ETSI GS ECI 001-2 V1.2.1 (2018-03)

Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 2: Use cases and requirements

Disclaimer

The present document has been produced and approved by the Embedded Common Interface (ECI) for exchangeable CA/DRM solutions ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
RGS/ECI-001-2 Ed2

Keywords
CA, DRM, swapping

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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

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

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Embedded Common Interface (ECI) for exchangeable CA/DRM solutions.

The present document is part 2 of a multi-part deliverable covering Use cases and Requirements for the Embedded Common Interface for exchangeable CA/DRM solutions specification, as identified below:

Part 1: "Architecture, Definitions and Overview";

Part 2: "Use cases and requirements";

Part 3: "CA/DRM Container, Loader, Interfaces, Revocation";

Part 4: "The Virtual Machine";

Part 5: "The Advanced Security System";

Part 6: "Trust Environment".

The use of terms in bold and starting with capital characters in the present document shows that those terms are defined with an **ECI** specific meaning, which may deviate from the common use of those terms.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**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

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 services. This includes the distribution of HD and UHD content to various types of customer premises equipment (CPE) in order to protect business models of content owners and service providers, including Broadcasters and PayTV **Operator**s. While CA systems primarily focus on the protection of content distributed via unidirectional networks as usually used in broadcast environment, DRM systems originate from bidirectional network environments and permit access to content on certified devices for authenticated **Users**, with typically rich content rights expressions. In practice, a clear distinction between CA and DRM functionalities is not feasible in all cases and therefore within the present document the term CA/DRM systems is used.

Currently implemented CA/DRM solutions, whether embedded or as detachable hardware, often result in usage restrictions for service/platform providers on one side and consumers on the other. The consequences for consumers are dependencies with regard to the applicable network, service and content providers and the applied CPE suited for classical digital broadcasting, IPTV or OTT (over-the-top) services. While CPEs with embedded platform-proprietary CA or DRM functionality bind a **User** to a specific platform operator, detachable hardware modules allow using retail CPE as e.g. Set-Top-Boxes (STB) and integrated TV sets (iDTV). Due to their form factor and cost, detachable hardware modules do not fulfil future demands, especially those with regard to consumption of protected content on tablets and mobile devices and for cost-critical deployments.

Existing technologies thus bind the freedom of many players in digital multimedia content markets. Due to technological progress, innovative, software-based CA/DRM solutions become feasible. Maximizing interoperability while maintaining a high level of security, these solutions promise to meet upcoming demands in the market, allow for new businesses, and broaden consumer choice with respect to content consumption via broadcast and broadband connections.

It is in consumers' interest that bought and owned CPEs are available for further use after a move or a change of the network provider and those devices can be utilized for services of different commercial video portals. This can be achieved by the implementation of interoperable CA and DRM mechanisms inside CPEs based on appropriate security architecture. Further fragmentation of the market for CPEs can only be prevented and competition encouraged by ensuring solutions for consumer-friendly and flexible exchangeability of CA and DRM systems, associated with a state-of-the-art security environment.

It is in the Platform **Operator**'s interest that security technology can be deployed flexibly and managed easily across various networks and on all kinds of devices. The advantage of updating existing devices with the latest security systems in a seamless way provides unparalleled business opportunity.

Requirements of an **ECI Ecosystem** as specified in the present document as part of the ECI multi-part deliverable lay the bases for important attributes, as flexibility and scalability due to software-based implementation, exchangeability fostering a future-proof solution as well as for enabling innovation. Further aspects are applicability to content distributed via different types of networks, including classical digital broadcasting, IPTV and OTT services. The ECI system specification of an open eco-system, fostering market development, provides the basis for exchangeability of CA and DRM systems in CPEs, at lowest possible costs for the consumers and with minimal restrictions for CA or DRM vendors to develop their target products for the PayTV market.

The present document, part 2 of this multi-part deliverable, specifies all requirements, which the specifications have to fulfil in order to build the **ECI Ecosystem** in an appropriate way. The requirements reflect the needs of the different stakeholders along the value-chain.

1 Scope

The present document serves as a collection of requirements and use-cases of the different stakeholders along the value-chain for the **ECI Ecosystem** as specified in the **ECI** multi-part deliverable, including specification of the architecture of the **ECI** system as defined in **ECI** specification ETSI GS ECI 001-1 (V1.2.1) [1]. An **ECI Ecosystem** which fulfils these requirements will reveal the following features:

A major advantage and innovation of the **ECI Ecosystem**, compared with currently deployed systems, is a complete software-based architecture for the loading and exchange of CA/DRM systems, avoiding any detachable hardware modules. Software containers provide a secure ("Sandbox") environment for either CA or DRM kernels, hereafter named as **ECI Clients**, together with their individual **Virtual Machine** instances. The **Advanced Security System** is a powerful tool for the **ECI Client** to enhance its security. The download process is embedded in a secure and trusted environment, providing a trust hierarchy for installation and exchange of **ECI Host** and **ECI Clients** and thus enabling an efficient protection against integrity- and substitution attacks.

The present document covers requirements details in the following clauses:

Clause 4 contains all requirements structured in clauses:

- 4.1 Generic Requirements;
- 4.2 Versatility related Requirements;
- 4.3 Practicability related Requirements;
- 4.4 **ECI Client** Swap related Requirements;
- 4.5 **ECI** System Security related Requirements; and
- 4.6 Content protection and Usage Rights Information (URI) related requirements.

Annex A deals with relevant use cases.

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 https://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.

[1] ETSI GS ECI 001-1 (V1.2.1): "Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 1: Architecture, Definitions and Overview".

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] Recommendation ITU-T H.222.0 (2017)/ISO/IEC 13818-1:2007: "Information technology - Generic coding of moving pictures and associated audio information: Systems".

[i.2] ISO/IEC 14496-12:2015 : "Information Technology - Coding of Audio-Visual Objects - Part 12: ISO Base Media file format".

[i.3] ISO/IEC 23001-7:2016: "Information technology - MPEG systems technologies - Part 7: Common encryption in ISO base media file format files".

[i.4] NIST Special Publication 800-90C:2016: "Recommendation for Random Bit Generator (RBG) Constructions".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Advanced Security System (AS System): function of an **ECI** compliant **CPE**, which provides enhanced security functions (hardware and software) for an **ECI Client**

certificate: data with a complementary secure **Digital Signature** that identifies an **Entity**

NOTE: The holder of the secret key of the signature attests to the correctness of the data - authenticates it - by signing it with its secret key. Its public key can be used to verify the data.

content protection system: systems that employs cryptographic techniques to manage access to content and services

NOTE: The term may be interchanged frequently with the alternate Service Protection system. Typical systems of this sort are either Conditional Access Systems, or Digital Rights Management systems.

CPE Manufacturer: company that manufactures **ECI** compliant CPEs

digital signature: data (byte sequence) that decrypted with the public key of the signatory of another piece of data can be used to verify the integrity of that other piece of data by making a digest (hash) of the other piece of data and comparing it to the decrypted data

ECI (Embedded CI): architecture and the system specified in the ETSI ISG "Embedded CI", which allows the development and implementation of software-based swappable **ECI Client**s in customer premises equipment (CPE) and thus provides interoperability of CPE devices with respect to ECI

ECI Client (Embedded CI Client): implementation of a CA/DRM client which is compliant with the Embedded CI specifications

NOTE: It is the software module in a CPE which provides all means to receive, in a protected manner, and to control execution of 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.

ECI Ecosystem: commercial operation consisting of a TA and several platforms and ECI compliant CPEs in the field

ECI Host: hardware and software system of a CPE, which covers ECI related functionalities and has interfaces to an **ECI Client**

NOTE: The **ECI Host** is one part of the CPE firmware.

entity: organization (e.g. manufacturer, **Operator** or **Security Vendor**) or real world item (e.g. **ECI Host**, **Platform Operation** or **ECI Client**) identified by an ID in a **Certificate**

operator: organization that provides **Platform Operation**s that is enlisted with the **ECI TA** for signing the **ECI eco system**

NOTE: An **Operator** may operate multiple **Platform Operation**s.

platform operation: specific instance of a technical service delivery operation having a single ECI identity with respect to security

security vendor: company providing **ECI** security systems including **ECI Clients** for **Operators** of ECI **Platform Operations**

service: content that is provided by a **Platform Operation**

NOTE: In the context of **ECI** only protected content is considered.

smart card: detachable hardware security device used by several CA or DRM providers to enhance the level of security of their products

Trust Authority (TA): organization governing all rules and regulations that apply to a certain implementation of ECI and targeting at a certain market

NOTE: The Trust Authority has to be a legal **Entity** to be able to achieve legal claims. The Trust Authority needs to be impartial to all players in the **ECI Ecosystem** it is governing.

Trusted Third Party (TTP): security services provider, which issues **Certificate**s and keys to compliant **Manufacturer**s of the relevant components of an ECI-System

NOTE: It is under control of the **ECI Trust Authority (TA).**

user: person who operates an **ECI** compliant device

3.2 Abbreviations

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

AES	Advanced Encryption Standard
API	Application Programming Interface
AS	Advanced Security
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
HD	High Definition TV
HDMI	High Definition Multimedia Interface
iDTV	integrated Digital TV receiver
IP	Internet Protocol
IPTV	TV using the Internet Protocol (IP)
ISO	International Organization for Standardization
ISOBMFF	ISO Base Media File Format
MPEG	Motion Picture Experts Group
NIST	National Institute of Standards and Technology

OTT	Over The Top (over the open Internet)
PayTV	Pay Television
PVR	Personal Video Recorder
STB	SetTopBox
TA	Trust Authority
TTP	Trusted Third Party
TV	Television
UHD	Ultra High Definition TV
URI	Usage Rights Information
WEB	World Wide Web

4 Requirements

4.1 General remark

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 ecosystem, refer to [1], which has to be created by a **Trust Authority**, taking also into account a contractual framework, device certification and other issues. The following requirements are based on the use cases as given in annex A.

4.2 Generic Requirements

[R 01] **ECI** 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] **ECI** 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] **ECI** shall provide enhanced security features comparable to those available with today's state of the art CA/DRM Systems.

[R 04] **ECI** 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.

4.3 Versatility related Requirements

[R 05] **ECI** 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 **ECI**.

[R 09] **ECI** 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.

4.4 Practicability related Requirements

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

[R 12] **ECI** 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: 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.

4.5 ECI Client Swap related Requirements

[R 14] **ECI** 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 pertained 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] **ECI** shall not unreasonably restrict the possibilities of CA/DRM manufacturers to develop different interoperable/swappable **ECI Clients** according to the market requirements.

4.6 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 1: The unified abstraction layer is what a virtual machine would provide to the **ECI Client**.

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

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

[R 22] **ECI** 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.

[R 23] The **ECI** System shall allow the migration of existing DVB/ETSI compatible CA/DRM systems to this new **ECI** System.

NOTE 2: 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] **ECI** shall provide hooks allowing the backwards compatible further development of the **ECI** System 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] **ECI** shall support both system implementations with and without Smart Cards as security devices and shall provide the resources for both types of solutions.

[R 26] **ECI** 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 **ECI** shall not require replacement of any hardware component. However, according to this requirement, the swap of a Smart Card of a Smart Card-based CA/DRM systems is generally not considered as a replacement of a hardware component.

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

[R 29] **ECI** shall support at least DVB CSA and AES scrambling systems and the Host shall support at least MPEG-Transport Stream (ISO/IEC 13818-1 [i.1]) and ISOBMFF (ISO/IEC 14496-12 [i.2] including Amendment 3 and conforming to the signalling defined by the Common Encryption scheme as defined in ISO/IEC 23001-7 [i.3] file but potentially with a different encryption algorithm). The ECI System shall provide scrambling functionality with a security level comparable to AES128 or higher.

NOTE 3: Support of this requirement would be compatible with DRMs used by DECE today and would provide a standard format for other DRMs to adopt for **ECI** support.

[R 30] The **ECI** System shall provide APIs for establishing a secure communication channel between **ECI Clients** either on the same device or on different devices.

[R 31] Appropriate APIs shall be provided enabling the implementation of content protection solutions, which require the on-line delivery of keys for the decryption of content.

[R 32] Tools shall allow the implementation of **ECI Clients** which are able to minimize the number of compromised devices in case a single device is compromised.

[R 33] The **ECI** System shall allow binding the decryption of content to an individual device the content is targeted to be processed.

[R 34] The **ECI** System shall allow the renewal of individual keys or **Certificate**s relevant for different security related operations.

NOTE 4: This does not need to be fulfilled for the unique key of the CPE.

[R 35] The **ECI** System shall allow the implementation of ECI compliant devices supporting the requirements of HDCP2.2 or higher.

[R 36] The **ECI** architecture shall support a random number generator compliant with NIST 800-90c [i.4]

[R 37] The **ECI** architecture shall support integrity checking of downloaded **ECI Host** and **ECI Client** applications.

[R 38] The **ECI** specifications shall describe the principles and the technical aspects of how appropriate compliance and robustness rules and an associated certification process can be set up, ensuring the correct and reliable implementation and usage of the content protection mechanisms.

[R 39] The **ECI** specifications shall describe the technical aspects of how to ensure that the contractual licensing framework covers appropriate contractual provisions, remedy procedures and liability obligations in case there is a failure of any of the relevant content protection functionality.

4.7 Content protection and Usage Rights Information (URI) related requirements

[R 40] The **ECI** architecture shall provide APIs for the implementation of watermarking systems for content protection.

[R 41] The **ECI** System shall provide tools that enable **ECI** compliant CA/DRM systems to enforce the content protection rules selected by a content owner and to verify that they are correctly fulfilled.

[R 42] The **ECI** System shall define a secured interface to the host system for the delivery of relevant content protection data and rules. Content protection rules may need to verify CPE device features. The interface protocols shall support control commands for consumption and storage devices connected to the **ECI Host**.

[R 43] The **ECI** System shall support future extensions of the possible set of content protection parameters and rules. Therefore the interface specification needs to include a layering mechanism, allowing the definition of future extended (URI)-protocols.

[R 44] Generally output of protected content by the host shall be allowed via HDMI or similar interface with activated HDCP-protection on basis of the URI signalling. Forwarding to other devices (e.g. via IP-streaming) shall be under control of and needs to be enabled by the content-provider using URI-signalling. The URI-signalling shall include features for content stored in a PVR.

[R 45] An appropriate layering mechanism of the URI signalling shall allow to support future interface and content protection schemes.

[R 46] If requested by the content-provider, forwarding shall only be allowed encrypted using a trusted protection-system. If required, all restrictions signalled in URI shall be in force also for second screen usage.

NOTE: Decisions which content protection systems are trusted are taken solely by the relevant content provider.

[R 47] **ECI** shall support the content protection requirements and the Usage Rights Information (URI) at least for the established business models of encrypted Free-TV, Pay TV, and advertising financed encrypted TV by providing the appropriate functionalities of the interface between the **ECI Client** and the **ECI Host**.

[R 48] **ECI** shall support the transport of usage rights information (URI) between **ECI Clients**.

[R 49] The **ECI** System shall provide a URI signalling which allows the content provider to prohibit trick modes (time shifting, fast forward, skipping...) for a certain content element. This feature shall also be available in case such protected content element is replayed from a storage device by an appropriate URI signalling. It shall not prohibit the setting and usage of markers in such protected recorded content.

[R 50] Changes of the URI signalling shall become effective within one crypto-period of the CA-system and shall become effective no later than the start of the next crypto-period.

Annex A (informative): List of use cases

A.0 Use cases

The number of use cases covered in this annex 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 **Users**. 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 **Users** 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 flaw or 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.
- A **User** has bought a CPE in any shop and connects it to the network of provider A. One or more Service Providers offer their services over this network. The **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 **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 **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 **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

In addition to consumption only applications, the **ECI** system should also support delivery of protected content to secondary devices as well. Two examples for relevant use cases 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 receives the encrypted content from the network.

NOTE: 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**s** 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**. E.g. the current Common Interface based CA solution widely used in Europe 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.

History

Document history		
V1.1.1	September 2014	Publication
V1.2.1	March 2018	Publication