ETSI TR 101 532 V1.1.2 (2015-03)

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

Reference

RTR/E2NA-00007-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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

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 Specification 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