International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.1010

(09/2016)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

Conditional access and protection – Exchangeable embedded conditional access and digital rights management solutions

Embedded common interface for exchangeable CA/DRM solutions; Use cases and requirements

Recommendation ITU-T J.1010

Recommendation ITU-T J.1010

Embedded common interface for exchangeable CA/DRM solutions; Use cases and requirements

Summary

Recommendation ITU-T J.1010 specifies use cases and requirements for exchangeable, embedded conditional access/digital rights management (CA/DRM) solutions, enabling customer premises equipment (CPE), which are capable of receiving broadcast and broadband content, to download CA/DRM clients under a trusted environment. By utilizing downloadable multi-CA/DRM service, entitled consumers can consume broadcast and broadband content, which is controlled by DRM and/or conditional access (CA) systems, even though a CPE does not have a required content-related CA/DRM client available by downloading it from a trusted source into various types of CPEs including set-top-boxes (STBs), smart TVs, PCs, smart phones and/or smart tablets.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T J.1010	2016-09-02	9	11.1002/1000/12772

Keywords

CA/DRM, exchangeable embedded common interface, retail CPE.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	1
3.1	Terms defined elsewhere	1
3.2	Terms defined in this Recommendation	1
4	Abbreviations and acronyms	2
5	Conventions	2
6	Requirements for exchangeable embedded CA/DRM solutions	3
6.1	General remarks	3
6.2	Generic requirements	4
6.3	Versatility related requirements	5
6.4	Practicability related requirements	5
6.5	ECI Client Swap related requirements	5
6.6	ECI System Security related requirements	6
Annex A – Use Cases		8
A.1	Use case 1	8
A.2	Use case 2	8
A.3	Use case 3	9
A.4	Use case 4 (Trusted third party (TTP) related use case)	9
Bibliography		10

Introduction

Service and content protection realized by conditional access (CA) and digital rights management (DRM) are essential in the rapidly developing area of digital broadcast and broadband, including content, services, networks and customer premises equipment (CPE), to protect business models of content owners, network operators and PayTV operators. While conceptually CA focuses on mechanisms to access protected content distributed by a service provider over a network, DRM originally describes type and extent of the usage rights, according to the subscriber's contract.

PayTV operators have established digital TV platforms, which implement standards for basic functions, extended with proprietary elements. Most CA and DRM systems used for classical digital broadcasting, IPTV or new OTT (over-the-top) services capture consumer premises equipment by binding it with proprietary security related elements. As a result, consumer premises equipment configured for use in network or platform A cannot be used in network or platform B or vice versa. Thus, the consumer electronics (CE) market for digital TV is still fragmented, as specifications differ not only per country, but also per platform. Detachable CA/DRM modules only offer a partial solution: the modules are again proprietary to the CA/DRM system, they are not cheap either, and they are used primarily for cable or satellite TV and are not usable in modern-type equipment such as tablets due to lack of appropriate physical interfaces.

Currently implemented solutions, whether embedded or as detachable hardware, result in "Lock-in" effects. This seriously restricts the freedom of many players in digital multimedia content markets. Due to technological advances, innovative, software-based CA/DRM solutions become feasible. Maximizing interoperability while maintaining a high level of security, they promise to meet upcoming demands in the market, allow for new businesses, and broaden consumer choice.

It is in consumers' interest that they are able to continue using the CPEs they bought e.g., after a move or a change of network provider or even utilize devices for services of different commercial video portals. This can only be achieved by interoperability of CPEs regarding CA and DRM, based on an appropriate security architecture. Further fragmentation of the market for CPEs can only be prevented and competition encouraged by ensuring a consumer-friendly and context-sensitive exchangeability of CA and DRM systems.

Recommendation ITU-T J.1010

Embedded common interface for exchangeable CA/DRM solutions; Use cases and requirements

1 Scope

The object of this Recommendation is a set of basic requirements for an exchangeable, embedded common interface, in order to download any necessary CA/DRM system to CPE. The download process is operated under a trusted environment and enables the consumption of protected content delivered via broadcast and/or broadband connections with various types of terminal equipment in line with the acquired content rights of the end-user. This Recommendation is one in a series of Recommendations, specifying the whole ECI eco-system.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation. The following referenced documents are necessary for the application of the present document.

[ETSI GS ECI 001-1] ETSI GS ECI 001-1: 2014, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions (ECI); Part 1: Architecture, Definitions and Overview.*

[ETSI GS ECI 001-2] ETSI GS ECI 001-2: 2014, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 2: Use cases and requirements.*

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 embedded common interface (ECI): Architecture and system to be specified in the ETSI ISG "Embedded CI", which allows the development and implementation of software-based swappable ECI clients in customer premises equipment (CPE) and thus provides interoperability of CPE devices with respect to ECI.

3.2.2 embedded common interface client (ECI client): Implementation of a CA/DRM client which is compliant with the planned Embedded CI specifications. Note that it is the software module in a CPE which provides all means to receive, in a protected manner, a consumer's entitlements and rights concerning the content that is distributed by a content distributor or operator. It also receives the conditions under which a right or an entitlement can be used by the consumer, and the keys to decrypt the various messages and content. An Embedded CI client may have an associated smart card.

3.2.3 embedded common interface (ECI) host: Hardware and software system of a CPE, which covers ECI related functionalities and has interfaces to an ECI Client. Note that the ECI host is one part of the CPE firmware.

3.2.4 protected content: All kinds of protected media, in particular A/V and associated metadata, delivered to the customer application either via linear or non-linear delivery means.

3.2.5 software container: Set of software interfaces to the host and to the client, which strictly separates the CA/DRM client from the host. The provisioning of the interfaces enables the exchangeability of the CA/DRM clients.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES	Advanced Encryption Standard
CA	Conditional Access
CA/DRM	Conditional Access/Digital Rights Management
CE	Consumer Electronics
CPE	Customer Premises Equipment
CSA	Common Scrambling Algorithm
DECE	Digital Entertainment Content Ecosystem
DRM	Digital Rights Management
DVB	Digital Video Broadcasting
ECI	Embedded Common Interface
IP	Internet Protocol
IPTV	TV using the Internet Protocol
OMA	Open Mobile Access
OTT	Over The Top (over the open Internet)
PVR	Personal Video Recorder
TTP	Trusted Third Party
URI	Usage Rights Information
VM	Virtual Machine

5 Conventions

In this Recommendation:

The keywords **"is required to"** indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords **"is recommended"** indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords **"is prohibited from"** indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords **"can optionally"** indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's

implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this document and its annexes, the words *shall*, *shall not*, *should*, and *may* sometimes appear, in which case they are to be interpreted, respectively, as *is required to*, *is prohibited from*, *is recommended*, and *can optionally*. The appearance of such phrases or keywords in an appendix or in material explicitly marked as *informative* are to be interpreted as having no normative intent.

6 Requirements for exchangeable embedded CA/DRM solutions

6.1 General remarks

The Group Specification on **ECI** basic requirements, as covered by the present Recommendation, is part of a multi-part deliverable specifying a system architecture for general purpose, software-based, embedded and exchangeable CA/DRM systems which would be the most appropriate and future-proof solution for overcoming market fragmentation and enabling interoperability. Key benefits of the envisaged approach for content security are:

– Flexibility and scalability due to software-based implementation.

– Exchangeability fostering future-proof solution and enabling innovation.

– Applicability to content distributed via broadcast and broadband, including OTT.

– Support of multi-screen environment.

– Stimulation of the market for platform operators, network/service providers, and consumers by avoiding "Lock-in".

– The specification of an open eco-system fostering market development.

The **ECI** system aims at exchangeability of CA and DRM systems in CPEs on all relevant levels and aspects, at lowest possible costs for the consumers and at minimal restrictions for CA or DRM vendors to develop their target products for the PayTV market. Therefore, amongst others, the ECI has the following functionalities:

– A software container for the CA respectively the DRM kernel – hereafter called **ECI Client** – with:

  • standardized interfaces to all relevant functionalities of the CPE;

  • a standardized **Virtual Machine (VM)** to run upon.

– Support of smartcard-less systems as well as use in smartcard-based systems.

– Inclusion of a multitude of such software containers in a CPE, each container running on its own instance of the **VM**.

– Installation of the **ECI Client** independently from other CPE software by a secure and standardized loader concept.

– **Advanced Security**, also known as Chip Set Security, to support content protection and to prevent unauthorized content access.

– Methods for the user to discover the right **ECI Client** to download.

– Methods for revocation of (parts of) the **ECI Client's** functionality and CPE's functionality.

– Suited for classical digital broadcasting, IPTV or modern OTT-based systems.

Although ECI shows some similarity with already deployed solutions, there are substantial differences:

1) The module is in software, no longer in hardware, hence no need for costs at the consumer side to swap a CA or DRM system.

2) Several parallel **ECI Clients** can be implemented in one and the same CPE, without adding relevant cost.

3) These clients can run concurrently in one device.

As a result, a CA or DRM component can be exchanged much easier, allowing the end-user to change operator or get services from a variety of operators on his CPE, without having to exchange expensive modules.

The complete multi-part deliverable consists of a group of specifications, including a Group Specification on Use cases and requirements, in combination with the underlying specifications:

– Part 1: Architecture, Definitions and Overview [ETSI GS ECI 001-1]

– Part 2: Use cases and requirements [ETSI GS ECI 001-2]

– Part 3: CA/DRM Container, Loader, Interfaces, Revocation [b-ETSI GS ECI 001-3]

– Part 4: The Virtual Machine (VM) [b-ETSI GS ECI 001-4]

– Part 5: The Advanced Security System [b-ETSI GS ECI 001-5]

– Part 6: Trust Environment [b-ETSI GS ECI 001-6]

– Part 7: Extended Requirements [b-ETSI GS ECI 001-7]

which together describe a solution allowing replacement of **ECI Clients** at any time by just downloading the **ECI Clients** requested by an end customer. The **ECI Clients** are installed in a standard software container in the CPE by a separate loader, with separate security algorithms and keys to protect the **ECI Clients** against integrity and substitution attacks independently from all other software in the CPE. The container's interfaces with the CPE are generic and defined in GS ECI 001-3 [b-ETSI GS ECI 001-3], enabling the **ECI Client** to interact with the various functions in the CPE and beyond.

The **ECI Clients** run upon a virtual machine instance that is defined in GS ECI 001-4 [b-ETSI GS ECI 001-4].

GS ECI 001-5 [b-ETSI GS ECI 001-5] specifies an Advanced Security mechanism to protect the key to the content during its travel into the CPE processor chip's content decryption facility.

This Recommendation addresses use cases and requirements as the basis for the implementation of interoperable CA/DRM systems in CPEs.

The **ECI** specification only applies to the reception and further processing of content which is controlled by a Conditional Access and/or Digital Rights Management system and has been scrambled by the service provider. Content that is not controlled by a Conditional Access and/or DRM system is not covered by this Recommendation.

The **ECI** Group Specification is intended to be used in combination with a contractual framework (license agreement), compliance and robustness rules, and appropriate certification process (see Note), under control of a **Trust Authority**, GS ECI 001-6 [b-ETSI GS ECI 001-6].

The end-to-end security of an ECI compliant CA/DRM system is not subject to the technical specifications only. The ECI technology is only one element of an ECI compliant eco system, GS ECI 001-1 [ETSI GS ECI 001-1], which has to be created by a Trust Authority, also taking into account a legal framework, device certification and other issues. The following requirements are based on the use cases as given in Annex A:

6.2 Generic requirements

[R 01] **Embedded CI** shall be applicable to any broadcasting, broadband and hybrid (means a combination of broadcast and broadband) services, delivering Protected Content via any type of appropriate access network to any type of applicable device.

[R 02] **Embedded CI** shall define a **Software Container** for ECI kernel software and closely related CA/DRM software functionalities, clearly separated from the remaining software elements of a CPE.

[R 03] **Embedded CI** shall provide Enhanced Security features comparable to those available with today's state of the art CA/DRM Systems.

[R 04] **Embedded CI** shall allow the design of secure CA/DRM system implementations, which can be operated and maintained for a long period of time, in all cases for at least a 5 years period.

6.3 Versatility related requirements

[R 05] **Embedded CI** shall support the implementation of more than one CA/DRM client in a CPE which provides a solution for the concurrent processing of at least two different **Protected Content** events.

[R 06] The architecture shall enable that different ECI clients in a CPE are able to recognize each other, can establish trust between each other, and are able to transfer content and the associated **URI** from one to another.

[R 07] The architecture shall enable that **ECI Clients** are able to establish trust to the **ECI Host** they are connected to and are able to securely transfer **URI** to the **ECI Host**.

[R 08] Compliance with national legal and regulatory requirements e.g., data privacy protection and protection of minors shall be ensured by **Embedded CI**.

[R 09] **Embedded CI** shall support the export of legally acquired **Protected Content** to other terminals (including mobile terminal devices) within a home domain or home network. This implies that the architecture provides the necessary interfaces that an ECI client in a CPE is able to talk to another ECI client in the same device. This shall only be possible in line with the usage rights issued by the respective content owners.

[R 10] An ECI client may be implemented in such a way, that it can export **Protected Content** to a non-ECI-compliant device. This shall only be possible in line with the usage rights issued by the respective content owners.

6.4 Practicability related requirements

[R 11] **Embedded CI** shall provide APIs for the implementation of user interfaces providing excellent usability and easy handling of user interactions.

[R 12] **Embedded CI** should not add noticeable delay with respect to comparable CA/DRM solutions even if the affected two channels (services) use different CA/DRM systems. Note that it is not assumed that the CA/DRM system has to be swapped during a regular channel (service) change.

[R 13] All ECI related activities (e.g., normal operation, download of an **ECI Client**) should not have noticeable **impact** on the user experience and performance.

6.5 ECI Client Swap related requirements

[R 14] **Embedded CI** shall allow changing to a new service provider without a required consent of the CA/DRM manufacturer, device manufacturer, platform, or service operator.

[R 15] In case of a swap of the ECI client the interruption of services shall be limited to a minimum.

[R 16] Subsequent to the exchange of an **ECI Client** the consumption of **Protected Content** (e.g., scrambled PVR content) legally acquired before the swap shall be possible without the need for any complex actions to be performed by the user.

[R 17] **Embedded CI** shall not unreasonably restrict the possibilities of CA/DRM vendors to develop different interoperable/swappable **ECI Clients** according to the market requirements.

6.6 ECI System Security related requirements

[R 18] It shall be possible to securely download, to install and to exchange the **ECI Client** for a CPE, and it shall be possible to do so in a standardized way. Downloading and installing the **ECI client** shall rely solely on standardized solutions.

[R 19] The CPE shall provide a **Software Container**, which shall provide a unified abstraction layer to any ECI client. Note that the unified abstraction layer is what a virtual machine would provide to the ECI client.

[R 20] The **ECI Clients** and the **Host** system shall be able to assert and prove its trustworthiness at any time.

[R 21] **Embedded CI** shall support the development and establishment of a **Trust Authority**.

[R 22] **Embedded CI** shall not depend on a specific hardware (component) or a specific operating system being present. This requirement does not generally prohibit advanced security features, as long as the specification of those features are publicly available and those features are compliant with today's security architectures of relevant CPE chip vendors. Note that advanced security systems specified in a publicly available document are not considered as a specific hardware.

[R 23] **The Embedded CI** system shall allow the migration of existing DVB/ETSI compatible CA/DRM systems to this new **Embedded CI** System. Note that this implies that an operator can address with his existing CA/DRM system both the legacy devices as well as new ECI compliant devices running an ECI client compatible with the existing CA/DRM system.

[R 24] **Embedded CI** shall provide hooks allowing the backwards compatible further development of **Embedded CI** and ECI implementations. It shall be possible that existing ECI implementations are able to handle usage rights introduced by future feature extensions of the CPE capabilities or ECI client capabilities.

[R 25] **Embedded CI** shall support both system implementations with and without SmartCards as security devices and shall provide the resources for both types of solutions.

[R 26] **Embedded CI** shall provide the necessary functionalities for all levels of content security required for the different CA/DRM system applications. It shall be applicable to mass markets and to the full range of pay products, from low end to premium products.

[R 27] In case of an ECI client swap **Embedded CI** shall not require replacement of any hardware component. However, according to this requirement, the swap of a SmartCard of a SmartCard-based CA/DRM systems is generally not considered as a replacement of a hardware component.

[R 28] **Embedded CI** shall not require significantly more resources (processing power, memory, etc.) of the CPE device than comparable, available today, embedded CA/DRM systems and the implementation of the system architecture shall not imply significant higher/additional cost.

[R 29] **Embedded CI** shall support at least DVB CSA and advanced encryption standard (AES) scrambling systems and the Host shall support at least MPEG-Transport Stream (ISO/IEC 13818-1 [b-ITU-T H.222.0]) and ISOBMFF (ISO/IEC 14496-12 [b-ISO/IEC 14496-12:2012] including Amendment 3 and conforming to the signalling defined by the Common Encryption scheme as defined in ISO/IEC 23001-7 [b-ISO/IEC 23001-7:2011] file but potentially with a different encryption algorithm). Note that Support of this requirement would be compatible with DRMs used by digital entertainment content ecosystem (DECE)

today and would provide a standard format for other DRMs to adopt for **Embedded CI** support.

[R 30] **Embedded CI** shall support a broad range of usage rights by providing the appropriate functionalities of the interface between the ECI container and the host.

[R 31] Embedded CI shall be able to describe usage rights and usage capabilities to an ECI client or from one ECI client to another.

[R 32] The Embedded CI shall provide a secure communication channel between ECI clients either on the same device or on different devices.

Annex A

Use Cases

(This annex forms an integral part of this Recommendation.)

The number of use cases covered in Annex A is not exhaustive.

A.1 Use case 1

In the digital TV business environment, different reasons might occur that require exchanging the CA/DRM system in CPE equipment.

– A digital media content provider may decide to change the CA/DRM system of CPEs for its customers. Reasons may be:
  - Different technical or commercial reasons, such as requirements of enhanced CA/DRM functionalities, higher security levels or higher system performance or in case of a deep hack of the current system.
  - Acquisition of new customers in a certain network, which used to access services of a competitor.

– A platform operator may decide to change the CA/DRM system of CPEs in its platform. Reasons may be:
  - Different technical or commercial reasons, such as requirements of enhanced CA/DRM functionalities, higher security levels or higher system performance or in case of a deep hack of the current system.
  - Harmonization of technologies after acquisition of a network.

– A CA/DRM vendor acquires a new customer which operates a platform, where a competitor had already established its CA system, or a CA/DRM vendor takes over another CA/DRM vendor and wants to harmonize the security technologies.

– An end-user has bought a CPE in any shop and connects it to the network of access network provider A. One or more service providers offer their services over this network. The end-user can choose any of these services and download their CA/DRM system, if he is registered (including authentication and authorization) with the corresponding service provider. After some time, the same end-user decides to be connected to the network of access network provider B. He connects his CPE to this network. If his CPE supports the required reception technologies (e.g., DVB-C/C2, -S/S2, -T/T2, Ethernet, xDSL), one or more service providers offer their services over this network. The end-user can choose any of these services and exchange/swap the CA/DRM systems accordingly, if he is registered (including authentication and authorization) with the corresponding service provider.

– A CE manufacturer wants to bring CPEs to the retail market, which support both FreeTV and PayTV. The CPEs may however be adapted for use with specific PayTV services by software upgrade with consent of the end-user.

A.2 Use case 2

Today, if the CA-System of an installed base of CPEs of an operative CA platform has to be changed (for whatever reason), there are always four partners involved:

– The current CA vendor.

– The platform operator or digital media content provider.

– The CPE manufacturer.

– The new CA vendor.

The current CA vendor has to provide the new vendor with both the technical information to access the installed base of CPEs, as well as a licence to use certain hardware components, protocols or software elements implemented in those CPEs. In any case the new CA-vendor has to adapt its CA System to the functionalities, hardware/software limitations and protocols available in the CPEs in the field. The CPE manufacturers have to integrate the new CA-System into the software of the different installed CPEs. In the worst case the swap of the CA/DRM system may be even not a viable technical/commercial option. This situation should be changed in order to achieve more interoperability.

As proprietary security modules are today an integral part of most state of the art CA systems, CPEs are mostly manufactured for dedicated CA systems. This may limit the level of security that can be provided by a swapped CA system for CPEs in the field. This situation should be changed in a way that any security enhancement should be completely transferrable.

A.3 Use case 3

The ECI system shall support consumption-only applications, including delivery of **Protected Content** to secondary devices. Two use cases are relevant for the support of secondary devices applications:

– Centralized application: The gateway type, ECI compliant CPE is delivering usage rights information (URI) and encrypted content to the secondary device.

– Decentralized application: The gateway type, ECI compliant CPE is delivering only URI to the secondary device and the secondary device derives the encrypted content from the network. Note that the ECI system has no requirements with respect to the implementation of a DRM client in a secondary device. In order to deliver protected content from a gateway to a secondary device it is only necessary that the two DRM clients are able to securely communicate between each other and the content owner support the implemented DRM system.

A.4 Use case 4 (Trusted third party (TTP) related use case)

Today, any required unique IDs or certificates are embedded in CPE in a proprietary way, defined by the provider of the CA/DRM system. With respect to interoperability this is not an appropriate solution, as vendors will most likely not disclose the mechanisms to access their unique IDs or certificates. For example, the CI plus consortium has demonstrated that it is feasible to transfer the secure handling of certificates to a "Trusted Third Party". Similar solutions will be required for interoperable CA/DRM systems.

Bibliography

[b-ITU-T H.222.0] Recommendation ITU-T H.222.0 (2006) | ISO/IEC 13818-1 (2007), *Information technology – Generic coding of moving pictures and associated audio information: Systems.*

[b-ETSI GS ECI 001-3] ETSI GS ECI 001-3, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 3: The CA/DRM Container: Loader, Interfaces, Revocation.*

[b-ETSI GS ECI 001-4] ETSI GS ECI 001-4, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 4: The Virtual Machine.*

[b-ETSI GS ECI 001-5] ETSI GS ECI 001-5, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 5: The Advanced Security System.*

[b-ETSI GS ECI 001-6] ETSI GS ECI 001-6, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 6: Trust Environment.*

[b-ETSI GS ECI 001-7] ETSI GS ECI 001-7, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 7: Extended Requirements.*

[b-ETSI ISG ECI] ETSI ISG ECI White Paper-v1_20 (2014), *Industry Specification Group on Embedded Common Interface for exchangeable CA/DRM solutions.*

[b-ISO/IEC 14496-12] ISO/IEC 14496-12:2012, *Information Technology – Coding of Audio-Visual Objects – Part 12: ISO Base Media file format.*

[b-ISO/IEC 23001-7] ISO/IEC 23001-7:2011, *Information technology – MPEG systems technologies – Part 7: Common encryption in ISO base media file format files.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	**Cable networks and transmission of television, sound programme and other multimedia signals**
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017