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

Copyright Notification

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.