ETSI GR ECI 004 V1.1.1 (2018-03)

Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Guidelines for the implementation of ECI

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
DGR/ECI-004

Keywords
CA, DRM, security

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

The present document on Guidelines for the implementation of **ECI** complements ETSI GS ECI 001 (all parts), [i.1] to [i.7] for the Embedded Common Interface for exchangeable CA/DRM solutions Group Specification (GS).

NOTE: 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 "**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 operators.

Existing CA/DRM technologies limit 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.

An **ECI Ecosystem,** compliant with ETSI GS ECI 001 (all parts) [i.1] to [i.7], addresses important attributes, such as enabling a high level of system security, flexibility and scalability due to software-based implementation, as well as exchangeability fostering a future-proof solution and enabling innovation. Further aspects are applicability to content distributed via different types of networks, including classical digital broadcasting, IPTV and OTT **Service**s. The **ECI** system specification of an open eco-system, fostering market development, provides the basis for exchangeability of CA and DRM systems in **CPE**s, 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.

Complementing ETSI GS ECI 001 (all parts) [i.1] to [i.7], the present document gives further guidance and addresses beside necessary performance requirements a number of use cases and scenarios, which on one side make use of the **ECI Ecosystem** and on the other extend its possibilities.

1 Scope

The present document serves as a guidance document for the **ECI Ecosystem** as specified in ETSI GS ECI 001 (all parts) [i.1] to [i.7], including specification of the architecture of the **ECI** system as defined in ETSI GS ECI 001-1 [i.1] and specification of the requirements as defined in **ECI** Group Specification ETSI GS ECI 001-2 [i.2]. A major advantage and innovation of the **ECI Ecosystem**, compared with currently deployed systems, is a fully software-based client container architecture, backed by a standardized advanced security hardware and secure software functionality for the loading and exchanging of CA/DRM client systems in **CPE**s. **ECI** compliant solutions do not require any detachable hardware modules in **CPE**s. Software containers provide a secure ("Sandbox") environment for either CA or DRM kernels, hereafter named as **ECI Client**s, together with their individual **Virtual Machine Instance**s. The download process is embedded in a secure and trusted environment, providing a trust hierarchy for installation and exchange of **ECI Host** and **ECI Client**s and thus enabling an efficient protection against integrity- and substitution attacks. For this reason, the **ECI Ecosystem** integrates an advanced security mechanism.

The present document covers implementation guidance details in the following clauses:

- Clause 4 contains performance requirements and parameters for the **ECI Host,** the **ECI Client**, the Virtual Machine and for the **Advanced Security System**.

- Clause 5 deals with use cases and applications based on the **ECI Ecosystem**, which either complement the **ECI** multi-part Group Specification or address given scenarios in more detail.

The present document has the objective to make available to **ECI** implementers as much as possible of the common understanding captured during the work of the ISG **ECI** developing the **ECI** specification series [i.1] to [i.8]. The present document was prepared with the intention to provide know-how complementary to the content of the **ECI** specifications [i.1] to [i.8] itself and about the environment in which an **ECI Ecosystem** will be operated. It is planned to extend this guideline by further guidance and background information gained during the implementation and operation of **ECI** compliant ecosystems.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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

[i.2] ETSI GS ECI 001-2 (V1.2.1): "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 2: Use cases and requirements".

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

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

[i.5] ETSI GS ECI 001-5-1: "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 5: The Advanced Security System; Sub-part 1: ECI specific functionalities".

[i.6] ETSI GS ECI 001-5-2: "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 5: The Advanced Security System; Sub-part 2: Key Ladder Block".

[i.7] ETSI GS ECI 001-6: "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 6: Trust Environment".

[i.8] ETSI GS ECI 002: "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; System Validation".

[i.9] ISO/IEC 23001-12:2015: "Information technology -- MPEG systems technologies -- Part 12: Sample Variants in the ISO base media file format".

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**

NOTE: The details are specified in [i.5] and [i.6].

AS slot: resources of the Advanced Security block provided exclusively to an **ECI Client** by the **ECI Host**

AS slot session: resources and computing in an **AS slot** related to the de-cryption or re-encryption of a content element

Certificate: data structure as defined in clause 5 of [i.3] 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.

CPE: ECI compliant customer premises equipment

NOTE: A **CPE** can be a stationary device (e.g. SetTopBox or iDTV) or any kind of mobile or portable device, which is able to process digital media content within an **ECI Ecosystem**.

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

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**s 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 Client Image: file with software as VM code, and initialization data required by the **ECI Client Loader**

ECI Client Loader: software module part of the **ECI Host** which allows downloading, verifying and installing new **ECI Client Image**s in an **ECI Host**

ECI Ecosystem: commercial operation consisting of a **TA** and several platforms and **ECI** compliant **CPE**s 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, (Entities): organization (e.g. **Manufacturer, Operator** or **Security Vendor**) or real world item (e.g. **ECI Host**, **Platform Operation** or **ECI Client**) identified by a unique ID in an **ECI Ecosystem**

Manufacturer: Entity which develops and sells **CPE**s, which accommodate an implementation of the **ECI** system and allow **ECI Host**s and **ECI Client**s to be installed per software download

Media Handle: reference to a single program decryption or re-encryption processing setup between an **ECI Client** and an **ECI Host**

Operator: organization that provides **Platform Operation**s and is enlisted with the **ECI TA** for signing the **ECI Ecosystem**

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

Request: message from a sender to a receiver asking for certain information or to perform a certain operation within an **ECI Ecosystem**, which is specified in the data fields of that request

NOTE: More details are given in clause 9.2.3 of [i.3].

Response: message within an **ECI Ecosystem** answering a **Request**

NOTE: More details are given in clause 9.2.3 of [i.3].

Revocation List (RL): list of **Certificate**s that have been revoked and therefore should no longer be used

Root: public key or **Certificate** containing a public key that serves as the basis for authenticating a chain of **Certificate**s

Root Certificate: trusted **Certificate** that is the single origin of a chain of **Certificate**s

Secure Authenticated Channel (SAC): communication path (channel) that has been established between two **Entities** where the **Entities** have securely identified themselves to each other (authenticated) and agreed on an encryption of data transferred between them (secure)

Security Vendor: company providing **ECI** security systems including **ECI Client**s for **Operator**s of **ECI Platform Operation**s

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

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

Trust Authority (TA): an 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.

User: person who operates an **ECI** compliant **CPE**

VM Instance: instantiation of VM established by an **ECI Host** that appears to an **ECI Client** as an execution environment to run in

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
BAT	Bouquet Association Table
CA	Conditional Access
CA/DRM	Conditional Access/Digital Rights Management
CAT	Conditional Access Table
CI	Common Interface
CPE	Customer Premises Equipment
CPS	Certificate Processing Subsystem
CPU	Central Processing Unit
CW	Control Word
DMIPS	Dhrystone Million Instructions Per Second
DRM	Digital Rights Management
DVB	Digital Video Broadcasting
ECM	Entitlement Control Message
EIT	Event Information Table
EITpf	EIT related to the present and the following content event
GS	Group Specification
HD	High Definition (Television)
HDD	Hard Disk Drive
HTTP	Hypertext Transfer Protocol
HTTP(S)	Hypertext Transfer Protocol Secure
iDTV	integrated Digital Television
IP	Internet Protocol
IPTV	TV using the Internet Protocol (IP)
MPEG	Motion Picture Experts Group
NIT	Network Information Table
NV	Non-Volatile (memory)
OTT	Over The Top (over the open Internet)
PAT	Program Association Table
PayTV	Pay Television
PID	MPEG Packet IDentifier
PMT	Program Map Table
PVR	Personal Video Recorder
RL	Revocation List
SAC	Secure Authenticated Channel
SD	Standard Definition (Television)
SDT	Service Description Table
SI	Service Information
SOC	System-On-a-Chip
SW	Software
TA	Trust Authority
TCP	Transmission Control Protocol
TECM	Time (delay) ECM
UHD	Ultra High Definition (Television)
URI	Usage Rights Information
VM	Virtual Machine

4 Guidelines for the implementation of an ECI compliant CPE

4.1 Introduction

Performance of CPE controllers is growing especially due to enhanced silicon technologies. Therefore performance figures for the **ECI**-implementation in **CPE**s have been defined separately in the present document, allowing **ECI** following any technological development in an easy way by updating or extending the present document.