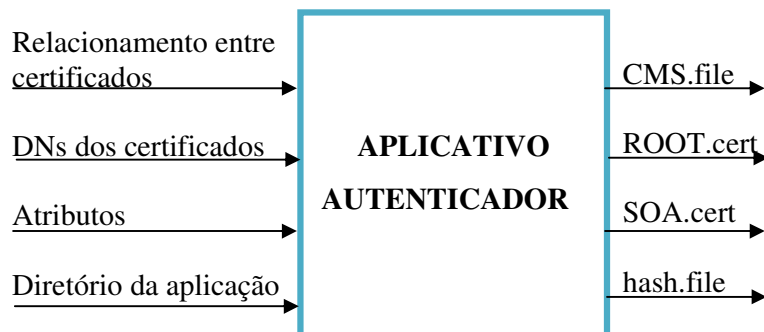


Figura 42. Entradas e saídas do aplicativo Autenticador.

O autenticador recebe pela interface com usuário as configurações necessárias para gerar os diferentes casos de uso da autenticação de aplicativos. Pela interface é determinada a cadeia de certificados de atributos e para cada um a cadeia de certificação de identidade. Para cada certificado de atributos podem ser configurados os seus privilégios. São informados os nomes (DN – *Distinguished Names*) de cada entidade para o certificado de identidade. Além disso, deve ser informada a localização do diretório da aplicação para a realização da autenticação.

The screenshot displays the configuration interface for an application authenticator, titled 'Eixo'. It is divided into several sections for configuring different entities and certificate chains.

- Entity 1: Signer**:
 - Alias: Fabricante de Dispositivo Externo
 - DN: C=BR, O=ICP-Brasil, OU=RFB, CN=End entity
 - Entity Privileges:
 - Alterar software residente
 - Instalação de driver
 - Rodar aplicativo Ginga
 - Delegação para Alterar sw residente
 - Delegação para instalação de driver
 - Delegação para rodar aplicativo Ginga
 - Id Certificate Chain:
 - Entity 1 Id Cert Issuer Alias: Int1
 - Root Cert Authority Alias: Root1
 - Object Privileges:
 - Acesso ao front-end
 - Persistência do aplicativo
 - Acesso ao canal de retorno
- Entity 2: Attributes Authority**:
 - Alias: [Empty]
 - DN: C=BR, O=LG-Itas, OU=RFB e-CNPJ A1, CN=Atributos Authority
 - Entity Privileges:
 - Alterar software residente
 - Instalação de driver
 - Rodar aplicativo Ginga
 - Delegação para Alterar sw residente
 - Delegação para instalação de driver
 - Delegação para rodar aplicativo Ginga
 - Id Certificate Chain:
 - Entity 2 Id Cert Issuer Alias: [Empty]
 - Root Cert Authority Alias: [Empty]
- Entity 3: Source of Authority**:
 - Alias: Fabricante do receptor
 - DN: C=BR, O=LSITEC-Itas, OU=RFB e-CNPJ A1, CN=SOA
 - Entity Privileges:
 - Alterar software residente
 - Instalação de driver
 - Rodar aplicativo Ginga
 - Delegação para Alterar sw residente
 - Delegação para instalação de driver
 - Delegação para rodar aplicativo Ginga
 - Id Certificate Chain:
 - Entity 3 Id Cert Issuer Alias: Int2
 - Root Cert Authority Alias: root2
- Id Certificate Chain Creation**:
 - Entity 1: Alias Int1, DN FB e-CNPJ A1, CN=Int1
 - Entity 2: Alias Int2, DN FB e-CNPJ A1, CN=Int2
 - Entity 3: Alias Root1, DN si|OU=RFB,CN=RFB1
 - Entity 4: Alias Root2, DN si|OU=RFB,CN=RFB2
- Application**:
 - Directory: C:\Documents and Settings\Laisa\Meus [Search]
- Certificates Storage**:
 - Directory: Ingo\Laisa\Meus documentos\Mestrado [Search]

Buttons for 'Authenticate' and 'Clean' are located at the bottom right of the interface.

Figura 43. Interface gráfica do Aplicativo Autenticador.

Com base nestas informações, o autenticador gera os arquivos necessários para garantir a autenticação e verificação do aplicativo. O diretório da aplicação recebe os arquivos *hash.file* e o *CMS.file*. O arquivo *CMS.file* contém a assinatura digital do arquivo *hash.file* superior, as cadeias de certificação de identidade e de atributos, as LCRs. Além disso, são gerados os certificados de identidade raiz de confiança e o certificado de atributos da fonte de autoridade (SOA) para utilização na verificação de autenticação do aplicativo.

A criação dos certificados de atributos pode receber configurações de dois tipos, para

entidade e para objeto. Os atributos para objeto são formatados em XML e os de entidade em OID (*Object Identifier*). Quando atributos em XML são configurados o Autenticador automaticamente gera um certificado com detentor sendo o aplicativo (diretório especificado pela interface gráfica). Caso os atributos de objeto não sejam utilizados, o Autenticador gera o certificado de atributos para a entidade final que assina o aplicativo.

O aplicativo Autenticador possui como restrição o limite de três níveis de certificação para a cadeia de certificados de atributos e, para cada um, um limite de três níveis para a certificação de identidade.

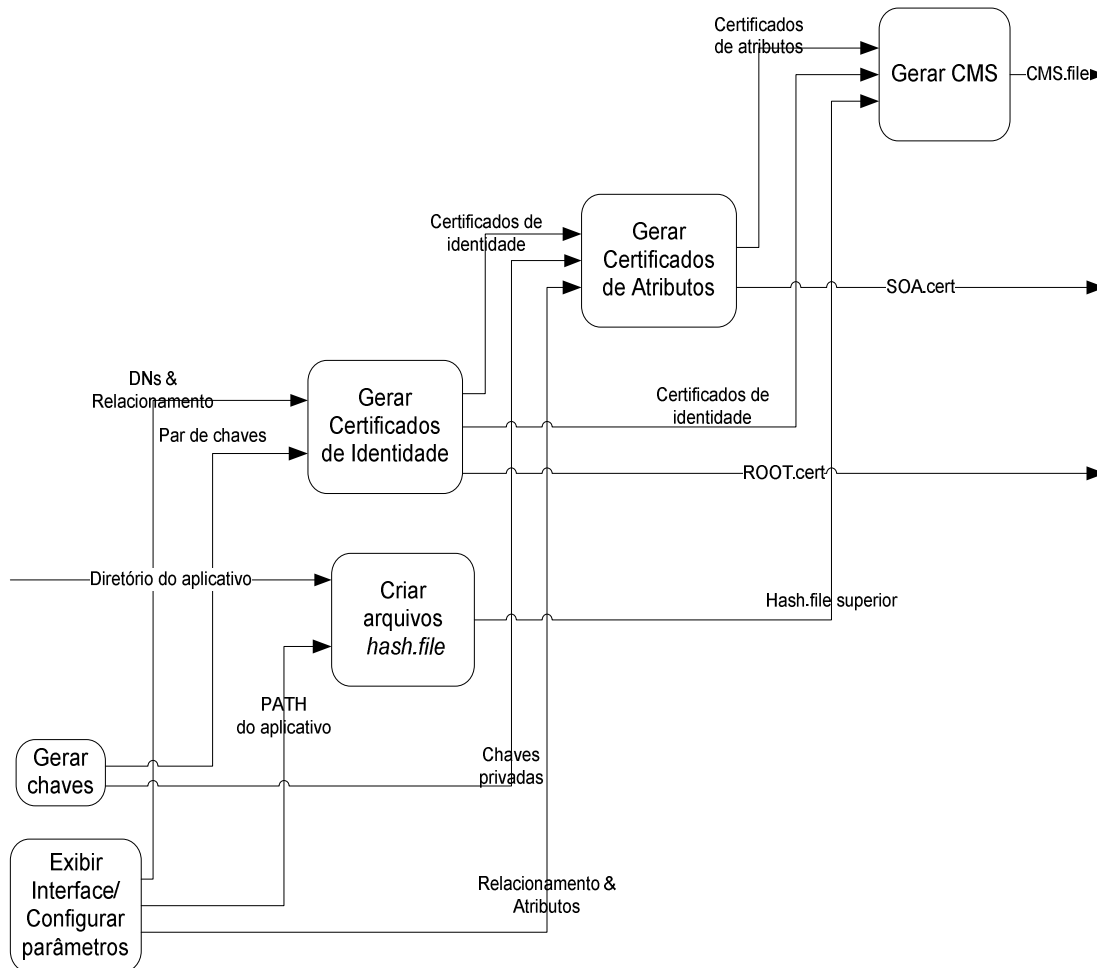


Figura 44. Blocos internos do aplicativo Autenticador.

4.2.2 O aplicativo Verificador de Autenticação

O segundo aplicativo prototipado é denominado de Verificador de Autenticação, é responsável por verificar a autenticidade de um aplicativo. Ele possui uma interface gráfica, apresentada na Figura 46, permitindo a configuração da localidade do aplicativo a ser verificado e os certificados de confiança a serem utilizados nesta verificação. A Figura 45 apresenta as entradas e saídas do autenticador e a Figura 47 apresenta o diagrama IDEF0 do Verificador de Autenticação.



Figura 45. Entradas e saídas do Verificador de Autenticação.

O Verificador de Autenticação recebe pela interface com o usuário as configurações necessárias para fazer a verificação da autenticação de aplicativos. Pela interface são determinados a localização do aplicativo, a localização dos certificados de confiança (*ROOT.cert* e *SOA.cert*) e os privilégios que se quer utilizar. No diretório do aplicativo devem estar presentes os arquivos *hash.file* e o CMS – contendo as cadeias de certificados de atributos e de identidade e a assinatura do arquivo *hash.file*.

Com base nestas informações, o Verificador informa se a autenticação foi realizada com sucesso e retorna os privilégios que podem ser utilizados pelo aplicativo. Inclusive retorna o arquivo XML com os privilégios de objeto, se houver.

A primeira etapa de processamento do aplicativo é a de verificação de integridade dos arquivos que fazem parte do aplicativo pela conferência dos valores de *hash* dos arquivos *hash.file*. Caso este passo não tenha sucesso, a verificação já é dada como falha. O próximo

passo é a verificação da assinatura do aplicativo. A assinatura do arquivo *hash.file* de nível superior deve ser recuperada do CMS e verificada a sua cadeia, fazendo uso da lista de certificados raiz de confiança com localização informada na configuração do Verificador de Autenticação e verificando-se a lista de certificados revogados também enviada no CMS.

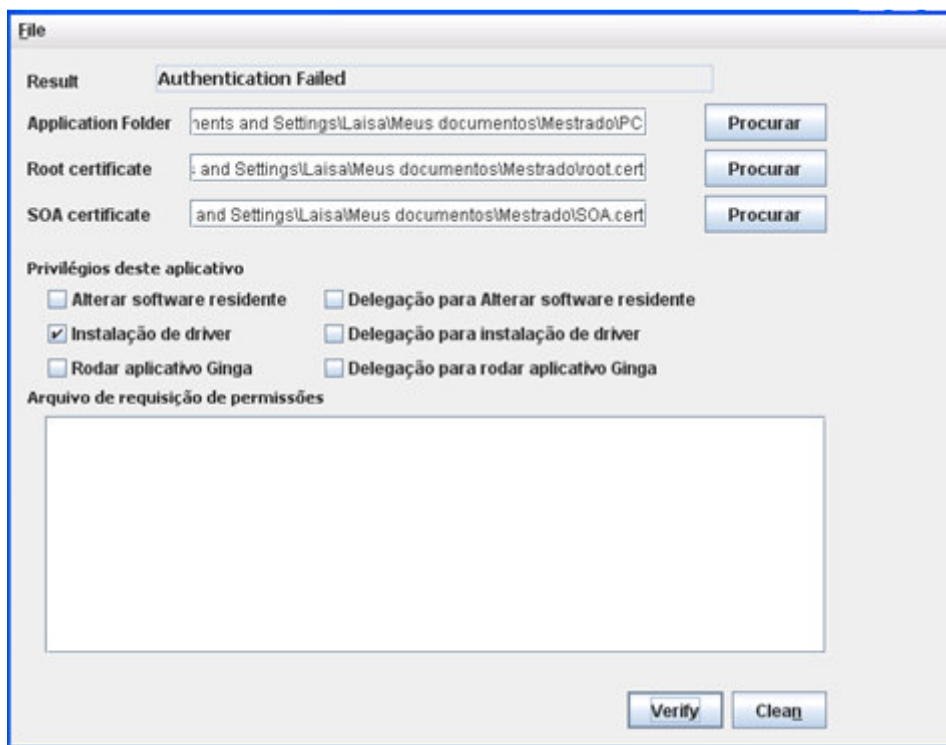


Figura 46. Interface gráfica do Verificador de Autenticação.

Caso a assinatura seja conferida com sucesso, serão verificados os privilégios da entidade final. A verificação de privilégios da entidade final exige a verificação da validade do certificado de atributos do signatário do aplicativo. A verificação da validade do certificado inclui verificação de validade, assinatura, revogação e cadeia de delegação com uso do certificado SOA local.

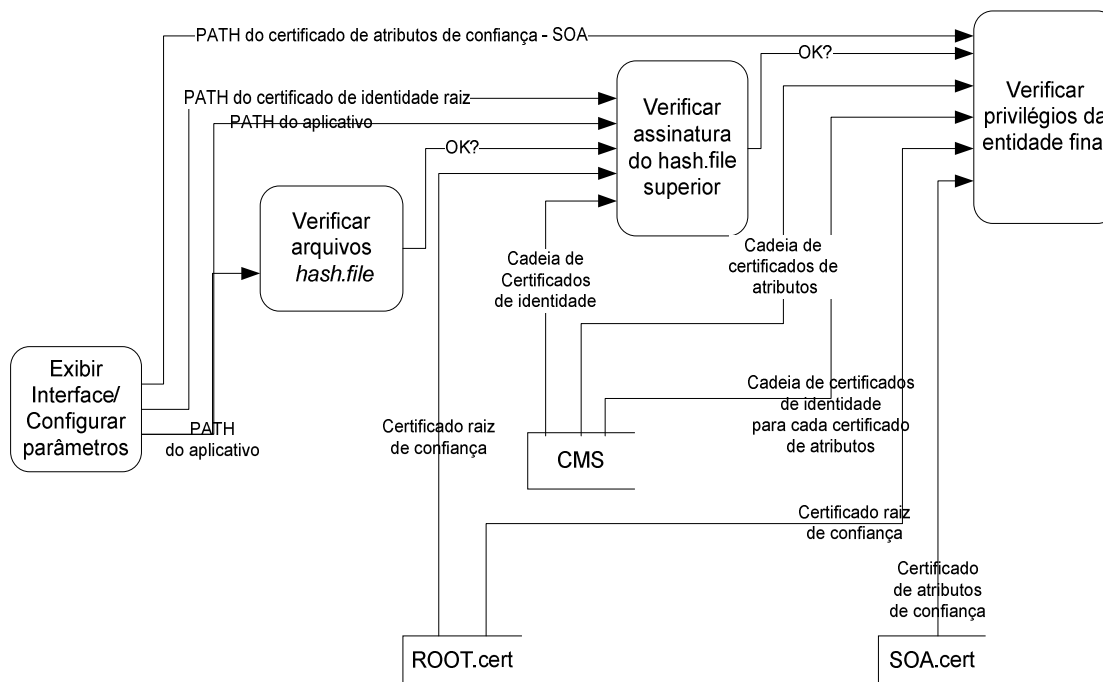


Figura 47. Diagrama IDEF0 do Verificador de Autenticação

4.2.2.1 Interface de Programação para o Verificador de Autenticação

O Verificador de Autenticação utilizou uma série de APIs Java no seu desenvolvimento. Estas APIs se dividem em três principais grupos: APIs de suporte, arquitetura Java de segurança e APIs *BouncyCastle*. Esta seção apresenta os pacotes utilizados na verificação de autenticidade feita pelo AUTV, simulando o cenário de autenticação de aplicações TV digital.

Das APIs de pacotes básicos do Java SE para suporte a programação, foram utilizados os pacotes de manipulação de entrada e saída (*java.io*), o pacote de utilitários (*java.util*) e de apoio matemático (*java.math*). Estes pacotes foram utilizados para realização de leitura e escrita de arquivos, manipulação de data, listas de objetos e para utilização de números grandes para número de séries de certificados.

Da arquitetura de segurança Java, foram utilizadas classes do pacote principal (*java.security*) e os pacotes de manipulação de certificados (*java.security.cert*). Do pacote

principal foram utilizadas as classes de geração e manipulação de códigos *hash*, chaves criptográficas e geração de valores aleatórios.

Da *BouncyCastle* foram utilizados pacotes relacionados ao padrão X.509, à estrutura CMS e às extensões criptográficas do Java (JCE). Para o padrão X.509, a *BouncyCastle* possui dois pacotes principais, um contendo as estruturas ASN.1 (*org.bouncycastle.asn1.x509*) e outro funcional (*org.bouncycastle.x509*), que cobrem as funções de manipulação tanto de certificados de atributos como de identidade. Do pacote que processa CMS (*org.bouncycastle.cms*) foram utilizadas as classes voltadas aos CMS do tipo de dados assinados ou de propósito geral (não foram utilizadas as classes de CMS do tipo envelope de dados). As extensões do JCE utilizadas foram as do pacote de apoio ao processamento de certificados (*org.bouncycastle.jce.cert*).

4.2.3 Exercitando casos de uso sobre o AUTV

A partir dos protótipos das aplicações Autenticador e Verificador de Autenticação, aplicamos sobre eles os casos de uso apresentados na seção 3.3.2. Os casos de uso utilizados foram: **conexão de um dispositivo e execução local de aplicativo interativo com uso de recursos críticos**.

As entidades e certificados utilizados foram:

- Autoridade de Certificação – AC
- Certificado de Identidade – CI_AC
- Autoridade de Registro 1 – AR1
- Certificado de Identidade – CI_AR1
- Autoridade de Registro 2 – AR2
- Certificado de Identidade – CI_AR2
- Fabricante de Receptor – SOA 1
- Certificado de Identidade – CI_R

- Certificado de Atributos – CA_R
- Fabricante de Dispositivo Externo – HOLDER
- Certificado de Identidade – CI_D
- Certificado de Atributos – CA_D
- Fórum SBTVD – SOA 2
- Certificado de Identidade – CI_F
- Certificado de Atributos – CA_F
- Emissora A – AA
- Certificado de Identidade – CI_A
- Certificado de Atributos – CA_A
- Aplicativo Interativo – Objeto
- Certificado de Identidade – CI_O
- Certificado de Atributos – CA_O

Para o caso de teste de **conexão de um dispositivo**, as cadeias de certificação testadas foram as apresentadas na Figura 48. Neste caso os certificados de identidade do Fabricante de Receptores de TVD e do Fabricante de Dispositivos Externos possuem seus certificados de identidade da ICP Brasil, seguindo cadeias distintas CI_R e CI_D respectivamente. Como o Fabricante do Receptor de TVD pode ser inserido como uma fonte de autoridade nesta IGP, o seu certificado de identidade pode assinar o seu próprio certificado de atributos (CA_R). O Fabricante de Dispositivos Externos, homologado pelo Fabricante de Receptor de TVD, recebe um certificado de atributos emitido pelo Fabricante de Receptor de TVD, este certificado recebe assinatura pelo par de chaves do fabricante de receptores, da ICP (deve ser verificado pelo CI_R).

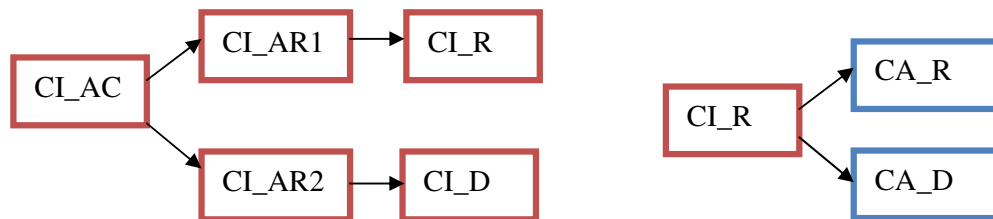


Figura 48. Cadeia de certificação para o caso de autenticação de driver.

Para o caso de teste de **execução local de aplicativo interativo com uso de recursos críticos**, as cadeias de certificação testadas estão apresentadas na Figura 49. Neste caso os certificados de identidade do fabricante de receptores e de dispositivo externo possuem seus certificados de identidade da ICP Brasil, seguindo a mesma cadeia de certificação. O fórum SBTVD é inserido como uma fonte de autoridade nesta IGP, por isso, o seu certificado de identidade pode assinar o seu próprio certificado de atributos. A emissora de TV recebe o privilégio de construção de aplicativo interativo com acesso a recursos restritos, possuindo um certificado de atributos com a assinatura do Fórum SBTVD. A emissora gera um software e atribui a ele (objeto) privilégios, através da geração de um certificado de atributos destinado a objeto e com a assinatura da emissora A (utiliza o par de chaves da ICP).

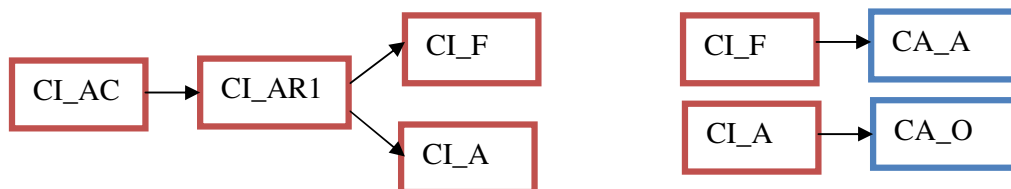


Figura 49. Cadeia de certificação para o caso de aplicativo interativo avançado.

4.3 Conclusão da análise de viabilidade dos sistemas AUTV e SPDA-BR

Este capítulo apresentou evidências de viabilidade do sistema de direitos autorais SPDA-BR e do sistema de autenticação de aplicativos AUTV.

O sistema SPDA-BR foi analisado em relação a sua eficiência, considerando a

ocupação de banda para operações de gerenciamento de grupos e a viabilidade da sua implementação em cartões criptográficos comerciais. Como o SPDA-BR inseriu o conceito de chaves de grupo na arquitetura de proteção de direitos autorais em relação ao sistema base ISDB, foi analisado o ganho de desempenho trazido. Além disso, foi verificado se o ganho proposto seria suficiente para garantir a disponibilidade do sinal de TV pelo envio periódico das chaves de acesso dos receptores. Os resultados obtidos mostraram que as estratégias utilizadas na avaliação teórica de ocupação de banda permitem que os receptores recebam a atualização das suas chaves de acesso em um período considerado aceitável e consumindo uma banda irrisória da banda total dos radiodifusores. Este capítulo mostrou também que é possível operacionalizar este sistema utilizando cartões criptográficos comercialmente disponíveis.

Já em relação ao sistema AUTV, foram desenvolvidos aplicativos para prova de conceito do sistema. Estes aplicativos foram exercitados nos casos de uso identificados nos capítulos anteriores. A partir da prova de conceito do AUTV foram obtidas evidências da sua viabilidade e completude. O trabalho de desenvolvimento das provas de conceito contribuiu com a realimentação da proposta apresentada nesta dissertação. Originalmente não havia sido considerado o uso de certificados revogados, nem a associação de emissor de certificados por nome, que posteriormente foram incorporados à proposta. Além disso, foram aprimoradas as determinações de privilégios a serem utilizados no sistema.

5 Conclusão

Este trabalho atingiu os objetivos esperados, apresentou uma sistematização das questões de segurança em televisão digital, identificando e propondo contribuições para o SBTVD. No Capítulo 2, Segurança e televisão digital, foram investigadas as questões de segurança em televisão digital, mostrando um panorama das tecnologias e padrões empregados na área de televisão digital e segurança. Durante o estudo do panorama de segurança em televisão digital, foram identificadas duas áreas de interesse, segurança em serviços e proteção de propriedade intelectual. Estas áreas de interesse podem ser mapeadas com as duas principais características do SBTVD, interatividade e alta qualidade de som e imagem.

O Capítulo 3 apresentou as contribuições no sistema de segurança para o SBTVD, partindo da proposição de casos de uso e requisitos para sistematização das questões de segurança para a televisão digital e apresentando contribuições para o SBTVD. Como contribuições, foram propostos os sistemas AUTV e SPDA-BR, que propõe um sistema de autenticação de aplicativos e um sistema de proteção de direitos autorais, respectivamente. O AUTV e o SPDA-BR foram testados e analisados em relação à sua viabilidade nos Capítulos 4 e 5. O AUTV foi implementado por meio de uma prova de conceito para testar a sua completude. O SPDA-BR foi testado por simulações teóricas em relação à sua eficiência em relação a consumo de banda e viabilidade de implementação em cartões criptográficos.

Este capítulo apresentará nas seções seguintes uma análise das contribuições desta dissertação, apresentando os seus impactos já identificados. Posteriormente serão apresentados alguns dos possíveis trabalhos futuros que podem ser explorados. O trabalho é fechado com uma seção de considerações finais.

5.1 Resultados, contribuições e impactos

O tema segurança em televisão digital requer uma visão ampla do sistema de televisão digital, envolvendo questões técnicas de transmissão, especialmente de demultiplexação, e amplo conhecimento da arquitetura de receptores de televisão digital. Para conseguir identificar as questões de segurança e propor alternativas que contribuíssem significativamente com o cenário brasileiro, foi necessária uma fase de fundamentação teórica e aprendizado.

Como resultado deste trabalho inicial de embasamento e abrangência, foi obtida a identificação dos casos de uso e requisitos de segurança em televisão digital, no item 3.1, Sistematização da segurança para a TV terrestre brasileira, e a publicação de dois artigos. Em Zuffo ET AL (2007) é discutida a arquitetura do dispositivo receptor de televisão digital para o Brasil, incluindo discussão em relação à sua infraestrutura de segurança para suporte à TV interativa. Em Hira ET AL (2007), é discutida a camada de abstração de sistema operacional, tratando também dos requisitos de segurança desta interface para acesso do *middleware* a recursos como cartão criptográfico e para a área de armazenamento segura de certificados digitais.

Os casos de uso do item 3.1, foram realizados de forma abrangente, mas não exaustiva. Foram identificados os casos mais relevantes, com o objetivo de identificar as áreas de contribuição deste trabalho e temas para trabalhos futuros. Esta meta foi cumprida com sucesso, pois as contribuições identificadas como potenciais para este trabalho possuem melhorias significativas para o cenário brasileiro frente aos seus sistemas base: o sistema AUTV e o SPDA-BR.

5.1.1 Resultados do sistema de proteção de direitos autorais: SPDA-BR

Nesta seção serão apresentados os resultados e análise do sistema SPDA-BR, apresentado como uma contribuição em relação ao sistema de proteção de direitos autorais

utilizado no ISDB. Desta contribuição podem ser ressaltados os seguintes pontos: adequação do algoritmo criptográfico, uso combinado do sistema embarcado com cartão criptográfico, uso de hierarquia lógica de chaves, protocolo de descrição de regras de uso, ferramentas de descrição de conteúdo, proteção contra cópias.

O sistema SPDA-BR foi discutido no âmbito de padronização do Sistema Brasileiro de Televisão Digital para sua adoção e aplicação. Ela não foi adotada em sua totalidade, mas serviu de subsídios para as decisões do sistema, como apresentado no artigo Costa e Zuffo (2008) e resultou em na publicação de Costa, Nascimento e Zuffo (2007).

5.1.1.1 Adequação de algoritmo criptográfico

Como melhoria em relação ao sistema de proteção de direitos autorais do ISDB, o SPDA-BR substituiu o algoritmo MULTI-2 pelo AES, com maior eficiência para a proteção do TS. Conforme apresentado no item 0, o algoritmo AES pode ser implementado em processadores embarcados em cartões criptográficos de maneira eficiente e viável.

5.1.1.2 Uso combinado de sistema embarcado e com cartão criptográfico

No ISDB é utilizado o cartão criptográfico para realização do processamento das mensagens ECM e EMM. No SPDA-BR este mecanismo é flexibilizado, pois permite que seja utilizado tanto um sistema embarcado como o cartão criptográfico. Desta maneira, o sistema de proteção de direitos autorais nativo de todo receptor de televisão digital viria embarcado, mas todos os receptores teriam disponível uma interface para leitura de cartões criptográficos. Caso o sistema fosse corrompido, o legado de receptores poderia receber um cartão criptográfico para atualização do sistema de DRM, enquanto os novos receptores já viriam com este novo sistema embarcado.

5.1.1.3 Uso de hierarquia lógica de chaves

Como demonstrado na simulação apresentada no item 4.1, a utilização da hierarquia lógica de chaves viabiliza o sistema de distribuição de chaves para o vasto conjunto de receptores do cenário de televisão digital aberta. Utilizando este sistema, as operações de gerenciamentos podem ser realizadas sem ocupar quantidades significativas da banda das emissoras e sem deixar o usuário sem sinal. Os cálculos realizados foram feitos considerando um tempo de espera dentro dos limites determinados por especialistas em interação entre humano e computador.

Em relação às estratégias de distribuições de chaves apresentadas, pudemos perceber que a estratégia de formação de grupos de receptores por Localização Geográfica é a que apresenta a menor ocupação de banda para as operações de gerenciamento de grupos. Apesar de possuir uma menor necessidade banda, esta estratégia requer que os receptores estejam cadastrados por região. Se os todos os receptores possuíssem canal de interatividade, seria possível que eles fizessem os seus próprios cadastramentos através de informações das tabelas SI, recebidas (identificação da torre de rádio-difusão, por exemplo). Como o canal de retorno não estará necessariamente disponível aos receptores de TVD, este cadastramento teria que ser feito pelos usuários finais, informando também a localização do seu receptor no caso de mudança de área.

Considerando o critério de facilidade de operacionalização do sistema, a estratégia de agrupamento por Ordem de Requisição apresenta o menor custo benefício, pois possui boa eficiência em termos de consumo de banda e não possui o inconveniente de cadastro de receptores. Sendo identificada como a estratégia mais promissora dentre as apresentadas.

A principal contribuição neste tópico foi a identificação de alternativas e a realização de uma estimativa de ocupação de banda para diferentes configurações, visando a prova da viabilidade da proposta. A seleção da hierarquia para o sistema de TV pode ser alterada com o tempo, pois o sistema proposto permite o gerenciamento dos grupos, viabilizando a troca da configuração dos grupos pelo envio de novas chaves.

5.1.1.4 Protocolo de descrição de regras de uso

O protocolo de descrição de regras de uso adotado no SPDA-BR é minimalista para viabilizar a sua integração com os mecanismos de proteção contra cópias. As regras de uso são utilizadas atualmente em sistemas como o HDCP e o DTCP, por exemplo. O uso de sistemas de descrição mais completos, como os propostos pelo MPEG-21, por exemplo, flexibilizaria o sistema permitindo a construção de novos casos de uso e modelos de negócio, mas carecem amadurecimento para aplicação a cenários tão complexos como o de televisão.

Além de permitir o envio das regras de uso nas tabelas SI como no sistema ISDB, o SPDA-BR permite o envio das regras de uso do conteúdo protegido, encapsulado nas mensagens ECM. Desta maneira, o núcleo de segurança recebe as mensagens ECM e EMM e retorna tanto as chaves Ks como os descritores com as regras de uso do conteúdo. Esta abordagem possui a vantagem de dificultar a alteração indevida das regras de uso no cabeçalho do TS como maneira de contorná-las.

A televisão possui como valor, não apenas o conteúdo que é transmitido, mas também a grade de programação. Visando evitar a re-transmissão indevida do conteúdo, o SPDA-BR permite que as emissoras enviem um comando para identificar receptores que estejam funcionando como retransmissores ilegais do conteúdo.

5.1.1.5 Ferramentas de descrição do conteúdo

No sistema de televisão digital terrestre, a descrição de conteúdo está intimamente relacionada aos multiplexadores. No Brasil, foi utilizada a restrição, para minimização de custos, de que as alterações em norma não impactassem os transmissores e multiplexadores. Por isso, a descrição do conteúdo segue de maneira geral a norma ARIB STD B10 (2002), conforme ABNT NBR 15606-3 (2007) que utiliza tabelas SI com informações do programa, contendo: gênero, classificação indicativa, sinopse, formato e codificação.

5.1.1.6 Proteção contra cópias

As contribuições deste trabalho para os mecanismos de proteção contra cópias são concentradas no levantamento de casos de uso e requisitos, mantendo como mecanismos propostos, os mesmos utilizados no sistema ISDB. Foi verificado que os mecanismos adotados no ISDB possibilitam a expansão do uso do conteúdo da TV digital terrestre e aberta no cenário das redes domésticas. Isto se dá através de mecanismos, como o HDCP, que protegem o conteúdo com criptografia e propagam as suas regras de uso para os dispositivos que recebem este conteúdo.

5.1.2 Resultados do sistema de autenticação de aplicativos AUTV

O sistema AUTV foi a contribuição dada neste trabalho para a área de segurança em serviços. Ele é um sistema de autenticação de aplicativos, do qual podem ser ressaltadas as seguintes características: delegação de privilégios, separação entre ICP e IGP, uso de estruturas padronizadas, atribuição de privilégios a objetos, complexidade de autenticação.

Além das contribuições sistêmicas, o AUTV tem um papel importante por identificar os pacotes e classes necessários para comporem a API de autenticação do sistema. Esta API é fundamental para colocar o sistema proposto em prática e faria parte da especificação dos pacotes de segurança de um *middleware* de TV digital em caso de adoção do sistema. O fato de utilizar a *BouncyCastle*, uma biblioteca aberta e livre e com foco em dispositivos embarcados, é um ponto muito favorável para a adaptação desta mesma API para uso final.

O sistema AUTV vem sendo discutido no âmbito de padronização do Sistema Brasileiro de Televisão Digital para sua adoção e aplicação. Caso ele seja adotado, estaria presente nas normas de segurança, volume relativo a aplicações e na norma de *middleware*, no volume relacionado à parte Java do Ginga. O AUTV foi divulgado em Zuffo e Costa (2008) até o presente momento.

Também no AUTV é importante considerar a questão de robustez e conformidade dos receptores para a operacionalização do sistema. A integridade de sistema operacional e o armazenamento seguro dos certificados de confiança são exemplos de requisitos de robustez necessários para garantir o correto funcionamento do sistema. Assim como no SPDA-BR, as regras de robustez e conformidade não foram exploradas nesta dissertação, por serem consideradas com viés de produtização.

A seguir são apresentadas discussões sobre cada um dos pontos identificados:

5.1.2.1 Delegação de privilégios

No MHP/GEM não há mecanismos de suporte à delegação de privilégios entre entidades finais. Isso significa que não há meios para que uma entidade final atribua privilégios a outras entidades finais sem a anuência de uma terceira parte. No modelo proposto, essa facilidade é alcançada, descentralizando a gerência do sistema de geração de certificados de atributos, minimizando os custos de gerenciamento e ampliando a flexibilidade do sistema.

5.1.2.2 IGP e ICP desvinculadas

O AUTV permite o uso de ICP e IGP desvinculadas, enquanto o MHP/GEM unifica as duas infraestruturas. Dada a existência de uma ICP nacional padronizada no Brasil, a ICP-Brasil, a adoção de ICP e IGP distintas favorece o aproveitamento desta infraestrutura já estabelecida. Além disso, os escopos das duas são distintos, já que a IGP refere-se aos privilégios das entidades envolvidas no âmbito de TV Digital, enquanto a ICP refere-se à identificação jurídica da entidade (garantindo a sua responsabilidade sobre o material assinado).

5.1.2.3 Uso de estruturas padronizadas

Para a transmissão de certificados, lista de certificados revogados e assinatura, o AUTV recorre ao uso de estruturas padronizadas e amplamente utilizadas em sistemas criptográficos. Por outro lado o MHP/GEM faz uso de arquivos proprietários. A vantagem da utilização das estruturas padronizadas é a pré-existência de APIs para gerenciamento destas estruturas e a minimização do número de arquivos a serem tratados.

5.1.2.4 Atribuição de privilégios a objetos

Como MHP/GEM utiliza ICP e IGP unificadas, os privilégios são associados à entidade. Permissões de objetos são realizadas pelo arquivo de requisição de permissões, enviado junto ao aplicativo. No AUTV estes privilégios são colocados em formato XML como mais um atributo do certificado de atributos; e o detentor deste certificado passa a ser o próprio objeto.

5.1.2.5 Complexidade de autenticação

Pelo uso de certificados de atributos em associação com o certificado de identidade, o AUTV exige um maior número de verificação de certificados. Este maior número de verificações dá-se devido à necessidade de verificar a validade da cadeia de certificados de atributos e para cada um, verificar a cadeia de certificados de identidade. Por outro lado, esta verificação é feita apenas no recebimento do aplicativo, e apenas para aplicativos que façam uso dos recursos de uso restrito do receptor.

5.1.2.6 Homologação de terceiros para serviços de engenharia

O AUTV foi expandido para casos que utilizam/alteram camadas de software inferiores ao *middleware*, o que não é coberto pelo escopo do GEM/MHP. Neste caso o sistema AUTV possui o inconveniente de requerer a localização do certificado de atributos adequado ao receptor-alvo. Diferentemente do caso de aplicativo sobre o *middleware*, os serviços de engenharia são destinados a grupos de receptores, e a extensão de identificação de grupo alvo deve ser utilizada.

5.1.3 Impactos no Sistema Brasileiro de TV Digital

Esta seção fará o mapeamento dos impactos da dissertação no SBTVD. A autora tem participado ativamente do grupo de trabalho de segurança no módulo técnico do Fórum SBTVD. As propostas aqui realizadas foram apresentadas ao grupo de trabalho do fórum e consideradas para uso no Brasil.

A norma de segurança do SBTVD é denominada ABNT NBR 15605, ela é influenciada pelos trabalhos aqui desenvolvidos desde a sua estruturação. A norma possui dois volumes, sendo que o primeiro volume trata das questões de proteção de direitos autorais e o segundo, da segurança em serviços.

O volume 1 da ABNT NBR 15605, já foi publicado ABNT NBR 15605-1 (2008) e apresenta um sistema de proteção de direitos autorais. Ele possui a especificação do protocolo de descrição de regras de uso, mecanismos de proteção contra cópias, regras de conformidade e robustez. O SBTVD não possui o mecanismo mais básico dos sistemas de proteção de direitos autorais, que é a proteção do conteúdo. A proposta técnica do grupo de trabalho de segurança do Fórum SBTVD foi consolidada considerando todas as contribuições aqui citadas. Devido a uma decisão política, foi abolido o esquema de proteção de conteúdo para garantir a impossibilidade de bilhetagem de conteúdo futura pelos radiodifusores.

O volume 2 da ABNT NBR 15605, está em fase de construção e trata da segurança em serviços. A estruturação do volume 2 sofreu influência dos requisitos e casos de uso mapeados neste trabalho. Ele possui a especificação de mecanismos de autenticação de usuários, segurança para uso de canal de interatividade, mecanismo de autenticação, perfis de segurança para o *middleware*, sistema de identificação do receptor e segurança para conexão de dispositivos externos, recebimento de aplicativos Ginga por diversos canais e atualização do *software* do receptor.

Todas as contribuições aqui apresentadas estão sendo aproveitadas no texto do segundo volume da norma de segurança do SBTVD, ela considera o uso de certificados de atributos associados a certificados de identidade ICP-Brasil, uso de estruturas CMS, unificação do sistema de autenticação de aplicativos para serviço de engenharia (atualização de software), aplicativos interativos avançados e conexão de dispositivos externos. A norma considera também outras contribuições que não foram abordadas neste texto, como o uso dos protocolos TLS e SSL para canal de retorno, parâmetros para identificação do receptor de maneira única, determinação de privilégios e formato do XML para privilégios de aplicativos Ginga, entre outros.

5.1.4 Contribuições da dissertação

Este item apresentou e analisou os principais resultados obtidos neste trabalho, inclusive seu impacto nas normas de segurança do SBTVD.

Como contribuições advindas destes resultados, podemos citar:

- Sistematização das questões de segurança para televisão digital brasileira. Este trabalho foi aproveitado para orientar a estruturação das normas de segurança do SBTVD e pode ser utilizado como referência para trabalhos futuros.
- Proposta do AUTV, um mecanismo de autenticação de aplicativos flexível (que possa ser utilizada para atualização de software, instalação de aplicativos, aplicativos interativos), compatível com padrões abertos e com a ICP Brasil.

- Proposta do SPDA-BR, um mecanismo de proteção de direitos autorais mais seguro, que permite a operação com cartão criptográfico ou sistema embarcado e que possui um sistema de gerenciamento de chaves criptográficas mais eficiente.
- Impacto na literatura. Foram publicados artigos em congressos científicos, nacional, internacional e *journal*. A saber:
 - COSTA, L. C. P., NASCIMENTO R., ZUFFO, M. K. A Digital Rights Management System Proposal for the Brazilian DTV. IEEE Broadcast Symposium. Setembro de 2007.
 - HIRA C.; COSTA, L. C. P. de; NUNES, R. P.; REAL, L. V.; ZUFFO, M. K. Sistema Operacional do Terminal de Acesso de Referência. SBRT 2007
 - ZUFFO M. K., CARVALHO E. R., BARROS G. G., COSTA L. C. P., FARIA R. R. A., NUNES R. P., LOPES R. D., The Brazilian Digital Television System Access Device Architecture, Journal of the Brazilian Computing Society, no. 1; V. 13; 2007.
- Impactos na sociedade: podem ser citadas as contribuições na escrita das normas de segurança do fórum SBTVD, participação em eventos e publicações não científicas. As normas de segurança que recebem contribuições desta dissertação são ABNT NBR 15605-1 (2008) e ABNT NBR 15605-2 (em construção). Podem ser citadas as participações: nos grupos técnicos do Fórum SBTVD; palestra Segurança em Serviços para TV Digital, no 6º Fórum de Certificação Digital em novembro de 2008; debate na Ordem dos Advogados do Brasil com a Comissão de Propriedade Imaterial, com o tema “Proposta de Segurança no Sistema Brasileiro de TV Digital” em novembro de 2007. Podem ser citadas as publicações não científicas: na Revista SET, o tutorial “Mecanismos de controle de cópias”, edição de novembro de 2008, Costa ET AL (2008); artigo Segurança em Serviços para a TV Digital no Brasil na Revista Digital, publicação do Instituto Nacional de Tecnologia da Informação (ITI), Zuffo e Costa (2009).

5.2 Trabalhos futuros

Com o objetivo de estender a aplicabilidade das contribuições propostas e aprimorar algumas as funcionalidades oferecidas, diversos temas para trabalhos futuros podem ser abordados. As seções seguintes apresentam alguns dos possíveis projetos futuros a partir do trabalho apresentado.

5.2.1 Modelo de gerenciamento da IGP para TV Digital

Um trabalho complementar em relação ao AUTV seria o de especificar o seu modelo de gerenciamento e operação, definindo as políticas de autorização, protocolos de acesso e requisição de certificados, além de processos de automatização.

5.2.2 Contribuição com as especificações do *middleware* do SBTVD

Como continuidade do AUTV estaria a definição das especificações das APIs a serem incorporadas nas especificações do *middleware* do SBTVD. Este trabalho inclui a revisão do uso da biblioteca *BouncyCastle* em relação à questão de direitos autorais e a melhoria da sua documentação e correção de limitações em relação ao uso de objeto como detentor do certificado de atributos.

5.2.3 Teste e aplicação do sistema AUTV em dispositivos embarcados

Uma das restrições de implementação do AUTV está relacionada ao ambiente de testes, realizados em computador pessoal e desconsiderando a entrega dos pacotes a serem autenticados. Como trabalho futuro, caberia a integração do AUTV aos ambientes de uso real, portando o sistema a dispositivos embarcado e com integração à distribuição do aplicativo por carrossel de dados, de objetos e porta USB.

5.2.4 Segurança para a integração de redes diversas

Como trabalho futuro poderia ser realizada a expansão das questões propostas neste trabalho para outras redes, considerando redes pessoais e com integração à Internet, cabo, entre outras.

5.2.5 Mecanismo de identificação de uso justo de conteúdo multimídia

Um dos maiores desafios em sistemas de proteção de direitos autorais é a identificação automatizada do uso justo do conteúdo, de maneira a não limitar o usufruto do conteúdo quando não há transgressão das regras de uso. O número de cópias de uma dada mídia não precisaria ser controlado se o usuário fosse o mesmo, por exemplo.

5.2.6 Mecanismo de alteração dos direitos do conteúdo

Como melhoria aos sistemas de direitos autorais atuais, poderia ser proposto um mecanismo que permitisse a atualização das regras de uso do conteúdo recebido pelos usuários e armazenado, por exemplo.

5.3 Considerações finais

O cenário de segurança para televisão digital é bastante amplo e não foi identificado na literatura um material que estruturasse as suas demandas de uma maneira efetiva. Neste sentido, esta dissertação sistematizou as questões de segurança e apresentou contribuições. Estas contribuições foram propostas, avaliadas e analisadas. Elas não cobrem todas as questões de segurança do cenário de televisão digital, possuem limites bem definidos e identificados. A definição de uma arquitetura de segurança para televisão digital dependeria de trabalhos futuros nos blocos complementares aos aqui definidos.

Esta arquitetura deve ser pensada não apenas para o cenário expandido, mas também para o convergente. As contribuições desta dissertação foram focadas no cenário expandido de TV digital, que considera tanto os requisitos de entretenimento e informação como o de interatividade e oferecimento de serviços pela plataforma de TV. A arquitetura de segurança deve evoluir para a consideração dos cenários convergentes, considerando os dispositivos em uma rede doméstica e com conexões múltiplas. Com a análise dos resultados deste trabalho pode-se afirmar que esta dissertação contribuiu para a obtenção desta arquitetura de segurança almejada, com foco nos cenários expandido e convergente.

Referências

AL HASIB, A.; HAQUE, A. A. M. M. **A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography**. Third International Conference on Convergence and Hybrid Information Technology, 2008 (ICCIT '08). Busan. ISBN: 978-0-7695-3407-7.

ARREBOLA, F. V. **Um modelo de controle de acesso a recursos de rede baseado em Infraestrutura de Chaves Públicas e Infraestrutura de Gerenciamento de Privilégios**. 2006. 86p. Dissertação (Mestrado). Escola Politécnica, Universidade de São Paulo, São Paulo, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 15603-2. **Televisão digital terrestre — Multiplexação e serviços de informação (SI) – Parte 2: Sintaxes e definições da informação básica de SI**. Rio de Janeiro, 2007.

_____. NBR 15604. **Televisão digital terrestre - Receptores**. Rio de Janeiro, 2007.

_____. NBR 15605-1. **Televisão digital terrestre – Segurança da Informação na Radiodifusão Digital - Parte 1: Controle de cópias**. Rio de Janeiro, 2008.

_____. NBR 15605-2. **Televisão digital terrestre – Segurança da Informação na Radiodifusão Digital - Parte 1: Mecanismos de segurança**. Rio de Janeiro, em construção.

ASSOCIATION OF RADIO INDUSTRIES AND BUSINESS (ARIB). STD-B21 Version 4.4 E0. **Receiver for Digital Broadcasting**. Japão, 1999.

_____. STD-B10 Version 3.8. **Service Information for Digital Broadcasting System**. Japão 2002.

_____. STD-B21 Version 4.6 E1. **Receiver for Digital Broadcasting**. Japão, 2007.

_____. STD-B25 Version 4.2 E0. **Conditional Access System Specifications for Digital Broadcasting**. Japão 2006

BARROS, G. G. **A consistência da interface com o usuário para a TV interativa**. São Paulo, 2006. p. 200 Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.

BBC – BRITISH BROADCASTING CORPORATION (Ed.) **Interactive Television Style Guide**. 2.1. Alemanha. 2002. 54 pg.

BIDER, I. **Tutorial on: Business Process Modeling as a Method of Requirements Engineering**. Espanha. ICEIS 2002.

BRASIL. **Decreto N° 4.901, de 26 de Novembro de 2003**. Institui o projeto do Sistema Brasileiro de Televisão Digital (SBTVD). Diário Oficial da União, Brasília, DF, 26 Nov 2003.

_____. **Decreto N° 5.820, de 29 de Junho de 2006**. Dispõe sobre a implantação do SBTVD-T, estabelece diretrizes para a transição do sistema de transmissão analógica para o sistema de transmissão digital do serviço de radiodifusão de sons e imagens e do serviço de retransmissão de televisão, e dá outras providências. Diário Oficial da União, Brasília, DF, 29 Jun 2006.

Boeyen, S.; Howes, T.; Richard, P. **RFC 2559 - Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2, 1999. Disponível em: <<http://www.faqs.org/rfcs/rfc2559.html>>**. Acessado em: 24 de março de 2008

BORMANS, J.; GELISSEN J.; PERKIS, A. **MPEG21: The 21st century multimedia framework**. IEEE SIGNAL PROCESSING MAGAZINE, Março de 2003

BRUNETT, I. S.; PEREIRA, F.; WALLE, V. R.; KOENEN, R. **The MPEG-21 Book**. John Wiley & Sons Ltd, 2006.

CHADWICK, D. W.; OTENKO, A.; BALL, E. **Role-Based Access Control With X.509 Attribute Certificates**. IEEE Computer Society. 2003. p.62 – p.69

COSTA, L. C. P.; NASCIMENTO R.; ZUFFO, M. K. **A Digital Rights Management System Proposal for the Brazilian DTV**. IEEE Broadcast Symposium .Setembro de 2007

COSTA, L. C. P. **Pesquisa e Desenvolvimento de uma Unidade Controladora de Vídeo Reconfigurável Baseada no Padrão MPEG-4**. 2003. Projeto de Pesquisa - Escola Politécnica, Universidade de São Paulo. São Paulo, 2003.

CHONG, C. N. “**LicenseScript: A novel digital rights language and its semantics,**” in *Proc.3rd Int. Conf. Web Delivery of Music, WEDELMUSIC-03*, Sept. 2003, pp.122–129.

COHEN, J. **A General Overview of Two New Technologies for Playing Protected Content on Portable or Networked Devices**, Microsoft Corporation, June 2004

COSTA, L. C. P.; ZUFFO, M. K.; NASCIMENTO, R.; SILVA, A. E. F. **Mecanismos de controle de cópias**. Revista SET. Novembro de 2008, p.22.

DALPOZ, M. A. S. **Um Terminal de Acesso Digital Reconfigurável Bidirecional Adaptável aos Padrões Multimídia Emergentes**. 2005. 195 p. Tese de Doutorado – Escola Politécnica, Universidade de São Paulo, São Paulo, 2005.

DIGITAL CINEMA INITIATIVES, LLC. **Digital Cinema System Specification**, Version 1.2. Março de 2008

DIGITAL CONTENT PROTECTION LLC, **High-Bandwidth Digital Content Protection System Specification**, version 1.3, 2006.

DIGITAL VIDEO BROADCASTING (DVB), **A Guideline for the Use of DVB Specifications and Standards**. Maio de 2000.

EUROPEAN STANDARD (EN) 50221. **Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications**. 1997.

European Telecommunications Standards Institute (ETSI). TS 102 543. **Digital Video Broadcasting (DVB); Globally Executable MHP (GEM) Specification 1.2**. Março de 2008

_____. ETSI TR 102 035. **Digital Video Broadcasting (DVB); Implementation Guidelines of the DVB Simulcrypt Standard**. 2002

FARRELL, S.; HOUSLEY, R. RFC3281 - An Internet Attribute Certificate Profile for Authorization, 2002. Disponível em: <<http://www.ietf.org/rfc/rfc3281.txt>>. Acesso em: 24 de março de 2008.

FERNANDO, G.; JACOBS, T; SWAMINATHAN, V. Project DReaM, An Architectural Overview. Setembro de 2005. Disponível em: <www.openmediacommons.org/collateral/DReaM-Overview.pdf >. Acessado em março de 2008.

FERRAILOLO, D. F.; KUHN, D. R. Role Based Access Control. In: NIST-NSA National Computer Security Conference, 15, 1992, Estados Unidos. **Proceedings...** Estados Unidos: NIST, 1992, p. 554-563.

FCC, **Report and order of Federal Communications Commission**, Washington, DC, Doc. 53-1663, Dec. 17, 1953.

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 180-1 (FIPS PUB 180-1). **Secure Hash Standard**. Abril de 1995.

_____.180-2 (FIPS PUB 180-2). **Secure Hash Standard**. Agosto de 2002.

_____. 186 (FIPS PUB 186). **Digital Signature Standard (DSS)**. 1994.

_____. 197 (FIPS PUB 197). **Advanced Encryption Standard (AES)**. 2001.

FRIER, A.; KARLTON, P.; KOCHER, P. **The SSL 3.0 Protocol**. Netscape Communications Corp, Nov 18, 1996.

FRAUSTO, P.; ANTOTNE, C. **Role Based Control Via Attribute Certificate**. 0-7803-8482-2. IEEE. 2004. p.81 – p.82

HIRA, C.; COSTA, L. C. P. de; NUNES, R. P.; REAL, L. V.; ZUFFO, M. K. **Sistema Operacional do Terminal de Acesso de Referência**. SBrT 2007

HIRA, C. **Arquimedia: Uma Proposta de Arquitetura de Software para Terminais de Acesso à TV Digital Interativa**. São Paulo, 2008. p. 133. Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.

HITASHI. **Digital Transmission Content Protection White Paper**, 1998

HOOK, D. **Beginning Cryptography with Java**. Estados Unidos: Wrox Press 2005. 480p.

HOUSLEY, R. **RFC 3852 – Cryptographic Message Syntax**, 2004. Disponível em: <<http://www.ietf.org/rfc/rfc3852.txt>>. Acesso em: 24 de março de 2008.

HOUSLEY, R.; POLK, W.; FORD, W.; SOLO, D. **RFC 2459- Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**, 1999. Disponível em: <<http://www.ietf.org/rfc/rfc3280.txt>>. Acesso em: 10 de agosto de 2008.

HOUSLEY, R.; POLK, W.; FORD, W.; SOLO, D. **RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**, 2002. Disponível em: <<http://www.ietf.org/rfc/rfc3280.txt>>. Acesso em: 24 de março de 2008.

HUANG J., MISHRA S. **Mykil: A Highly Scalable Key Distribution Protocol for Large Group Multicast**, IEEE GLOBECOM 2003

IANNELLA, R. **Open Digital Rights Language (ODRL)**, Version 1.0. IPR System Ptd Ltd. Nov. 2001. Disponível em: <<http://odrl.net/1.0/ODRL-10-HTML/ODRL-10.html>>

INTEL, **Wireless USB: The First High-speed Personal Wireless Interconnect**, 2005.

Disponível em: <www.intel.com/technology/comms/wusb/>, Acesso em: Setembro de 2007.

INTEL, **Intel and DTCP, Protecting premium content and its use in digital home**.

Disponível em http://www.intel.com/standards/case/case_dtcp.htm, acessado em dezembro de 2006.

ISO/IEC **13818-6**. Information technology — Generic coding of moving pictures and associated audio information — Part 6: Extensions for DSM-CC, 1998.

ISO/IEC 13818-1. **Information technology — Generic coding of moving pictures and associated audio information: Part 1: Systems**, 2000.

ISO/IEC 8824. **Information technology - Abstract Syntax Notation One (ASN.1)**, 2002.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Anexo: Padrões e Algoritmos Criptográficos Da ICPBrasil (DOC ICP 01.01), da Instrução Normativa N° 4**. 18 de maio de 2006.

ITU-R Rec. **BT.810**: Conditional-access broadcasting systems, 1992

INTERNATIONAL TELECOMMUNICATIONS UNIT – ITU-T Recommendation X.500, Information Technology – Open Systems Interconnection – The Directory: **Overview of concepts, models and services**, 2001.

____. ITU-T Recommendation **X.509**, Information Technology – Open Systems Interconnection – The Directory: **Public-key and attribute certificate frameworks**, 2005.

____.ITU-T Recommendation X.812, Information technology - Open Systems Interconnection - Security Frameworks for open systems: **Access control framework**, 1995.

JONKER, W.; LINNARTZ, J. P. **Digital Rights Management in Consumer Electronics Products**. IEEE SIGNAL PROCESSING MAGAZINE pg 82 a 91. Março de 2004

Lakshminarayanan, A.; Zhou J. **FlexiCert: Merging X.509 Identity Certificates and Attribute Certificates**. In: Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03), 2003 IEEE 1529-4188/03 IEEE Computer Society

LI, B.; ZHAO Y. **A Scalable key distribution scheme for secure multicast**, IEEE Proceedings of the Third International Conference on Machine Learning and Cybernetics 2004

LSI-TEC. **Terminal de Acesso de Referência: Sumário Executivo**, Consórcio TAR-SBTVD, Convênio 2038/04 em atendimento a carta convite MC/MCT/FINEP/FUNTTTEL-TV Digital – 05/2004. São Paulo, 02 de Março de 2006

MARTINEZ, J. M. **MPEG-7 Overview** (version 10). Palma de Mallorca. Outubro de 2004

MERABTI, M.; LLEWELLYN-JONES, D. **Digital Rights Management in Ubiquitous Computing**. IEEE MultiMedia Magazine, p.32 a p. 42. Junho de 2006.

MYERS, M.; ANKNEY, R.; MALPANI, A.; GALPERIN, S.; ADAMS, C. **RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)**, 1999. Disponível em: <<http://www.ietf.org/rfc/rfc2560.txt>>. Acesso em: 24 de março de 2008.

NAMBA, S. **Scrambling (Conditional Access System)**, NHK STRL Broadcast Technology no.12, Autumn 2002.

NetBeans Project. Disponível em: < <http://www.netbeans.org/index.html> >. Acessado em: setembro de 2008.

NINOMIYA, Y. **HDTV Broadcasting Systems**, em IEEE Communicatios Magazine, Agosto de 1991

NINOMIYA, Y. **The Japanese scene**, *IEEE Spectr.*, vol. 32, no. 4, pp. 54–57, Abril de 1995. [art_hist4]

NOMOTO, Y. **NHK Digital Data Broadcasting System and Services**. In: BROASCASTASIA CONFERENCE PAPERS, 3., 2004, Singapura. Disponível em: <<http://www.broadcastpapers.com/BcastAsia04/BAsia04JapanBCDigBcast.pdf>>. Acesso em: 30 jun. 2005.

NUNES, R. P. **Estudo, Otimização e Implementação de uma Arquitetura Reconfigurável para Set-Top-Box Digital**. 2003. Projeto de Pesquisa - Escola Politécnica, Universidade de São Paulo. São Paulo, 2003.

OUGI, H. **Cryptographic communication method, encryption algorithm shared control method, encryption algorithm conversion method and network communication system**. United States Patent 7110548. Setembro de 2006

PARK, J.-S.; SANDHU, R. **Smart Certificates: Extending X.509 for Secure Attribute Service on the Web**. NISSC, 1999.

POLK, W.; HOUSLEY, R.; BASSHAM, L. **RFC 3279 – Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**, 2002. Disponível em: <<http://www.ietf.org/rfc/rfc3279.txt>>. Acesso em: 24 de março de 2008.

RECEITA FEDERAL. **Leiaute dos Certificados Digitais da Secretaria da Receita Federal do Brasil**. Versão 4.1. Publicado em 2002. Disponível em <http://www.receita.fazenda.gov.br/acsr/LeiautedeCertificadosdaSRF.pdf>. Acessado em: fevereiro de 2009.

RIBEIRO, G. **Como funciona o certificado digital**. 2008. Disponível em: <<http://informatica.hsw.uol.com.br/certificado-digital.html>>. Acesso em: 13 de agosto de 2008.

RIVEST, R. RFC1321 - **The MD5 Message-Digest Algorithm**. Network Working Group. Abril de 1992

ROUGHLY. **How FairPlay Works: Apple's iTunes DRM Dilemma**. 26 de Fevereiro de 2007. Disponível em : < <http://www.roughlydrafted.com/RD/RDM.Tech.Q1.07/2A351C60->

[A4E5-4764-A083-FF8610E66A46.html](#)>. Acessado em : 30 de março de 2008

SANCHEZ-AVILAF, C.; SANCHEZ-REILLOT R. **The Rijndael Block Cipher (AES Proposal): A Comparison with DES**, IEEE, 2001

SHIREY, R. **RFC 2828 - Internet Security Glossary**, 2000. Disponível em: <<http://www.ietf.org/rfc/rfc2828.txt>>. Acesso em: 28 de março de 2008.

SNOEYINK, J.; SURI, S.; VARGHESE, G. **A lower bound for multicast key distribution**. IEEE INFOCOM 2001 Proceedings. Alaska. 2001.

SOARES, L. D.; PEREIRA, F. **Protecção de Informação de Vídeo em Arquitecturas Baseadas em Objectos**. Disponível em: <www.img.lx.it.pt/~fp/artigos/CONFTELE97_errores.doc>. Acessado em: Dezembro de 2008.

SUBRAMANYA, S. R.; YI, B. K. **Digital rights management**. IEEE POTENTIALS pg 31 a 34. Março de 2006.

SDN. **Sun Developers Network**. Disponível em: <<http://java.sun.com/javase/downloads/index.jsp>>. Acessado em: setembro de 2008.

STM. **Smartcard ICs for pay-TV applications**. Outubro de 2008. Disponível em: <<http://www.st.com/stonline/products/promlit/pdf/flscpaytv1008.pdf>>. Acessado em: janeiro de 2009.

YOSHIMURA, T. **Conditional Access System for Digital Broadcasting in Japan**, proceedings of the IEEE, VOL. 94, NO. 1, JANUARY 2006

UNIÃO BRASILEIRA DE VÍDEO. **UBV a Serviço do Produto Legal**, Disponível em: <<http://www.ubv.org.br/>>. Acessado em: 30 de março de 2008.

US CODE COLLECTION, title 44, chapter 35, subchapter iii, § 3542. **Information Security**. Disponível em: <http://www.law.cornell.edu/uscode/html/uscode44/usc_sec_44_00003542---000-.html>. Acessado em: 30 de março de 2008.

VAZ, R. A. **Uma Interface de Comunicação Sem Fio em TV Digital Baseada em Rádio Definido por Programa de Computador**. São Paulo, 2007. p. 200 Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.

VOLLBRECHT, J.; CALHOUN, P.; FARRELL, S.; GOMMANS, L.; GROSS, G.; BRUIJN, B.; LAAT, C.; HOLDREGE, N.; SPENCE, D. **RFC 2904 - AAA Authorization Framework**, 2000. Disponível em: <<http://www.ietf.org/rfc/rfc2904.txt>>. Acesso em: 25 março de 2008.

XStream Project. Disponível em: < <http://xstream.codehaus.org/>>. Acessado em: 30 de dezembro de 2008.

XRML— The Technology Standard for Trusted Systems in the eContentMarketplace. Disponível em: <http://www.xrml.org/>. Acessado em: janeiro de 2009.

WALTMAN, W. D.; PRESLEY A. **Reading and Critiquing na IDEF0 Model**. Automation & Robotics Research. Institute, Texas. Julho de 1993.

WANG, X.; Yin, Y. L.; YU, H. **Finding Collisions in the Full SHA-1**. CRYPTO 2005

YANG, C. H. **Performance Evaluation of AES/DES/Camellia on the 6805 and H8/300 CPUs**. Symposium on Cryptography and Information Security. Oiso, Japão. 2001

ZUFFO, M. K.; CARVALHO, E. R.; BARROS, G. G.; COSTA, L. C. P.; FARIA R. R. A.; NUNES, R. P.; LOPES, R. D. **The Brazilian Digital Television System Access Device Architecture**, Journal of the Brazilian Computing Society, no. 1; V. 13; March 2007

ZUFFO, M. K.; COSTA, L. C. P. **Segurança em Serviços para a TV Digital no Brasil**. Revista Digital, ano 1, nº1. Uma publicação do Instituto Nacional de Tecnologia da Informação (ITI). 2009.