ETSI TR 101 532 V1.1.1 (2015-02)

End-to-End Network Architectures (E2NA);
Mechanisms addressing interoperability of multimedia service and content distribution and consumption with respect to CA/DRM solutions

Reference
DTR/E2NA-00004-CA-DRM-interop

Keywords
CA, DRM, interoperability, terminal

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Project End-to-End Network Architectures (E2NA).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**may not**", "**need**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Alongside well established TV delivery solutions, new services and applications offering content via a variety of technical platforms over managed and unmanaged networks have emerged in a rapidly evolving environment. This has led to a widely fragmented market in terms of proprietary and standardized elements of the platforms and the CA/DRM solutions in use.

The variety of solutions, involving standardized and proprietary elements, presents obvious challenges to content providers wanting to distribute their content to broad communities of end-users while a fragmented world market is an obstacle for manufacturers of consumer equipment wanting to maximize economy of scale due to the need to adapt for different technical platforms and CA/DRM systems. Last but not least, consumers may appear to lack the utmost flexibility in choosing services and available content due to the service providers use of different delivery platforms and CA/DRM systems.

The present document examines the underlying reasons for the variety of delivery platforms focussing on standards and solutions in the market for CA/DRM interoperability and considers whether new standardization initiatives will help to reduce market fragmentation and improve interoperability in the solutions used for distribution and consumption of multimedia content.

1 Scope

The present document about "Mechanisms addressing interoperability of multimedia service and content distribution and consumption with respect to CA/DRM solutions" gives an overview and provides guidance on several CA/DRM subjects, presents related activities in standardization bodies and discusses implementation issues. Special attention is paid to existing solutions already introduced to the market with regard to interoperability as well as to emerging software-based solutions, all operated under a trusted environment.

Analysis of solutions for interoperable multimedia content distribution and consumption with respect to CA/DRM, suitable for Multimedia platforms (broadcast, broadband or hybrid) and to the content/services delivered over them is the main focus of the present document, addressing:

- A review of the status of existing and emerging standards together with other attempts to produce interoperable and interchangeable CA/DRM solutions suitable for multimedia consumption across multiple networks and platforms.
- A presentation of the practical framework required for implementation and operation of a CA/DRM system.
- An analysis of the interoperability available using current solutions and lessons from all the attempts reviewed.
- Emerging market needs.
- Concepts for market implementation including business roles, liability and trust.
- Regulatory and legal issues.

The present document covers all aspects of interoperability involving standardized elements concerning Conditional Access (CA) and Digital Rights Management (DRM) solutions associated with content distribution and consumption across various technical platforms for conventional Broadcast TV (DVB-C/C2, -S/S2, -T/T2) as well as for Broadband TV (including IPTV, WEB-TV) and Mobile TV.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 102 688-1: "Media Content Distribution (MCD); MCD framework; Part 1: Overview of interest areas".

[i.2] ETSI TR 102 688-3: "Media Content Distribution (MCD); MCD framework; Part 3: Regulatory issues, social needs and policy matters".

[i.3] Recommendation ITU-T X.1191: "Functional requirements and architecture for IPTV security aspects".

[i.4] ETSI TS 187 021: "Security services and mechanisms for customer premises networks connected to NGN".

[i.5] ETSI TS 187 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".

[i.6] Recommendation ITU-T J.293: "Component definition and interface specification for the next generation set-top box".

[i.7] ETSI TS 102 796: "Hybrid Broadcast Broadband TV".

[i.8] IETF RFC 5027: "Security Preconditions for Session Description Protocol (SDP) Media Streams".

[i.9] IETF RFC 4046: "Multicast Security (MSEC) Group Key Management Architecture".

[i.10] IETF RFC 3830: "MIKEY: Multimedia Internet KEYing".

[i.11] IETF RFC 4909: "Multimedia Internet KEYing (MIKEY) General Extension Payload for Open Mobile Alliance BCAST LTKM/STKM Transport".

[i.12] IETF RFC 4535: "GSAKMP: Group Secure Association Key Management Protocol".

[i.13] ISO/IEC 14496-12: "Information technology -- Coding of audio-visual objects -- Part 12: ISO base media file format".

[i.14] ISO/IEC 23001-7: "Information technology -- MPEG systems technologies -- Part 7: Common encryption in ISO base media file format files".

[i.15] ISO/IEC 23009-1: "Information technology -- Dynamic adaptive streaming over HTTP (DASH) -- Part 1: Media presentation description and segment formats".

[i.16] ETSI TS 103 162: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; K-LAD Functional Specification".

[i.17] Information about gaining access to the DVB Common Scrambling Algorithms (DVB-CSAX).

NOTE: Available at http://www.etsi.org/services/security-algorithms/dvb-csa-algorithm.

[i.18] ETSI TS 100 289 (V1.2.1): "Digital Video Broadcasting (DVB); Support for use of the DVB Scrambling Algorithm version 3 within digital broadcasting systems".

[i.19] ETSI TS 101 699 (V1.1.1): "Digital Video Broadcasting (DVB); Extensions to the Common Interface Specification".

[i.20] ETSI TS 103 197 (V1.5.1): "Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt".

[i.21] ETSI TS 102 474: "Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Service Purchase and Protection".

[i.22] ETSI TS 102 825: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM)".

[i.23] ETSI EN 300 294: "Television systems; 625-line television Wide Screen Signalling (WSS)".

[i.24] HDCP Rev 2.2: "High Bandwidth Digital Content Protection (HDCP)".

[i.25] CI Plus v1.3 CI Plus version 1.3.

[i.26] EC Universal Service Directive 2002/22/EC amended by Directive 2009/136/EC.

[i.27] Recommendation ITU-T X.1192: "Functional requirements and mechanisms for the secure transcoding of IPTV".

[i.28] Recommendation ITU-T X.1193: "Key management framework for secure IPTV services".

[i.29] Recommendation ITU-T X.1195: "Service and content protection (SCP) interoperability scheme".

[i.30] DLNA® Guidelines.

NOTE: Available to DLNA® members at http://www.dlna.org/dlna-for-industry/guidelines.

[i.31] ATIS specifications.

NOTE: Available to ATIS members at http://www.atis.org/iif/digitalrm.asp.

[i.32] W3C Encrypted Media Extensions (EME).

NOTE: Available at http://www.w3.org/TR/encrypted-media/.

[i.33] W3C Media Source Extensions (MSE).

NOTE: Available at https://dvcs.w3.org/hg/html-media/raw-file/tip/media-source/media-source.html.

[i.34] Open Mobile Alliance (OMA) Mobile Broadcast Services Enabler.

NOTE: Available at http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/oma-mobile-broadcast-services-v1-3.

[i.35] Open Mobile Alliance (OMA): "BCAST DRM profile based on OMA DRM 2.0".

[i.36] Open Mobile Alliance (OMA): "BCAST SmartCard profile".

[i.37] IETF RFC 380: "Multimedia Internet Keying (MIKEY)".

[i.38] 3GPP TS 23 246: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description".

[i.39] 3GPP TS 33 246: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)".

[i.40] DECE Common File Format (CFF).

[i.41] ETSI TS 103 127 (V1.1.1): "Digital Video Broadcasting (DVB); Content Scrambling Algorithms for DVB-IPTV Services using MPEG2 Transport Streams".

[i.42] Recommendation ITU-T X.1194: "Algorithm selection scheme for service and content protection descrambling".

[i.43] Recommendation ITU-T X.1196: "Framework for the downloadable service and content protection system in the mobile IPTV environment".

[i.44] Recommendation ITU-T X.1197: "Guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection".

[i.45] Recommendation ITU-T X.1198: "Virtual machine-based security platform for renewable IPTV service and content protection".

[i.46] Recommendation ITU-T J.1001: "Requirements for conditional access client software remote renewable security system".

[i.47] CENELEC EN 50221: "Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications".

[i.48] MovieLabs group specification for enhanced content protection.

NOTE: Available at http://www.movielabs.com/ngvideo/MovieLabs%20Specification%20for%20Enhanced%20Content%20Protection%20v1.0.pdf.

[i.49] ETSI ISG ECI white paper.

NOTE: Available at http://portal.etsi.org/ECI/ETSI%20ISG%20ECI%20White%20Paper-v1_20.pdf.

[i.50] ATIS-0800001.v003: "IPTV DRM Interoperability Requirements".

NOTE: Available at https://www.atis.org/docstore/product.aspx?id=26099.

[i.51] ATIS-0800006.v002: "IIF Default Scrambling Algorithm (IDSA) IPTV Interoperability Specification".

NOTE: Available at https://www.atis.org/docstore/product.aspx?id=25435.

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3DES	Triple Digital Encryption Standard
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
AAA	Authentication, Authorization, Accounting
AES	Advanced Encryption Standard
AMD3	Ammendment 3
API	Application Programming Interface
ARDP	Access Right Distribution Protocol
ARIB	Association of Radio Industries and Businesses
ASIC	Application Specific Integrated Circuit
ATIS	Alliance for Telecommunications Industry Solutions
ATTM	Access, Terminals, Transmission and Multiplexing
AVMSD	AudioVisual Media Services Directive
B2B	Business to Business
BB	Marlin Broadband specification
BCAST	OMA Mobile Broadcast services specifications
BCMCS	3GPP BroadCast MultiCast Service
C&R	Compliance and Robustness
CA	Conditional Access
CA/DRM	Conditional Access/Digital Rights Management
CAM	Conditional Access Module
CAS	Conditional Access System
CCSA	China Communications Standards Association
CE	Consumer Electronics
CENC	Common ENCryption
CENELEC	European Committee for Electrotechnical Standardisation
CFF	Common File Format
CGMS-A	Copy Generation Management System - Analog
CI Plus	Common Interface Plus
CI	Common Interface
CISSA	Common IPTV Software-oriented Scrambling Algorithm
CMLA	Content Management License Administrator
CMMB	China Mobile Multimedia Broadcasting
CORAL	The Coral Consortium
CPCM	Content Protection & Copy Management
CPE	Customer Premises Equipment
CPU	Central Processing Unit

CSA	Common Scrambling Algorithm
DASH	Dynamic Adaptive Streaming over HTTP
DCAS	Downloadable Conditional Access System
DECE	Digital Entertainment Content Ecosystem
DIS	DRM Interoperability Solution
DLNA®	Digital Living Network Alliance
DPA	Differential Power Analysis
DRM	Digital Rights Management
DTCP-IP	Digital Transmission Copy Protection - Internet Protocol
DTG	Digital TV Group
DTLA	Digital Transmission Licensing Administrator
DVB	Digital Video Broadcasting
DVB-C/C2	Digital Video Broadcasting - Cable, First and Second Generation
DVB-CA	DVB Conditional Access
DVB-CBMS	DVB Convergence of Broadcasting and Mobile Services
DVB-CI	DVB Common Interface
DVB-H	DVB Handheld
DVB-NGH	DVB Next Generation Handheld
DVB-S/S2	Digital Video Broadcasting - Satellite, First and Second Generation
DVB-SH	Digital Video Broadcasting - Satellite Handheld
DVB-T/T2	Digital Video Broadcasting – Terrestrial, First and Second Generation
DVD	Digital Versatile Disc
EBU	European Broadcasting Union
EISA	Extended Industry Standard Architecture
EME	Encrypted Media Extensions
ETSI	European Telecommunications Standards Institute
EU	European Union
eUMTS	Enhanced Universal Mobile Telecommunications System
FCC	Federeal Communications Commission
FLO	Forward Link Only
FLUTE	File Delivery over Unidirectional Transport
GBA	Generic Bootstrapping Architecture
GSAKMP	Group Secure Assciation Key Management Protocol
GSM	Global System for Mobile
HbbTV®	Hybrid Broadcast Broadband TV
HD	High Definition
HDCP	High-bandwidth Digital Content Protection
HSF	Harmonized Security Framework
HTML	HyperText Markup Language
HTML5	HyperText Markup Language version 5
HTTP	HyperText Transfer Protocol
IAB	Internet Architecture Board
ID	Identity
IDSA	IIF Default Scrambling Algorithm
iDTV	Integrated Digital Television
IEC	International Electrotechnical Commission
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IIF	IPTV Interoperability Forum
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPDC	Internet Protocol Datacast
IPR	Intellectual Property Rights
IPSEC	Internet Protocol Security
IPTV	Internet Protocol Television
IPTV-GSI	Internet Protocol Television Global Standards Initiative
ISDB-T	Integrated Services Digital Broadcasting Terrestrial
ISG ECI	Industry Specific Group Embedded Common Interface
ISMA	Internet Streaming Media Alliance
ISO BMFF	ISO Base Media File Format
ISO	International Organization for Standardization
ITU	International Telecommunication Union

ITU-T	International Telecommunication Union-Telecommunication
JTC	Joint Technical Committee
KLAD	Key LADder
LLP	Limited Liability Partnership
LTE	Long Term Evolution
LTKM	Long Term Key Message
MBMS	Multimedia Broadcast Multicast Services
MIKEY	Multimedia Internet Keying
MLDv2	Multicast Listener Discovery version 2
MPEG	Moving Picture Experts Group
MPEG2 (M2TS)	Motion Picture Experts Group 2 Transport Stream
MPEG-DASH	Motion Pictures Expert Group - Dynamic Adaptive Streaming over HTTP
MSE	Media Source Extensions
MSEC	Multicast SECurity
MSK	MBMS Service Key
MSOs	Multiple System Operators
MTK	MBMS Traffic Key
NGN	Next Generation Networks
OIPF	Open IPTV Forum
OMA	Open Mobile Alliance
OS	Operating System
OTT	Over-The-Top
PKI	Public Key Infrastructure
QoS	Quality of Service
RAM	Random Access Memory
RFC	Request For Comments
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
RUIM	Removable User Identity Module
SARFT	State Administration of Radio, Film and Television
SCP	Service and Content Protection
SDP	Session Description Protocol
SE	Secure Element
SIM	Subscriber Identity Module
SPP	Service Purchase and Protection
SR	Special Report
SRTP	Secure Real-time Transport Protocol
STB	Set-Top Box
STKM	Short Term Key Message
SW	Software
TA	Trust Authority
TC	Technical Committee
TEE	Trusted Execution Environment
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TNT2	Digital Terrestrial Television 2
TR	Technical Report
TS	Technical Specification
TTA	Telecommunications Technology Association
TTC	Telecommunications Technology Committee
TV	Television
UHD	Ultra High Definition
UHDTV	Ultra High Definition Television
UIM	User Identity Module
UK	United Kingdom
UMTS	Universal Mobile Telecommunications System
US	United States
USA	United States of America
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
USP	Unique Selling Point
W3C	World Wide Web Consortium
WEB-TV	Web delivered Television

WiMAX	Worldwide Interoperability for Microwave Access
WM	Windows Media
WMDRM-ND	Windows Media Digitial Rights Mechanism Network Devices

4 The role and importance of CA/DRM solutions

4.1 Introduction

This clause provides background information about why CA/DRM systems are used to provide security for pay TV content and how the integrity of each CA/DRM system is assured by an entity known as a "Trust Authority" which accepts liability for the system and consequently sets rules which govern its use.

4.2 Basic introduction to CA/DRM systems

Content rights owners, and system operators acting on their behalf, want to restrict consumption of their content to just those users who are explicitly authorized to consume it and to prevent it from being copied or re-transmitted unless the user has been granted the right so to do. The rights owners may wish to apply further restrictions such as a limit to the period of time over which a piece of stored content can be consumed. The purpose of Conditional Access (CA) and Digital Rights Management (DRM) systems is to fulfill the content rights owners' requirements to protect content from misuse according to the rules and rights they wish to impose.

The term CA was applied to earlier pay TV security systems in which content consumption is *conditional* on the system operator authorizing a viewer to have *access*. These CA systems usually relied on a piece of removable hardware - a viewing (or smart) card as part of their architecture - and did little apart from protect the TV content while it was in a unidirectional broadcast channel. The removable hardware was introduced as an enabler to the concept of renewability - the ability to upgrade and renew important parts of a security platform without having to change out the whole of it. Although not without cost, the replacement of, for example, a viewing card and download of new accompanying software is considerably cheaper than changing a population of terminals and is regarded as a cost effective means to respond to piracy or the threat of it. The detailed design of the removable/replaceable hardware is proprietary, outside the scope of any standard, in order that it can support counter measures that are not known to hackers and so that it can be changed out at a time that suits business requirements. The new accompanying software is delivered using a secure download process. When using a CA module with no viewing card, the renewability can be achieved using a similar process to that for systems that include a viewing card. The application of Digital Rights Management or DRM systems began with a broader scope of applicable content than the traditional CA system, for example to books, images and other media, and implemented many of the usage restrictions, which most modern CA systems are now also able to support. These usage restrictions set, for example, rules to be applied to the storage of content and the means by which it may be exported or consumed from the user device. DRM systems typically have no removable hardware element such as a viewing card; the security system is composed of replaceable software although it may relate to and depend on certain fixed hardware elements. Hence, modern CA and DRM systems can provide similar functionality for a pay TV environment.

The fundamental architecture used by CA and DRM systems alike to protect content is one in which content is encrypted using a scrambling algorithm and a key to seed the scrambling. The key, or in some cases an artefact that allows the key to be locally generated, is encrypted so that it can be conveyed securely to the viewer at the point of reception; it is usually integrated into the broadcast channel or otherwise associated to the content. The security system of the viewer decrypts the key and uses it to descramble the content in order to allow the rights granted in terms of consumption, storage and re-transmission to be exercised. In broadcast applications, the key is normally changed periodically in order to make it harder for an attacker to determine what it is or to predict it when it changes.

In addition to a removable hardware element, CA systems based on the DVB Common Scrambling Algorithm specifications employ a scrambling algorithm that is designed to be far easier to implement in hardware than software on general purpose processors.

NOTE: Some DRM systems also support the use of the DVB Common Scrambling Algorithm, about which further information can be found in clause 5.1.

The design topology, involving fixed and typically removable hardware as well, is intended to make it more difficult for a system to be attacked by someone who seeks to gain an understanding of the software code of the system and to access it. In addition, a specific implementation design of a scrambling algorithm can be protected by registering IPR, operating a license regime for bona fide users and pursuing anyone who violates the terms of the license by legal measures. A high level of resilience and protection is particularly important in a security system in which the content rights owner or system operator is using a unidirectional broadcast system and has no direct bidirectional communication path with the viewer's security system.

Although it is important to ensure that scrambling algorithms in use are robust against current threats and those that can be predicted over the expected system lifetime, breaches to security systems are seldom accomplished by the exploitation of a direct attack involving the scrambling algorithm used to encrypt content. In practice, successful attacks are usually achieved by exploiting an inherent weakness in the implementation or in the key management system which allows the keys to be predicted, generated or discovered and transferred to the user's system at the rate at which they are required for the descrambling process.

It is of the utmost importance that a security system is designed to prevent unauthorized access to the code or any other aspect of the operation of the security system that might allow a third party to access or otherwise discover the keys that are used; it will be *robust* against attacks. It is also a necessary feature of a security system that it can be upgraded to respond to evolving security threats and business needs. In order to reconcile these two requirements, upgrades will be accomplished securely such that the viewer's system will only accept software from a verified source so that an upgrade can be *trusted*. The topics of robustness and trust are discussed in the following clause.

4.3 Introduction to the role of Trust Authorities

Content security systems necessarily rely on a Trust Authority (TA) for their commercial deployment. The Trust Authority has the following main roles:

- publish and maintain a set of compliance rules that define the mandatory behaviour of devices/entities belonging to the content security ecosystem;
- publish and maintain a set of robustness rules that define the minimum security level for a device/entity belonging to the content security ecosystem;
- provide device/entities that belong to the content security ecosystem (i.e. that conform to compliance and robustness rules) with the necessary cryptographic key material, e.g. a certificate and associated private key;
- monitor the content security ecosystem for early detection of devices/entities that do not conform to compliance and robustness rules or for early detection of security breaches;
- take necessary actions (e.g. revocation; compliance and robustness rules update; etc.) to remedy non-compliance or security breaches; and
- provide a legal framework for all entities belonging to the content security ecosystem.

In addition, some Trust Authorities verify compliance and/or security robustness or appoint external third parties to perform these verifications.

The absence of a Trust Authority would result in low- (or even zero-) security level implementations of the content security system that could be easily breached without any efficient means to remove these implementations from the content security ecosystem. Content providers may refuse to provide their content for distribution on such content security ecosystems.

For proprietary CA or DRM systems, the role of Trust Authority is often taken by the CA or DRM provider itself. For security systems defined by a standard or a consortium, a dedicated legal entity is generally created or used to play this role (e.g. DTLA for DTCP-IP or CMLA for OMA DRM).

5 Current landscape of CA and DRM solutions

5.1 Introduction

This clause covers the market status of CA and DRM solutions and related information, which either are standardized or being developed by industrial organizations and fora.

5.2 DVB

5.2.1 About the DVB

The DVB project is a consortium established in 1994 with about 200 members, which devises and maintains DVB standards and conditions in a Joint Technical Committee (JTC) with ETSI, CENELEC and the EBU. See also www.dvb.org.

5.2.2 DVB-CA

In September 1994, agreement was reached in the DVB project to offer three basic standards aimed at enabling interoperability of content and services across multiple networks using different proprietary CA systems.

- DVB Common Scrambling Algorithm (DVB-CSA) [i.17], (DVB-CSA3) [i.18].
- DVB Common Interface (DVB-CI) [i.19] (see also clause 5.2.5 introducing CI Plus).
- DVB Simulcrypt (DVB-SIM) [i.20].

These standards are used worldwide for broadcast and their principles are available in many other standards such as ISDB-T, FLO, CMMB, etc. These standards allow interoperability of broadcast service access across operator networks and devices insofar as commercial and business agreements allow such interoperability. DVB is not limited to broadcast; the principles of the approach also apply to IPTV, mobile TV, OTT and other services.

The encryption algorithms DVB-CSA v1/DVB-CSA v2 standardized by DVB are based on the same algorithm but with different key lengths. They were not published by the DVB project for security reasons but are available under licence. They were designed to be "hardware friendly", meaning that implementation in software was technically difficult to process. As processor power and speed has improved over time, resistance to software implementation has reduced and the key length is now beginning to be regarded as relatively short. These factors inspired DVB to create a new, more complex and secure version which was standardized as DVB-CSAv3 in 2007. CSAv3 is supported by new terminal equipment now arriving on the market, however migrating to CSAv3 requires the previous generation of terminal equipment to be replaced. The DVB-CSA licensing management for all 3 algorithms is handled by ETSI as the custodian.

In addition to the CSA algorithms DVB also standardized a software-oriented scrambling algorithm called CISSA (Common IPTV Software Oriented Scrambling Algorithm) [i.41] which was designed as "software-friendly", meaning that the algorithm is easy to implement in either hardware or software in order to support with a software implementation also terminals that are using general purpose CPUs. Low cost end user devices typically still use a hardware accelerator element. The algorithm uses the AES cipher.

CA systems are based on different technologies for management of keys but typically rely on the standardized common scrambling algorithm for content protection. CA systems from different technology providers are mutually incompatible. This means that a user's set-top box with an integrated CA/DRM system is not interoperable with other systems, although interoperability can be provided at the headend level when business agreements require this through the DVB Simulcrypt standard which provides for the synchronization of keys between different CA systems.

DVB also developed the Common Interface (DVB-CI) standard. This specifies the hardware interface on the terminal or host equipment and the CA module (CAM) interface and functionality. Typically a viewing (smart)card is used in conjunction with the CAM to personalize the service with viewer subscription products and essential security elements, but it is also possible to embed security credentials in a module. This architecture allows periodic updates to be made to the security system by changing the viewing card (where used) or the entire CA/DRM system can be replaced by changing the CAM.

Terminal devices can accept any compatible CAM allowing multiple CA systems to be used to access various services from multiple service providers when there is no commercial agreement to share the content through Simulcrypt. It is also possible to embed multiple CA systems in the same CAM allowing a single CAM to access several networks with different CA systems.

The Common Interface (CI) has not enjoyed lasting support in the international market in the standardized form of 1997. This is largely due to security concerns about the unencrypted digital transport stream interface which could be used for unauthorized copying; there were also concerns about possible circumvention of certain specific national requirements on Protection of Minors (refer also to AVMSD, protection of minors). These concerns led to a lack of support from some network operators and content providers (although it is still in use in for example Switzerland, Austria and the Netherlands). CI Plus was developed to fill these technical gaps. For further details see clause 5.2.5 on CI Plus.

Under the title "CA neutral CPE" DVB attempted to standardize all hardware components required for an encryption system and the required interfaces. This was supposed to ensure that the terminal equipment could be relatively easily switched via a software update from one CA system to another. This attempt, which was not the first of its kind in DVB, was not continued due to a lack of support from key market participants and a lack of market demand once a number of other complexities concerning divergent middlewares, network connectivity and liability had become apparent.

5.2.3 DVB-SPP

In the field of mobile broadcasting, DVB-H was the standard favoured both by many market partners for transmission. The key components for the provision of services and contents are located in the "service enabler layer", which was specified by the DVB-CBMS working group under the term DVB-IPDC [IP data cast]. The IPDC suite of specifications defines the security-related components under the term "Service Purchase and Protection (SPP)" [i.21].

Transport encryption is realized at or above IP level. With IPSec and SRTP, DVB uses the open standard procedures of the IETF and with ISMACryp an open procedure of a group of interested parties (ISMA). SRTP and IPSEC scramble at the link (IP) level whereas ISMACryp scrambles at the content level which allows content to remain encrypted further into the device architecture if required. All procedures are based on the AES cypher. Since agreement was not reached on one encryption method, the SPP specification includes three methods as alternatives that are all implemented in the terminal equipment according to the standard. In the current stage of market development, only the system ISMACryp achieved market penetration.

For the service-specific key management, the IPDC SPP specification provides for three alternative methods:

- the 18Crypt method is based on OMA DRM 2.0, providing a fully standardized solution;
- the OMA BCAST Smartcard Profile based on the secure tamper resistant module (USIM/RUIM) and providing a fully standardized solution; or
- the DVB Open Security Framework defines a framework enabling any proprietary, vendor-specific or standard solutions to be supported as plug-in.

The Open Security Framework approach was used in US and Italy with several millions of devices based on this technology in the field. The Open Security Framework was also adopted by the FLO Forum and standardized as the security framework by the US Telecom Industry Association in charge of US Telecom Standards. This Open Security Framework approach was used in the MediaFlo service deployment.

5.2.4 DVB-CPCM

The scope of CA systems on traditional transmission paths comprises safeguarding the transmission side and controlling the use of options in terminal equipment. It usually ends at the interfaces of the terminal equipment, where other copy protection systems, such as CGMS-A [i.23] and HDCP [i.24], are used. If other devices are to be connected in the home environment, the problem arises of how to control further use. With the "Content Protection and Copy Management" (CPCM DVB) standard [i.22], the DVB project has developed a system that - with reference to the required DRM functions - permits separation between the transmission side and the functions required in the home area.

Content is first protected and distributed on the distribution networks with arbitrary CA/DRM systems. In the terminal equipment, content and the associated rights information can be safely passed to the standardized CPCM system.

Within the "authorized domain" that defines the personal environment of the user in terms of rights, content can then be safely transported and used according to the transmitted rights information.

As for any other content protection technology, CPCM requires a Compliance and Robustness Regime (C&R) to be in place prior to being launched to the market. This C&R Regime is still missing despite several attempts to create it. Because of this and despite several companies having produced working implementations of CPCM, it is currently unclear to what extent CPCM is still supported by relevant market players. CPCM may also be perceived as too complex to have cost-effective implementations and to be understood by end-users.

5.2.5 CI Plus

The DVB-CIv1 (CI version 1) specification (refer to clause 5.1.1) was developed in the mid-90s based on the EISA physical format and no longer corresponds to today's requirements in terms of the following aspects:

- German "Protection of Minors Act" (in safe interaction with CA systems);
- Copy protection; and
- Re-encryption.

Consequently, fewer network operators and content providers were using it but EU directives [i.26] require a common interface to be fitted to all iDTVs (integrated digital televisions) with screen size larger than 30 cm; refer also to [i.1] and [i.2]. These factors inspired the creation of a successor interface.

Work on this successor began as CIv2 in the DVB project, for which appropriate commercial requirements were adopted in 2006. The subsequent work on the technical specification based on these commercial requirements did not progress within the DVB project due to differing ideas about the techniques to be applied and the timeframe to be met. Instead, some companies decided in mid-2007 to pursue work outside of the DVB Project in a new industry group, which they named "CI+ Forum". In November 2008 this resulted in the first version of the CI Plus specification and the creation of the related certificate issuing organization named Limited Liability Partnership (LLP CI Plus). The CI Plus Specification (V1.3) [i.25], CI Plus Device Interim License Agreement and the CI-Plus Test Specification can be found at: www.ci-plus.com.

As the certificate issuer, CI Plus LLP acts as a trust authority for the operation of CI Plus. For secure implementation, one will, as a subcontractor, make use of such a trust authority. The specification was developed in a small, closed group but responsibility for maintenance and development of the specification has now been taken back into DVB with the result that version 1.4 has been finalized for submission to ETSI. Up to v1.4, all specifications use the same form factor for the physical interface and retain backwards or legacy compatibility with earlier versions to the extent of the functionality that the earlier versions provide. V1.4 adds support for multi-stream handling and IP delivered content. The specification can be found at: www.dvb.org/resources/public/standards/a165_dvb-ci-plus_v_1_4.pdf.

DVB's plans for future versions of the CI Plus interface are all based on a new physical form factor based on USB that is expected to make it cheaper to implement in TV devices and CAMs than the current interface.

5.2.6 DVB Harmonized Security Framework

The DVB Harmonized Security Framework (HSF) was prepared by a group of security experts to provide clear advice in the form of guidelines to other DVB groups working on commercial requirements for future DVB standards. The first edition of the HSF was approved for use within DVB by the DVB Steering Board in April 2007. The group responsible for its maintenance has been working for the last two years on an update. In the meantime, the advice offered by the original 2007 document remains relevant to the communities working on standards who have need to consider user or system security and data privacy.

The HSF notes that "in the last several years, networks and devices capable of the delivery and rendering of premium content have increased in types and number". This is clearly a trend that is continuing as the proliferation of smart devices has gathered pace.

The HSF defines overarching security guidelines for DVB Commercial Requirements documents. These guidelines either address the generic security aspects, content protection/security, privacy and system security.

The stated aims of the HSF are to synchronize "security requirements across different DVB specifications" in order to:

- promote interoperability;
- facilitate choice;
- encourage competition for all stakeholders including security providers, CE manufacturers and broadcasters;
- not favour one particular vendor/operator;
- not prevent the introduction of new business models;
- not invalidate existing business models and platforms; and
- not invalidate existing DVB security specifications.

The requirements that are the most pertinent to a report about pay TV security cover:

- upgradeability;
- global system security (for example designs should ensure that single device hacks cannot being deployed system wide);
- minimizing changes to a standard that are necessary to overcome hacks; and
- counter measures to allow for revocation and renewal.

The HSF makes a special note about standardizing code download security, which it states "may compromise the security of other aspects of the device" and concludes that "DVB should not standardize a code download security mechanism".

5.3 ETSI - TISPAN

TC (Technical Committee) TISPAN (Telecoms & Internet converged Services & Protocols for Advanced Networks) was established in ETSI in 2003 for the standardization of Next Generation Networks (NGN) and services, extending the 3GPP IMS concepts to the fixed networks, and ended its activity in 2012.

The work on NGN Release 2 included specifications for IPTV, home networks and terminal equipment. Both the integration of IPTV solutions already available on the market into the NGN and a solution directly based on IMS were provided for IPTV. For the latter, a reference architecture was also defined for terminal equipment. Work on Release 3 includes extensions to IPTV and security issues. The activity in ETSI TISPAN has produced a complete set of documents that provide a comprehensive solution for IPTV support in NGN, both via the exploitation of the intrinsic IMS functionalities or by means of an external platform interworking with the NGN and the Customer Network devices.

For the aspects related to content and service protection, the reference document produced by TISPAN is ETSI TS 187 003 [i.5] "NGN Security; Security Architecture", with last revision in 2011. Its scope is in the main the security of NGN, but limited to its architecture, and one section covers specifically the IPTV service security.

The document does not focus on the technologies for content protection, but just provides indication about how this is to be taken into account in the general service security architecture described, defining the essential reference points and the basic functions.

For service protection, ETSI TS 187 003 [i.5] goes into more detail and provides a distinct specification for "any content protection" and for the case when OMA BCAST is the service protection solution of choice. For the first case it is requested that the content protection be compliant with the transport technologies specified for TISPAN IPTV. For the second case full reference is made to OMA BCAST specifications and a mapping between the two architectures provided.

A framework of specifications for IPTV was produced by TISPAN, including security aspects. In ETSI TS 187 021 [i.4] "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security services and mechanisms for customer premises networks connected to TISPAN NGN" a section covers aspects of a service and content protection architecture in association with a secure upgrade process.

OMA BCAST has been deployed but not on fixed IPTV networks. Deployments of IMS have been made, but none are known that include the IPTV framework.

5.4 ETSI KLAD System

ETSI TS 103 162 [i.16] defines a standardized key ladder to be used for secure provisioning of cryptographic keys (control words) for descrambling of video content in a multi-CA environment. The standard has three primary technical components:

a) a root-key derivation block used for deriving per-vendor unique root-keys from a single non-volatile key;

b) a 3-level key ladder using either AES or 3DES; and

c) a challenge-response mechanism for authenticating the device or for other uses.

The standard was created in response to a desire by the industry to have an interchangeable and multi-tenant security anchor integrated into the SoC, thereby avoiding the costly external security devices (CableCards, CI CAMs) used previously. Assuming an appropriate key management authority has been established in a given market, a device containing a chip implementing the ETSI standard can be sold in a retail environment that would support multiple CA systems and multiple Service Providers while retaining separation between the cryptographic keys used by each security system. The consumer could purchase the device and then connect it to the service provider of their choice and it would 'just work'. If moving to a new location, the customer could take their existing device with them and connect it to the network of their new service provider.

It is understood that there are millions of devices deployed worldwide that include hardware supporting the standard.

There are also three primary markets looking to deploy the entire 'ecosystem' described below:

1) USA: It is the early stages of deployment and service providers are acting as their own Trust Authority which gives them greater flexibility to change CA providers;

2) Korea: The regulator for the cable market is setting up a trust Authority; and

3) China: SARFT is setting up a trust authority.

5.5 ETSI ISG ECI

A new Industry Specification Group has been launched by ETSI in April 2014 on Embedded Common Interface for exchangeable CA/DRM solutions.

Industry Specification Groups have been established alongside ETSI's Technical Committees and Projects with Terms of Reference and a specific agreement for participation aimed at completing a defined task. Non-ETSI members can participate under certain conditions.

The reason to establish the ISG ECI is closely related to the current situation in a rapidly developing and converging area of digital Broadcast and Broadband, including content, services, networks and CPEs with service- and content protection realized by Conditional Access (CA) and Digital Rights Management (DRM) systems, which are essential to protect business models of content owners and PayTV operators.

The consumer electronics market for digital TV is fragmented, as Pay TV operators have defined specifications that differ not only per country, but also per platform. The five ISG ECI Founding Members saw the need to address one aspect of fragmentation by considering a standardized environment for a general purpose, SW based, embedded, exchangeable CA/DRM system to allow users to switch security system without changing the hardware platform.

The Founding Members of ETSI ISG ECI envisage in the white paper [i.49] that the key benefits of the approach for content security are

- Flexibility and scalability due to SW based implementation.
- Applicability to content distributed via broadcast and broadband, including OTT.
- Support of multi-screen environment.

- Opening of the market by avoiding "Lock-in" for platform operators, network/service providers, and consumers.
- Open entire eco-system fostering market development.

A number of Work Items and first Group Specifications have been approved within the ISG ECI so far and further activities will address architecture and interfaces for ECI clients in a CPE, including loader mechanisms, light virtual machine and an advanced security functionality based on a chain of trust.

The standardization work of ISG ECI is supported by several members of the value chain.

The target is that ISG ECI compliant CPEs will enable the end user to consume PayTV content from a broad range of Broadcast and Broadband sources delivered to retail devices (STB and iDTV) as well as to a number of mobile devices, including smart phones and tablets. This will involve creating tiered trust mechanisms and an architecture flexible enough to achieve these aims across a diverse device population. Legal arrangements supporting the trust mechanisms will need to be established in order to create an eco-system based on ECI technologies. These legal aspects are out of scope of the ISG ECI work.

5.6 ITU-T

The International Telecommunications Union (ITU) based in Geneva is a United Nations agency involved in worldwide technical aspects of telecommunications. Many of the developed Recommendations are adopted within the ITU by the ITU-T, the responsible Telecommunication Standardization Sector. Due to the broad scope of application and, at times, rather differing market structures in the individual member states, issues such as CA/DRM are always treated by the ITU-T within a wider context, such as IPTV and Security (in ITU-T Study Group 17). Recommendations regarding CA/DRM issues have been mainly taken into account in Asia so far. The ITU-T documents can be distinguished for the following fields of application:

- CA/DRM for "classic" broadcasting.
- CA/DRM for IPTV and web TV.
- CA/DRM for mobile TV.

Some documents so far are of a conceptual nature. Chapter 7.4 of the Recommendation ITU-T-Rev. J.293 [i.6] "Component Definition and Interface Specification for Next Generation Set-Top-Box" may be used for discussion on the CA/DRM issue. The approach of a flexible conditional access system (CAS) illustrated therein that is based on hardware and software components addresses requirements such as a security system that can be replaced by software-only download or the implementation feasibility of multiple encryption algorithms. Moreover, the Recommendation ITU-T X.1191 [i.3] (formerly developed as X.iptvsec-1 in the IPTV-GSI and approved by study group 17), entitled "Functional Requirements and Architecture for IPTV Security Aspects", includes requirements for content security and scrambling algorithms as well as the interoperability of Service and Content Protection (SCP).

Further parts of the X.iptvsec-series of Recommendation ITU-Ts have been finalized:

- **X.1192 (former X.iptvsec-2) [**i.27**]:** Functional requirements and mechanisms for the secure transcoding of IPTV
- **X.1193 (former X.iptvsec-3) [**i.28**]:** Key management framework for secure IPTV services
- **X.1194 (former X.iptvsec-4) [**i.42**]:** Algorithm selection scheme for service and content protection (SCP) descrambling
- **X.1195 (former X.iptvsec-5) [**i.29**]:** Service and content protection (SCP) interoperability scheme
- **X.1196 (former X.iptvsec-6) [**i.43**]:** Framework for the downloadable service and content protection (SCP) system in the mobile IPTV environment
- **X.1197 (former X.iptvsec-7) [**i.44**]:** Guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection (SCP)
- **X.1198 (former X.iptvsec-8) [**i.45**]:** Virtual machine-based security platform for renewable IPTV service and content protection (SCP)

Among these mentioned Recommendations X.1193 [i.28] describes a downloadable Service and Content Protection (SCP) system which includes a trusted environment.

Recently more Recommendations with regard to CA/DRM have been developed or are progressing; among new Recommendations specifically Recommendation J.1001 "Requirements for conditional access client software remote renewable security system" [i.46] provides abstract advice relating to secure software updates by security vendors.

5.7 Open IPTV Forum (OIPF)

In March 2007, network operators, service providers, manufacturers of terminal equipment and platform operators as well as content providers merged to form the "Open IPTV Forum". This initiative, now merged into the Hybrid Broadcast-Broadband TV Association, is aimed at developing open standards for a complete end-to-end systems approach for IPTV based upon existing technologies and specifications. The security solution specified initially by OIPF was Marlin, a specification developed by an industry consortium of companies. The scope of OIPF covers distribution of services via closed, managed networks and via the open Internet. Special precautions are taken by the network operator in the case of closed, managed networks to ensure the technical quality of transmission. This is not consistently possible for services via the Internet. The first set of specifications (Release 1) was adopted in early 2009. This includes part specifications of audio/video formats, content metadata, protocols for various network interfaces, middleware for interactive applications, and security of services and content (CA/DRM).

In a later development, support for CI+ content protection was added.

The Forum has defined two different approaches for the security of services and content:

- the "terminal-centric" approach defines a complete end-to-end solution based on the Marlin Broadband (BB) specification; and
- the "gateway-centric" approach defines a gateway function in the home network that terminates any network-based CA/DRM solutions and implements them into a standardized solution. This standardized solution can be based on DTCP-IP or CI + when external to the terminal, or embedded in the terminal.

The current specifications are available at the following link: http://www.oipf.tv/.

The Forum currently defines profiles for various applications of the specifications. Implementation should only be based on these profiles. Commercial deployments based on the end to end system have not been reported so far although parts of the specification are referenced by other specifications such as HbbTV®.

5.8 HbbTV®

The HbbTV® initiative started in 2008 with activities in France and Germany to define how a web browser in a TV set could be used to add value to broadcast television and enable services linking broadcast and broadband content delivery. The specification is an integration of selected elements from DVB and from the Open IPTV Forum. The first specification was finalized at the end of 2009 and published by ETSI as ETSI TS 102 796 [i.7] (V1.1.1) in June 2010. First implementations appeared in TV sets in 2010 with widespread introduction in products in 2011. Content protection was outside the scope of this version of the HbbTV® specification except that:

i) there is a standardized mechanism by which an HTML page can communicate with any content protection solution that may have been included in a terminal;

ii) a mapping of that mechanism to the CI+ specification is included; and

iii) for broadband delivered content, a definition is provided for the signalling of the type of content protection used.

The specification was revised during 2011/12 to add support for delivering video via broadband using MPEG DASH with the resulting specification published by ETSI as ETSI TS 102 796 [i.7] (V1.2.1) in November 2012. This adds MPEG common encryption [i.14] as an option and defines how that option can be used. Deployments of the HbbTV® specification have selected content protection solutions. The first such selection was for the French retail DVB-T specification (TNT2). An agreement was reached between broadcasters and manufacturers that broadcasters would support at least two DRM systems and manufacturers would support at least one of these two. Both constituencies are free to support other solutions as well. Other HbbTV® deployments for retail markets are following the French selection or have indicated the intent to do so.

CORAL

CORAL is a cross-industry consortium with the aim of providing interoperability between different DRM systems in terminal equipment. A general infrastructure framework (DRM-Bridge) for content and service providers and manufacturers of terminal equipment will be defined for this. It can be used with different DRM techniques and is thus independent of the DRM technology used in each case. CORAL does not specify its own DRM technology, however. CORAL relies on the concept of service-oriented architecture by defining trusted and secure services and interfaces via which all necessary information can then be exchanged. Establishing and ensuring the reliability of services and terminal equipment is thus a major challenge The rights themselves are not replaced, but references of DRM-information are exchanged with the aid of tokens independently of the particular DRM system.

This is achieved by assigning each terminal equipment a unique and certified ID. The certification is tied to roles within the CORAL frame. Based on this framework, interoperability between WM DRM 10, OMA, Marlin and even conditional access systems (CAS) can be provided.

The downside of using Coral for television is that the consumer is required to re-download the whole content item in the new format, which can be time consuming and costly to the network.

Coral has not been deployed.

5.9 Digital Living Network Alliance (DLNA®)

DLNA® aims at the interoperable networking of terminal equipment and PCs for stationary, portable and mobile use. Networking is mainly based on UPnP [universal plug and play]. DLNA®'s area of study is limited to communication between devices within a home network. They do not define any means of delivery to the home.

DLNA® has published two sets of guidelines that are related to content protection:

Link Protection guidelines [i.30] that aim at protecting content while it is delivered to another device for viewing purposes. These guidelines do not address content copying or moving functions. Implementing these guidelines is optional. When implemented, one technology is mandatory, DTCP-IP and one is optional, WMDRM-ND. There exist some commercial deployments of devices implementing these guidelines.

DRM Interoperability Solution (DIS) guidelines [i.30] that aim at permitting the secure transfer of content between home devices that implement different DRM solutions. Implementing these guidelines is optional. When implemented, two solutions are available: DTCP-IP (including content copy and move) and Coral. In practice, these guidelines have not been widely implemented in the marketplace.

5.10 ATIS (Alliance for Telecommunications Industry Solutions)

ATIS is an association of telecommunications operators and equipment suppliers in the U.S. ATIS founded the IPTV Interoperability Forum (IIF) back in July 2005 to formulate a framework and requirements as a basis for further specification and standardization of IPTV, especially on Digital Rights Management (DRM) and Quality of Service (QoS).

In addition to a number of other specifications to IPTV, the following have been published by ATIS [i.31], which deal specifically with DRM and security issues:

- IPTV DRM Interoperability Requirements ATIS-0800001.v003 [i.50].
- IIF Default Scrambling Algorithm (IDSA) Interoperability Specification ATIS-0800006.v002 [i.51].
- Secure Download Interoperability Specification.
- Application Level Interfaces (API) Interoperability Specification.
- Consumer Domain Attachment and Initialization Specification.
- Remote Management of Devices in the Consumer Domain.
- IPTV Digital Rights Management (DRM) Requirements Update.
- Certificate Trust Management Hierarchy.

- Standard Public Key Infrastructure (PKI) Certificate Format.
- Security Robustness Rules.
- Distribution of Content in the Subscriber's Authorized Service Domain.

These and all other ATIS specifications can be downloaded at www.atis.org.

No examples of ATIS deployments could be located and it is understood that all ATIS activities in the IIF group have closed down.

5.11 IETF (Internet Engineering Task Force)

The Internet is a "loosely" organized international collaboration of autonomous, interconnected networks. The IETF is the organization responsible for the technical development of the Internet. The IETF is an open, global association of network operators, manufacturers of terminal equipment, researchers, network experts and users. The standardization process within the IETF is organized in a variety of working groups and is managed by the Internet Architecture Board (IAB) and Internet Engineering Steering Group (IESG).

The IETF does not have a specific IPTV working group, but a variety of specifications on individual aspects of transmission, as well as on IPTV rights management, were developed as part of its activities. Almost all the other organizations mentioned in this clause have entered into liaison statements with the IETF and/or reference to the underlying specifications of the IETF. Some of the specifications dealing with the rights management for IPTV are:

- Framework and Requirements for an Access Node Control Mechanism in Broadband Multi-Service Networks (Internet-Draft, Mai 2008).
- Access Right Distribution Protocol (ARDP) (Internet-Draft, August 2007).
- Requirement of service provider for the Data Broadcasting Service over the internet protocol television.
- Security Preconditions for Session Description Protocol (SDP) Media Streams RFC 5027 [i.8].
- Multicast Security (MSEC) Group Key Management Architecture RFC 4046 [i.9], April 2005.
- MIKEY: Multimedia Internet KEYing RFC 3830 [i.10], August 2004.
- The Key ID Information Type for the General Extension Payload in Multimedia Internet KEYing (MIKEY).
- Multimedia Internet KEYing (MIKEY) General Extension Payload for Open Mobile Alliance BCAST LTKM/STKM Transport RFC 4909 [i.11], June 2007.
- GSAKMP: Group Secure Association Key Management Protocol RFC 4535 [i.12], June 2006.
- AAA and Admission Control Framework for Multicasting (July 1, 2008).
- MLDv2 User Authentication Problem Statement draft-liu-mboned-mldauth-ps-00.
- Real Time Streaming Protocol 2.0 (RTSP) (Internet draft, May 5, 2008).

All IETF specifications can be downloaded at www.ietf.org.

5.12 W3C

The W3C launched a "Web and TV Interest Group" in February 2011 to identify requirements and potential solutions to ensure that Web and TV services interact well. The membership included TV manufacturers, cable and satellite providers and online video distributors. The interest group has established liaisons with multiple W3C working groups, most notably the HTML working group.

In 2011 the interest group provided the HTML working group a set of requirements for commercial media support in HTML5. Two specifications address these requirements - the Encrypted Media Extensions [i.32] and the Media Source Extensions [i.33].

The Encrypted Media Extensions (EME) extend the HTMLMediaElement (video tag, audio tag) to define a common API that can be used to discover, select and interact with a DRM system. EME leaves it unspecified whether the DRM system accessed through the API is within the browser or in the platform. Based on the activities of involved industry fora, most applications will use EME in combination with the new ISO MPEG Common Encryption specification, while most browsers will implement an interface to a platform DRM.

The EME specification was published by the HTML Working Group as a Working Draft in February 2014.

The Media Source Extensions (MSE) extend the HTMLMediaElement to allow JavaScript to generate media streams for playback. Similar to the Encrypted Media Extensions, there appears to be strong industry interest in using MSE in conjunction with the ISO MPEG Dynamic Adaptive Streaming over HTTP (DASH) specification. The MSE specification was published by the HTML Working Group as a Candidate Recommendation in January 2014.

Together, EME and MSE are specifications intended to meet the requirements of the W3C Web and TV Interest Group, enabling both live and on-demand, DRM-protected commercial media delivery to standards-based browsers and other HTML5 application frameworks, and are designed to work with the new MPEG DASH and Common Encryption specifications.

5.13 Open Mobile Alliance (OMA)

The Open Mobile Alliance (OMA) is an association of service and product providers from the entire value chain of the mobile sector and adjacent industries. It aims at developing so-called "enablers" for market-ready, interoperable digital services, establishing them as global standards and thus ensuring the global interoperability of terminal equipment, software and content.

As part of the OMA work a toolbox of different techniques to support mobile broadcast service (OMA BCAST) was defined.

Mobile Broadcast Services Enabler [i.34] defines a technological framework and specifies globally interoperable technologies for the generation, management and distribution of mobile broadcast services over different BCAST distribution systems, (3GPP/MBMS, 3GPP2/BCMCS, DVB-H, DVB-SH, FLO, WiMAX, DVB-T2 and DVB-NGH). It also defines the procedures and parameters for securing services and content.

The common feature of all methods is a transport encryption on or above IP level, service-specific key management. Like DVB-SPP, transport encryption favours open standard procedures such as IPSec and SRTP of the IETF and the disclosed ISMACryp method. IP packets (IPSec) to be RTP packets (SRTP) or codec-specific data packets (ISMACryp) are encrypted. The last version of BCAST (BCAST1.3) adds the support of MPEG-DASH-based contents and the support of MPEG CENC encryption for these contents. The common basis of all encryption methods is the AES algorithm.

Two variants have been specified for key management.

- OMA BCAST DRM Profile [i.35]:
  - The OMA BCAST DRM profile is based on OMA DRM 2.0 for key management. As a central element for the authentication of the terminal equipment, the method relies on Public Key Infrastructure (PKI), where only the terminal equipment itself is authenticated. This authentication is not transferable, as in the case of a SIM card, to other terminal equipment. A smart card is not mandatory; a variant of the method also works on one-way broadcast channels.
- OMA BCAST SmartCard Profile [i.36]:
  - The OMA BCAST smartcard profile is based on a key management specified in 3GPP for MBMS (Multimedia Broadcast & Multicast Services) and securely implemented in the smartcard (USIM/(R)UIM) connected to the mobile phone. As such, it generally requires a return channel.

5.14 3rd Generation Partnership Project (3GPP)

The 3rd Generation Partnership Project (3GPP) unites six telecommunications standard development organizations from Europe USA and Asia (ARIB, ATIS, CCSA, ETSI, TTA, TTC). 3GPP covers cellular telecommunications network technologies.

3GPP has specified the multimedia broadcast and multicast service (MBMS) application independent transport service [i.38]. MBMS user services are based on broadcast or multicast services, and are bearer agnostic to enable access via generic IP access systems. It is used on UMTS and eUMTS (LTE) networks.

MBMS introduces the concept of a point-to-multipoint service into a 3GPP system. A MBMS User Service is able to securely transmit data to a given set of users. In order to achieve this, a method of authentication, key distribution and data protection for a MBMS User Service has been defined by 3GPP and is called MBMS security [i.39].

MBMS security is used to protect RTP sessions and FLUTE channels. As such MBMS User Service protection is Transport Service independent, in particular, it is independent on whether it is carried over point-to-point bearer or MBMS bearer.

The method of authentication is based on HTTP Digest and GBA (Generic Bootstrap Architecture) defined by 3GPP for establishment of keys between the server and the mobile/USIM.

The key distribution (Service Keys (MSK) and traffic keys (MTK)) is based on MIKEY defined by IETF [i.37].

5.15 ISO MPEG

On April 2012, ISO/IEC published the 1st edition of MPEG's Dynamic Adaptive Streaming over HTTP (MPEG-DASH) as ISO/IEC 23009-1 [i.15]. ISO MPEG-DASH supports both ISO Base Media File Format (ISO BMFF) and MPEG2 Transport Streams (M2TS). MPEG-DASH is being broadly adopted by consortia and industry for over the top delivery.

ISO also published Amendment 3 to the ISO Based Media File Format (ISO/IEC 14496-12 [i.13] AMD3) and Common Encryption for ISO base media file format files, ISO/IEC 23001-7 [i.14]. MPEG-DASH employed the above specifications to support multiple DRM interoperability for streaming services. ISO is in process of publishing the 2nd editions of MPEG-DASH (ISO/IEC 23009-1 [i.15]) and Common Encryption (ISO/IEC 23001-7 [i.14]). The 2nd editions enhance and extend these specifications features, including key rotation and additional encryption schemes.

Multiple industry fora referenced these new ISO standards as the basis for protected over the top video streaming specifications. The Digital Television Group (DTG) in the UK, the HD Forum in France, Hybrid Broadcast Broadband TV (HbbTV®) in Europe, the Digital Entertainment Content Ecosystem (DECE) and Digital Living Network Alliance (DLNA®), all adopted DASH and Common Encryption in their specifications, for both streaming and downloading protected content, supporting multiple DRM interoperability.

5.16 DECE and ULTRAVIOLET™

UltraViolet™ is an industry developed solution for downloadable video content, intended to bring the flexibility to downloaded content that consumers have today with optical disks such as DVD.

UltraViolet™ was developed by the Digital Entertainment Content Ecosystem (DECE) organization. UltraViolet™ provides for "DRM interoperability" by defining a Common File Format (CFF) [i.40] using the relevant ISO MPEG standards to provide content interoperability using devices running different DRM systems.

DECE has not selected a single DRM for enabling interoperability, but supports many, and the list is continuing to increase. Any device manufacturer implements the DRM of its choice from the list, there is no need to implement multiple DRMs in a single device. Once a device receives content and wants to display it, it connects to the user right locker and requests the license for this content according to the DRM used by this device. If the user now uses another device with another DRM, this second device asks the DECE right locker to send the licence for this other DRM. With this approach, the DECE central right locker enables the secure storing of all content purchased by a user and enable access to its content library from any place and any device using any supported DRM. Content can be either downloaded or streamed on any device the user may use either at home or on the move.

The content can be stored anywhere in the cloud or provided by any retailer, the right to access it is managed by the DECE central right locker. Once the user has the licence, there is no need to be connected further to consume the downloaded content.

Thanks to this approach and the common encryption and file format, DECE facilitates the access to any content on all registered devices with DECE compliant DRMs, without being concerned about the DRM used by the end-user device. The approach enables full interoperability without the need to either download any DRM or support multi-DRM, and also greatly facilitates the user's ability to exploit purchased rights effectively for life by having a single place where all content purchased are registered and made widely accessible.

A list of approved DRMs can be found at appendix C from the System Specification document, presently version "System—2.0r1" accessible at the following URL http://www.uvcentral.com/frontpage.

5.17 US DCAS

An attempt to define a Downloadable Conditional Access System (DCAS) solution was proposed several years ago in the US by CableLabs, supported by major US MSOs. This was an attempt to create an alternative to the CableCARD solution for "separable security", a requirement set by the FCC in its Telecommunications Act 1996 in order to encourage competition through a retail market for terminal equipment. Under the proposal, the MSOs set up a consortium (Polycipher) which designed a common architecture in the form of a software stack and dedicated ASIC created by a specially commissioned chip design company (Embedics). All participating CAS providers would have to rely on the same architecture to integrate their security and all manufacturers would have to implement the defined software and hardware. CableLabs was proposed as the entity responsible for testing products and implementations for conformance thereby having trust responsibilities for the host. However there was no entity established to take full liability.

After several years of work and large investment, the whole project failed because of disagreements between different sectors of industry about the specification, roles, responsibilities and liabilities. In the meantime, the CableCARD mandate has achieved just 616 000 devices as against over 47 million operator supplied devices. In 2014 the US House of Representatives voted to end the requirement for cable operators to support separable security.

In later developments, Comcast and TiVo have recently announced that they are working on a two-way non-CableCard security solution (refer to http://www.fiercecable.com/node/70746/print). Earlier, two other US cable operators, Cablevision from 2011 and Charter from 2012, had decided to establish downloadable security system. These are individual proprietary initiatives and bear no technical relation to the DCAS project.

5.18 GlobalPlatform®

GlobalPlatform® is a cross industry, non-profit association which identifies, develops and publishes specifications that promote the secure and interoperable deployment and management of multiple applications on secure chip technology. GlobalPlatform®'s objective is to create a standardized infrastructure that accelerates the deployment of secure applications and their associated assets, such as data and cryptographic keys, while protecting them from physical or software attacks.

It achieves this by publishing and advancing specifications which address:

- the implementation and management of tamper-resistant chips - such as smart cards and other SEs (Secure Elements);
- the TEE (Trusted Execution Environment) which ensures that sensitive data is stored, processed and protected in a trusted environment; and
- the messaging that enables service providers to connect their backend systems to the SE, TEE and any other actor within a secure application's ecosystem.

GlobalPlatform® specifications have been largely deploying in the banking sector for years, and GlobalPlatform® is now extending the scope to other markets as transportation, government, Internet-Of-Things and media content management and protection.

GlobalPlatform® established the Premium Content Task Force in 2012 in response to the growing consumption of premium content on mobile devices and requirement for the content to be hosted in a protected and secure environment. The intention of the taskforce is to address the requirements of premium content providers to protect their services on smart connected devices such as smartphones and tablets, to identify the key business and use cases in this market segment and to work with the relevant technical committees to ensure that GlobalPlatform® specifications can be enhanced to provide compelling solutions to the market. Content management and protection on devices is identified by GlobalPlatform® as a key driver for TEE adoption.

The CA/DRM applications are identified as downloadable trusted applications in this environment that could rely on specific API to the TEE and a protection profile to ensure an end-to-end security to the premium content when consumed.

A first requirement document addressing the trusted video playback platform has been issued by the group for implementation of a specific API in the TEE specifications, and another requirement document is in preparation enhancing furthermore the trusted media platform with watermarking and other functionalities.

The technical specification of the TEE including support of these requirements should be publicly available in the beginning of 2015 year.

6 Implementation and operation of CA/DRM systems

6.1 Introduction

This clause considers the factors that operators, content rights owners and other stakeholders in the provision of services should take into account of in making and keeping the security of their delivery systems at the level necessary to safeguard their business.

6.2 Effective implementation of systems

When designing and developing a CA/DRM solution, it is crucial to ensure that the solution be as effective as possible, i.e. is able to protect the content while maintaining good user experience. The goal of a CA/DRM system is to protect the encryption key, manage user and content rights, and deal with output controls.

This clause lists important practices that can be followed in order to build a more secure system.

The terminology "CA/DRM agent" is used to designate a piece of software and/or hardware that is part of the client environment and which is responsible for the CA/DRM enforcement of security.

Personalization

The CA/DRM agent requires an identification and a key. The personalization of the agent allows fine-grained identification of the device it operates within, and consequently of the customer. It is important to be able to identify uniquely one specific agent running into one device belonging to one customer associated with specific commercial rights.

This unique identification is the root of trust. A hardware based root of trust can be:

- an ID burnt into the agent at manufacturing phase; or
- an ID built from hardware unique IDs when the agent is purely software and downloaded into the device (e.g. a tablet). For example, it can be using a combination of unique id from the device (e.g. serial number).

Protection

The CA/DRM agent has to be protected at rest and in use.

When at rest, a CA/DRM agent is better stored encrypted in the device. This is to ensure that reverse engineering will not be possible directly. When it needs to be run, it will be authenticated, integrity-checked and decrypted.

When the CA/DRM agent runs (completely or a part of it) in software within the main chipset, there are specific tools that are used to ensure its safety. Safety here means that the running agent will not be successfully attacked while running. Some examples:

- obfuscation: The programming code of the agent is changed (without changing the final behaviour) in order to make it unreadable. This is to counter tools for reverse engineering that are able to read machine code;
- anti-debug/anti-dump: With such defense, the agent code can detect that it is being debugged and can stop; and
- key storage: Decryption keys are stored in the memory when the agent is running. They need to be irretrievable (e.g. split in parts, moving around, etc.).

Isolation

The CA/DRM agent is a piece of software running within an environment. As such, it shares resources with other programs, and more importantly the resources it uses (e.g. RAM) can be accessed.

This is why the agent tries to be isolated from the rest of the device. There are several levels of isolation that can be envisioned, depending on the capability of the platform. From the least to the most secure:

1) Mainstream OS. No specific isolation is available, the agent shares everything with the other processes within the OS. Its resources are easily readable;

2) Virtual Machine in an open OS. This isolation is purely software based;

3) Security Hypervisor (Virtual CPU). The agent process is separated from the other ones with specific resources;

4) Trusted Execution Environment. Isolation becomes hardware-based but sharing the chipset; or

NOTE: Up to now, the agent is not protected against hardware attacks (DPA, etc.).

5) Dedicated hardware secure element. The hardware is physically separated from the main chipset. A component of the agent runs in the main chipset to ensure communication with the hardware secure element.

Renewal and Diversification

Secure renewal allows CA/DRM agent replacement (parts of it or the whole agent). It can be done by applying patches or by upgrading the complete firmware. When using a hardware removable piece (for example a smartcard), it means replacing it.

Diversification allows not using the same agent models, codes, behaviour for all clients. The target is to segment/partition the population of clients.

These two concepts are means to counter breaches in the CA/DRM system. Diversification limits the spread of the breach, giving time for renewal to cure it.

Output Protection

This has to deal with commercial rights associated with the content. CA/DRM is used to securely transmit the rights information to the device. Protected content is encrypted to ensure safe delivery up to the customer device. There it is decrypted such that it is available in clear. Such clear content will still be protected so that it is not sent insecurely to external devices nor to insecure components of the customer device.

When building a complete CA/DRM protected solution, output control is used to ensure that clear content:

- does not leave the secure video path inside the device; and
- leaves the device by using approved only communication channels (e.g. HDCP).

6.3 Anti-hacking and counter piracy activities

Operators have to be vigilant to the possibility of hackers attacking their security systems. A successful hack can give rise to several adverse outcomes. For example, existing customers may cancel legitimate accounts and deploy hacked methods to access content instead, resulting in a loss of revenue. Potential customers may adopt the hacked method, resulting in a lack of new revenue. Falling market confidence in the service and the operator will surely follow.

Operators therefore have to ensure that they are looking for evidence of hacking activities, ideally before they have any impact; and they have to have the ability to securely upgrade applications or devices before hacking harms their business.

The kinds of surveillance likely to be carried out by or for an operator include internet trawling for evidence of blog posts or other website entries pertaining to, for example, individual hackers and pirated software versions. Internet trawling can be carried out from more or less any territory. There is also the possibility of locating physical evidence of hacking through website shops, market stalls and other local "black market" suppliers and through signs of attempts to penetrate networks.

The vigilant operator should be mitigating these threats by adopting prudent measures to ensure that they detect evidence early and are able to react effectively. For a reaction to be effective, it will be targeted at the most appropriate level to overcome the hack. Measures can range from a simple change of keys up to a complete security system change - operators have to be prepared for any eventuality in order to preserve their business and this means being ready for a worst-case scenario.

Countermeasures are usually prepared by the security provider to the operator. The best prepared security vendors and operators will ensure that it is always possible to completely replace a security system in a relatively short space of time, months rather than years. To be at this level of preparedness, it is necessary to have assured, trusted access to the devices that need to be updated and to have a replacement security system ready to deploy.

7 Interoperability in practice

7.1 Introduction

This clause examines use cases for interoperability in terms of the same protected content being received on devices with different CA/DRM solutions and the interchangeability of the CA/DRM solutions themselves.

7.2 Interoperability when several CA/DRM solutions are simultaneously used

The following use cases are typical of those given as example of cases not covered by existing standards:

- Receive content from multiple, managed networks (satellite, cable, terrestrial, Internet) using a single device. This is firstly related to the network interfaces of the device as decided by the manufacturer or the operator for a given market. A growing number of television receivers are "Smart TVs" equipped with triple tuners and internet connectivity and have a typical lifespan of 5 to 7 years which means they can be used on different networks, subject to operating system compatibility. Many set top terminal devices are equipped with Ethernet connectivity but only one tuner which means that they will only work on one type of broadcast network. The life span of a set top terminal device is typically 3 years (see http://www.slideshare.net/AminoTV/2012-0322-iptv-wf) according to recent research although some businesses aim to extend the life to 5 years. In this use case it is common that different CA/DRM solutions are used by different operators. Moreover, the operating system and middleware, which are often utilized to provide the USP - unique selling point of an operator - are very likely to be incompatible due to differing business requirements and delivery protocols of operators. Television receivers usually operate under a different business model with a longer lifespan but without an operator specified CA/DRM system. Users wanting to access pay TV content can attach a CI Plus module with viewing card if the service provider supports that option. If the user wants to access more than one pay TV network, it may be necessary to have more than one CI Plus module or a multi-CA module.

- Receive content from one operator using a set top terminal device from a different operator over the same or a similar network, for example when people move or simply want to change to an alternative operator while keeping their retailed set top terminal device. In such a case it is likely that the CA/DRM differs from one operator to the other.

- Receive all channels on a set top terminal device equipped for one network operator, including those primarily broadcast on another operator's network. This can be achieved through B2B agreements between the operator of the original network and the one of the alternative network so that the re-broadcasting may occur. In this case the CA/DRM used on the primary network might differ from the one in use on the second network.

- Receive foreign channels. This is a similar example to that of receiving channels from other operators in that it is a business decision to select the channels distributed. Operators acquire the rights for content for a specific territory because it suits their chosen business model which may rely on expertise for a particular market, and reception outside the designated territory is therefore not allowed contractually by the content owner unless specific rights are also acquired for that additional territory. As in other use cases, the CA/DRM system used on the primary network might differ from the one in use on the second network. Or

- Receive hybrid services unrelated to broadcast. On hybrid devices users have the opportunity to access OTT content distributed over the internet besides services offered by the network operator. The availability of services to users depends on service providers making their services available using the DRM system implemented in the user's device.

From a CA/DRM perspective, all the above use cases can be addressed, providing there is a business relationship between service providers, using DVB Simulcrypt and DVB CSA/CISSA for a CA protected content or DECE and MPEG Common Encryption for DRM protected content. DVB Simulcrypt actually enables each network to keep using their existing CA/DRM solutions while requiring each terminal to implement only one CA/DRM, since the terminal will always obtain ECMs or DRM licenses for the CA/DRM it implements. Simulcrypt has been widely and successfully used for many years over satellite networks where some channels are broadcast only once across multiple European countries and received in a large number of networks with various CA/DRM. The use of DVB Simulcrypt avoids having to implement at the manufacturing stage several CA/DRM solutions and the consequent increase in device cost. It has however to be noted that Simulcrypt may pose a risk to the overall security which is set by the weakest CA/DRM solution that is a part of the ecosystem. Should one of these CA/DRM solutions be successfully attacked, all networks and set top device terminals implementing other CA/DRM solutions are compromised. Security can however be recovered by ceasing the Simulcrypt link to the compromised CA/DRM. Some operators consider that DVB Simulcrypt is an excellent solution for migration from one CA/DRM solution to another (e.g. next generation solution of a CA/DRM vendor).

An alternative to Simulcrypt is CI Plus. The current version 1.3 is only applicable to transport stream signals and allows support for additional CA/DRM systems in addition to those natively supported in the set top device terminal. Many terminals currently implement a CI Plus interface. Making use of the CI Plus facility comes often at the cost of the CI Plus module. The module price at retail is often seen as high when compared with a complete set top terminal device with embedded security, however there are sometimes subsidies available from operators to reduce the cost to the end user and work is underway within DVB to specify a version with a new, more common form factor. Users wanting access to multiple service providers may need to have more than one module.

As shown by the above examples, interoperable solutions for CA/DRM exist and are deployed where there is the business justification for deploying them. The technologies mentioned in this clause have been shown to provide an appropriate balance between standardized security elements and components while leaving operators free to uniquely service their chosen business proposition.

7.3 Interchanging security systems

7.3.1 Current architecture

Another typically quoted use case is to enable operators to switch easily from one CA/DRM vendor to another. In current deployments, the CA/DRM is implemented during manufacturing process in the terminal device and this implementation is often based on dedicated, secure hardware elements specified by the CA/DRM vendor. One typical example is the device secure boot process. The first step of the secure boot generally requires the verification of the signature of a part of the booting software. This is done using a public key which cannot be changed, as a safeguard against tampering. If this public key belongs to the CA/DRM provider, this makes operations far more complex after a CA/DRM switching unless the operator can gain access to it. Many operators assume ownership of the public-private key pair to overcome this issue.

The following clauses analyze possible solutions to facilitate CA/DRM switching.

7.3.2 CA/DRM Switching in deployed terminals

There are two different cases:

- CA/DRM switching can be done with the intent to fully replace the software and relevant middleware code used by such operator controlled devices in order to use a different CA/DRM/middleware combination. This process has already occurred in several instances where existing set top terminal devices of an operator have been updated to another CA/DRM system without requiring a physical change to the devices, although there remains a dependence on the capabilities and robustness of the underlying hardware to work securely with the software components. This is achieved through use of the key/certificates and other security means to authorize such a change and it is managed through business contracts between the involved parties under control of the operator. Such a process is contractually secured and tightly managed between the security vendor(s) and the operator. In addition since the lifetime of a set top terminal device is typically 3 to 5 years, the operator is incentivized to contract with the security vendor and the manufacturer (who provides support for drivers) the ability to update/upgrade/maintain the device over its life.

- For retailed set top terminal devices with embedded CA/DRM systems, the current situation is that a CA/DRM system change is controlled by the manufacturer. As the manufacturer of the device and the "owner" of the keys and certificates needed to update the device, the manufacturer has responsibility for the behaviour of the device and the user may claim against the manufacturer if the device is not performing the function it was designed for. Hence if it proves necessary to update a retailed device, neither the security vendor nor the operator can do this without the full agreement and authorization of the manufacturer. On the other hand, the manufacturer alone is not able to change the CA/DRM system in a device which is linked to a particular network without authorization and support of the operator and both CA/DRM vendors.

In summary, it is currently always the entity that owns the set top terminal device's update keys and certificates who will take responsibility for fundamental changes. For the time being, no dilution or distribution of this ownership is possible without risking a loss of control and integrity of set top terminal devices with a consequent potential for damaging uncertainty in the service the devices offer to the end users. An activity within ETSI ISG ECI (refer to clause 5.4) plans to describe a circle of trust reaching from chip vendors to service providers which aims at facilitating the exchange of CA/DRM systems in comparison to the actual processes described above.

7.3.3 CI Plus solution

CI Plus is a suitable candidate for this CA/DRM system switching scenario in the case of fixed devices in a broadcast environment. Indeed, CI Plus allows any proprietary CA/DRM vendor(s) to support their security solution(s) in a CI Plus module provided that a related contract with the CI Plus LLP Trust Authority has been signed. Set top terminal or TV device manufacturers need to implement the general CI Plus specification and to sign the CI Plus device interim licence agreement. When a consumer wants to switch, it is sufficient to change the CI Plus module to go from one CA/DRM to another.

The European regulation concerning the broadcast environment mandates a CI (Common Interface) which is fulfilled by the Cenelec Common Interface in the past (EN 50221 [i.47]). CI Plus can be seen as a successor to the Cenelec CI interface in all TV receivers of over 30 cm display size. Many set top terminal devices have one or more CI/CI Plus interface slots.

The CI/CI Plus approach has the following pros and cons:

- it allows a full separation between the CA/DRM technology and the receiver;

- when the CI/CI Plus module is used directly in the TV it does not require an additional set-top terminal, nor a specific remote control, nor a separate power supply nor any connection cables. There is a caveat however in that the particular business model of a platform may not be fully supported in a retailed set top terminal device or TV receiver that supports CI Plus;

- CI/CI Plus modules allow the same content distribution security level as an operator specific set top terminal device;

- the current form factor of the module is now considered rather large but it will be reduced in future versions;

- in the same way as for set top terminal devices, support for one or more CA/DRM systems can be integrated into a CI Plus module depending on the market needs, but currently there is no evident demand; and

- the current deployed version 1.3 is applicable to fixed devices in a broadcast environment, later devices will address IP delivery.

However some stakeholders see a major drawback of CI Plus in the retail cost of the CI Plus modules. It is often set at a similar level to a complete set top terminal device due to scale issues. Where the operator subsidizes the module, changing the population of deployed CI Plus modules is a very significant cost although one which would only need to be incurred when a particular module had been compromised or a change to the security system was being carried out. A new version of CI Plus currently being worked on within DVB is intended to fit the latest market requirements.

7.3.4 Software download solutions

Another obvious candidate for the CA/DRM switching problem is the use of software download to replace a given CA/DRM with a new one. The concept is generally based on the definition of a standardized container for a secure execution environment within which each CA/DRM system could be downloaded as software and executed, based on customer initiation.

In principle, this solution may be appealing to various interested parties in and around industry as it seems to be simple, cost-effective, ecologically desirable and potentially sustainable in the long-term. Regarding such an approach to security, the following should be carefully considered:

- The interoperability achieved through such a standardized approach may pose a challenge to innovation and evolution if the specification does not achieve a balance between interoperability, security and scope for further novelty. Patches cannot be applied to standardized elements, for example as countermeasures to a security breach, without a change in the standard.

- For any CA/DRM system implementation, a security robustness and compliance certification is used to allow a CA/DRM provider to take liability and accountability and to allow a response to a security breach. In the case of a standard downloadable container for CA/DRM, the certification and compliance role will be necessary similar to the CI Plus Trust and Certificate Management. As the CA/DRM system would be operating within an environment secured by another trust authority, the liabilities in the case of a security breach may be unclear. And

- Implementing downloadable technology will introduce additional costs into terminal equipment whether or not a user ever makes a CA/DRM swap. Swapping a CA/DRM will also generate cost. These costs also apply in the case of CI Plus.

Some industry stakeholders from all parts of the digital TV value chain are working on swappable CA/DRM solutions because they claim that although the development of an eco-system of a swappable CA/DRM solution is a huge challenge, the advantages of interoperability will compensate for the efforts to develop and establish such a solution.

This approach also raises some software maintenance issues:

- in the case of a vertical market where the operator controls the set top terminal device, and has specified it, the useful lifetime of such device is typically 3 to 5 years and the operator will secure with the CA/middleware vendor and manufacturer the ability to update/upgrade/maintain the device over this period or longer; and

- in the case of a horizontal or retail market the involvement of a trust authority and well defined work-flows and mechanisms for software maintenance including contractual obligations outside the traditional manufacturer - user liability relationship have to be established that do not currently exist.

NOTE: Some TV device manufacturers have established their own portals within the TV devices they market incorporating DRM solutions for paid TV content delivered through broadband connections. In this case the TV manufacturer takes responsibility and liability for the portal and installed security solution, along with necessary updates and renewals, in the manner of a Pay TV operator in a vertical market.

8 New market needs

8.1 Introduction

This clause provides examples of new services and delivery options that may soon arrive or have recently arrived in the market.

8.2 UHDTV

It is still early days in terms of the provisioning of UHD (initially 4K) content. However - thanks to work by the MovieLabs group [i.48] an important stakeholder funded by the 6 major US based studios, produced a specification for enhanced content protection from which a basic set of needs have become clear. Fundamentally these are:

- The device is secure in itself and does not rely on other components in a wider security infrastructure or return communications channels.
- The software being executed remains unchanged without permission and certain key content protection elements (such as watermarking) continue even if the device has been compromised.
- The latest encryption technology protects the content using long key lengths, and is protected against side channel and other "short cut" type attacks.
- Content is encrypted in such a way that knowing the key that decrypts one piece of content does not lead to other instances being decipherable. Similarly, a successful hack to one type of device does not compromise other devices.
- Content is protected via on-screen watermarking.
- Support for revocation and renewal is available at the client, code and device levels.
- HDCP 2.2 and higher versions may carry UHDTV content, it is possible to disable other output interfaces.
- A secure media pipeline is implemented along with secure memory, application and processing environments.
- A random number generator is available.
- It is possible to bind the content to the device and to restrict copy and move functions.

NOTE: The needs expressed above are based on the information from the Movielabs document but readers of the present document are strongly recommended to rely on their own investigations and analysis to determine what individual content rights owners want for specific implementations.

8.3 Companion screen

The Companion (or "second") screen market is typically defined as being video services made available to mobile tablets and mobile phones using one of the three market leading, proprietary operating systems.

The list of needs below could be considered a base-line in order to provide support for HD services on mobile devices. It provides sufficient security to allow a business to manage cloning, device revocation, and to build processes around device concurrency and user session management.

Internal Security

Devices should be provisioned with a unique identifier in hardware that is, therefore, immutable and also made available through approved APIs.

The device should support a secure boot process that validates the integrity of the run-time image before executing it.

The device should provide a secure video pipeline. Specifically - the area of memory used to decrypt and decode video should not be accessible to other processes.

The device should have one or more keys provisioned in the SoC that are then used to allow indirect use (i.e. the keys are never exposed in code - just referenced) and used to provide a secure key store.

Output Security

The device (and its operating system) should ensure that, if required, video is not shared through wired or wireless output ports.

Upgradeability

The device is capable of being updated and this process ensures the update file is valid (trusted) and cannot be tampered with. Other DRM related security elements (e.g. keys) are capable of being updated from a trusted source, without modification as and when needed.

Interoperability

The existence of a common security platform would help content providers to avoid needing to write bespoke code to meet some or all of the above requirements.

9 Lessons from main body clauses 4 - 8

Clause 4 addresses the general features of CA/DRM security systems and notes that Trust Authorities are necessary for security system implementation but not sufficient on their own. Designs should allow for more than one trust authority but in practice, the complexity of supporting more than one trust authority in the market limits the number to just one per security system.

Clause 5 summarizes the work of a large number of industry collaborations producing specifications and standards with relevance to security. For pay TV market in Europe, DVB has provided a range of security standards which facilitate interoperability very successfully. Examples of these are:

a) the CSA suite, the third of which is now entering the market in silicon ready for implementation through suitable business models;

b) Simulcrypt, which has been deployed from time to time to suit particular business requirements; and

c) CI Plus, recently taken back into DVB and upgraded for IP streaming, it is now being developed to work over a faster physical interface that is more suited to the current market requirements.

DVB standards are agreed by parties representing a number of different industry sectors right across the value chain as providing an appropriate balance between the level of standardization and the opportunities for further innovation.

Under the title "CA neutral CPE" DVB attempted to standardize all hardware components required for an encryption system and the required interfaces. This was supposed to ensure that the terminal equipment could be relatively easily switched via a software update from one CA system to another. This attempt, which was not the first of its kind in DVB, was not continued due to a lack of support from key market participants and a lack of market demand once a number of other complexities concerning divergent middlewares, network connectivity and liability had become apparent.

The DVB Harmonized Security Framework makes a statement about standardizing code download security, in which it states that it "may compromise the security of other aspects of the device" and advises that "DVB should not standardize a code download security mechanism". In addition, it notes that "Notwithstanding the above, any standardized code download system has not to compromise other security aspects of the device".

ETSI ISG ECI is now making a new attempt to address standardization of downloadable CA/DRM solutions.

Further, in response to emerging trends and opportunities involving new types of devices and networks, there have also been successful standardization achievements in the field of security in other industry fora, some of the more recent of which are receiving strong market support. For example:

- DECE provides the means for the same content asset to be accessed by several CA/DRM systems through the use of a common file format and common encryption;

- ETSI KLAD is being widely deployed in consumer equipment and implemented in some markets; and

- the MPEG-CENC is being referenced by several bodies including DVB, HbbTV® and OMA.

Wide collaboration from, and consensus across industry seem to be factors that are important in creating standards which are successful in the market. However while industry collaboration and consensus appears to be essential, it is not always sufficient in leading to a standard which is viable in the longer term while some standards for security reviewed in the present document failed to achieve deployment because a suitable trust arrangement with a corresponding business model supporting it did not emerge.

Clause 6 provides a more abstract look at security in practice. Through a review of a number of factors influencing the level of security available, it shows that sound and comprehensive design is necessary to provide for the maintenance of system integrity. For that system integrity to be maintained and to secure access to the widest possible range of content, it will also be necessary to renew parts of the eco-system through a secure upgrade and in addition to maintain security through to the end display device. These fundamental constraints pose challenges to the ultimate level of interoperability that can be achieved.

In clause 7, various use cases are examined which illustrate that interoperable solutions are available and used in the market when there are business incentives for them. It is even possible to achieve a full interchange of a security solution through the support of a Trust Authority if there is a business imperative for an operator or system administrator to do so. In the case of a horizontal or retail market with involvement of a trust authority, a legal framework defining especially the rights and obligations of the relevant parties and well-defined work-flows and mechanisms for software maintenance including contractual obligations have to be defined. CI Plus is an established solution for CA/DRM interoperability and a feature of this is that manufacturers of TV terminal devices have no ongoing maintenance obligations. Another potential solution for interoperability is a software download framework. This requires the involvement of one or more trust authorities and well-defined work-flows, mechanisms and a legal framework for ongoing software maintenance including contractual obligations for all parties to the system, outside the existing traditional manufacturer - user liability relationship.

In clause 8 the newest trends for products and services are examined. It is clear that market needs for security evolve with new devices, products and services. In the case of UHDTV, the availability of encryption algorithms with longer key lengths is critical and this need was foreseen several years before, although not just with UHDTV in mind.

10 Conclusions

The comprehensive review of existing CA/DRM solutions and technical approaches in this report reveals that "security" is much more than just a technical feature, as it touches on business models, business agreements, trust and liability. In fact it is necessary to review the entire eco-system.

Market needs evolve with new products and services. New services and distribution means appear alongside with new business models complementing the traditional Pay-TV environment. Industry anticipates the need for new standards and collaborates to produce them through standard setting organizations, including many which were self-organizing, in order to facilitate the launch of these new products and services. The most successful standards are often produced through wide industry collaboration.

There are already several solutions for interoperability with regard to CA/DRM security available in the market, some of which have emerged quite recently to support new services such as UHDTV and new business models of video distribution and viewing via tablets and clients on other retail devices. These solutions evolved to meet quite different business needs and end user devices and are therefore deployed individually as necessary.

Some parties believe another solution for interoperability in security is desirable for consumers purchasing equipment in a retail market scenario and have tried to address this through standardization initiatives. Further work is underway in this area.

Industry agrees that interoperability is beneficial for economies of scale and inter-working between products. From a standardization point of view the specification and its implementation aims to provide for interoperability without compromising the required level of security while allowing space for competition and further innovation. As the level of security is determined by the weakest element of the system it is essential that the standardization of some components of a security system should not weaken the level of security.

A key component of a security system is its renewability feature, one example of which is a download mechanism. This component has similar needs to other components of a security system in terms of being secure and capable of being upgraded or refreshed.

Effective maintenance of security systems needs an entity acting as a trust authority to be responsible for the implementation and maintenance processes. Based on past evidence, parties embarking on the creation of a new security system or component with a clear understanding of how this responsibility will be implemented have enjoyed a greater degree of success with market deployments.

Having reviewed interoperable CA/DRM solutions, the present document concludes that producing successful standardized solutions is complex from both a business and technical perspective. New standards that fail to achieve sufficient support in the market can fragment the market further whereas achieving widespread adoption in the value chain can reduce fragmentation.

History

Document history		
V1.1.1	February 2015	Publication