ETSI GS ECI 001-1 V1.2.1 (2018-03)

Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 1: Architecture, Definitions and Overview

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-001-1 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 1 of a multi-part deliverable covering the Architecture, Definitions and Overview 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".

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 operators. 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 customer 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 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.

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 that 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.

1 Scope

The present document specifies the architecture of an **ECI Ecosystem**. 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. Necessary and relevant Application Programming Interfaces (API) between **ECI Clients** and **ECI Host** ensure that multiple **ECI Clients** can be operated in a secure operation environment and completely isolated from the rest of the CPE firmware and are specified in full detail. The installation, verification, and exchange of an **ECI Host** as well as multiple **ECI Clients** is the task of the corresponding **ECI** loaders. **ECI Host** and **ECI Clients** are downloaded via the DVB data carousel for broadcast services and/or via IP-based mechanisms from a server in case of broadband access. This 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. For this reason, the **ECI Ecosystem** integrates an advanced security mechanism, which relies on an efficient and advanced processing of control words, specified as "Key Ladder Block" and integrated in a System-on-chip (SoC) hardware in order to provide the utmost security necessary for **ECI** compliance.

ECI-specific advanced security functions play also a key role in a re-encryption process in case of stored protected content and/or associated with export of protected content to an **ECI**-compliant or non-compliant external device. An advanced Micro DRM system provides the necessary functionality and forms an integral part of such a concept. Advanced security functionality is relevant also in case of revocation of a CPE or a specific **ECI Client**. Related APIs are specified within the present document, while advanced security is covered in detail by ETSI GS ECI 001-5-1 [4] and ETSI GS ECI 001-5-2 [5].

A number of APIs characterize the **ECI Ecosystem**, guaranteeing communication with relevant entities associated e.g. with **ECI** Loaders, import and export of protected content, advanced security, decryption and encryption, local storage facilities and watermarking. Additional APIs are available for **ECI Client** Man-Machine-Interface (MMI) or for an optional **Smart Card** reader. Exchange of **ECI Clients** is initiated by the user or may be requested by a platform operator in case of necessary updates. A minimum of two **ECI Clients** are supported, with two additional **ECI Clients** as far as local storage on a Personal Video Recorder (PVR) is available or for export reasons. Guidance and recommendations on how to implement the **ECI** system are given in ETSI GR ECI 004 [i.1].

The present document covers the **ECI** architecture in the following clauses:

- Clause 4 covers the technical concept, core functionalities, and security aspects of the **ECI** system.
- Clause 5 addresses the basic requirements and structure for an **ECI Trust Environment**.
- Annex A gives an exemplary overview of the operational workflows of an **ECI Trust Environment**.

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 encrypted by the service provider. Content that is not controlled by a Conditional Access and/or DRM system is not covered by the present document.

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**, ETSI GS ECI 001-6 [6].

NOTE: Contractual framework (license agreement), compliance and robustness rules, and appropriate certification process are not subject to the standardization work in ISG **ECI**.

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

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

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

[4] 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".

[5] 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". .

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

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 GR ECI 004: "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Guidelines for the implementation of ECI".

3 Definitions and abbreviations

3.1 Definitions

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

advanced security: function of an **ECI** compliant CPE which provides enhanced security functions (hardware and software) for an **ECI Client**

NOTE: The details are specified in ETSI GS ECI 001-5-1 [4] and ETSI GS ECI 001-5-2 [5].

Embedded CI (ECI): architecture and the system 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**

Embedded CI Client (ECI 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 loader: software module part of the **ECI Host** which allows to download, verify and install new **ECI Client** software in an **ECI Container** of the **ECI Host**

Embedded CI Container (ECI Container): single **VM instance** with complementary support libraries and **ECI** API that permits a single instance of an **ECI Client** to run on a CPE

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. The **ECI Host** is responsible to ensure the isolation of each **ECI Container** and provides authenticated loading of **ECI Clients**.

ECI Host Loader: software module which allows to download, verify and install **ECI Host** software into a CPE

NOTE: In a multi-stage loading configuration this term is used to refer to all security critical loading functions involved in loading the **ECI Host**.

entity, entities: organization (e.g. manufacturer, operator) or real-world item (e.g. **ECI Host**, **ECI Client**) identified by a unique ID in an **ECI Ecosystem**

home domain: User's home network containing at least one **ECI** compliant CPE

Trust Authority (TA): organization governing all rules and regulations that apply to implementations of **ECI**

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 downloadable CA/DRM ecosystem.

trust environment: collection of rules and related process that constitutes the basis for an **ECI Ecosystem**

Trusted Third Party (TTP): technical service provider which issues certificates and keys to compliant manufacturers of the relevant components of an **ECI-System**

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

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

Virtual Machine Instance (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:

API	Application Programming Interface
CA	Conditional Access
CENC	Common Encryption
CI	Common Interface
CPE	Customer Premises Equipment
DRM	Digital Rights Management
DVB	Digital Video Broadcasting
ECI	Embedded Common Interface

HD	High Definition
HTTP	HyperText Transfer Protocol
iDTV	integrated Digital TV receiver
IP	Internet Protocol
IPTV	TV services delivered via IP protocol
ISO	International Standards Organization
LA	License Agreement
MMI	Man-Machine-Interface
MPEG	Motion Picture Experts Group
OS	Operating System
OSD	On Screen Display
OTT	Over The Top
PIN	Personal Identification Number
PVR	Personal Video Recorder
ROM	Read Only Memory
SI	Service Information
STB	Set-Top-Box
TA	Trust Authority
TTP	Trusted Third Party
TV	TeleVision
UHD	Ultra High Definition
UI	User Interface
VM	Virtual Machine

4 The technical concept of the **ECI** System

4.1 Basic considerations

The present document, in combination with parts 2 to 5-1 and 5-2 of the multi-part deliverable ([1], [2], [3], [4], [5] and [6]), specifies an architecture allowing downloading, installation, upgrading, removal and replacement of **ECI Clients** at any time, independently from other **ECI Clients** running on the same **ECI Host**, the **ECI Host** CPE's system software or applications running on that **ECI Host**. An **ECI Host** shall be capable to accommodate and to provide the runtime environment for as many **ECI Clients** as its resources can handle, but at least two. The **ECI Clients** shall be able to run in parallel, enabling simultaneous decryption or re-encryption of different content streams from different operators. Guidance and recommendations on how to implement the **ECI** system are given in ETSI GR ECI 004 [i.1].

The technical concept described in the present document and specified in [2] to [5], is applicable to both DVB Multicrypt compliant CA systems and Common Encryption (CENC) compatible DRM systems.

The CPE hosts a special loader only for **ECI Clients** with the necessary security functionality to protect the integrity and authenticity of the **ECI Clients**. This loader can be called and operated at any time to download and verify another **ECI Client** at any time. The loader with its associated security facilities is specified in ETSI GS ECI 001-4 [3].

Concerning this technical concept, each **ECI Client** is installed in a separate software container, with its own **Virtual Machine Instance** (**VM Instance**), which is specified in ETSI GS ECI 001-4 [3]. The **ECI Container** is specified for CA/DRM functionality only, which is reflected in ETSI GS ECI 001-3 [2]. The interface with the CPE, detailed in ETSI GS ECI 001-3 [2], enables the request and data exchange that is needed for the various CA/DRM functions. These requests and data exchanges may be performed between the **ECI Client** and the **ECI Host**, between two **ECI Clients** in the same **ECI Host** or two **ECI Clients** in different **ECI Hosts**.

TV-centric devices are defined as devices which include MPEG-2 transport stream processing inside the chip-set. **ECI** requires that those chip-sets implement **ECI**-compliant **Advanced Security** functionalities. ETSI GS ECI 001-5-1 [4] specifies provisions to leverage **Advanced Security** mechanisms in the chip-set, such as to protect the key associated with the content during its travel into the CPE processor chip's content decryption facility. This **Advanced Security** concept allows all **ECI Clients** using the facility, if needed, to operate simultaneously and independently from each other.

Devices for other environments, especially IPTV and tablets, smartphones, etc. typically implement more functionality in software and offer bidirectional IP-communication. This enables specific new types of security enhancement mechanisms. As chip-sets used in those devices include hardware for various processing security functions, **ECI** requires dedicated hardware-assisted security and robustness functionalities to be implemented in order to achieve **ECI**-compliance. Therefore, ETSI GS ECI 001-3 [2] includes methods for the **ECI Client** to obtain the relevant parameters of the **ECI Host**'s technical capabilities and functionalities, as far as relevant, including possible support of the **Advanced Security** as specified in ETSI GS ECI 001-5-1 [4] and ETSI GS ECI 001-5-2 [5].

The **Advanced Security** functionalities are available simultaneously to any **ECI Client** active in a CPE. **ECI Clients** can also be deployed in platforms with DVB compliant CA systems or with CENC compliant DRM systems running in simulcrypt or multicrypt mode, as long as the server sides of those systems are compliant with the respective DVB/CENC backend standards.

4.2 Architectural overview

The **ECI** allows CA/DRM providers to implement solutions for Conditional Access (CA) as well as for Digital Rights Management (DRM) within the domain of an individual customer. Figure 1 shows a reference configuration which is fully supported by a complete **ECI** implementation.

In order to support multi-screen environments within the individual consumer's domain, **ECI Clients** within that domain may communicate with each other, and may make use of a bidirectional network with the provider, depending on the availability of appropriate networks and supporting functionalities in the CA/DRM systems and their **ECI Clients**. ETSI GS ECI 001-3 [2] defines the necessary APIs required for those functionalities.

An **ECI Client** may be implemented in such a way that it is able to operate as a gateway also to non-**ECI**-conformant clients. The necessary APIs for it are specified in ETSI GS ECI 001-3 [2]. The specific protocols and implementations of proprietary clients are out of scope of the **ECI** specifications.

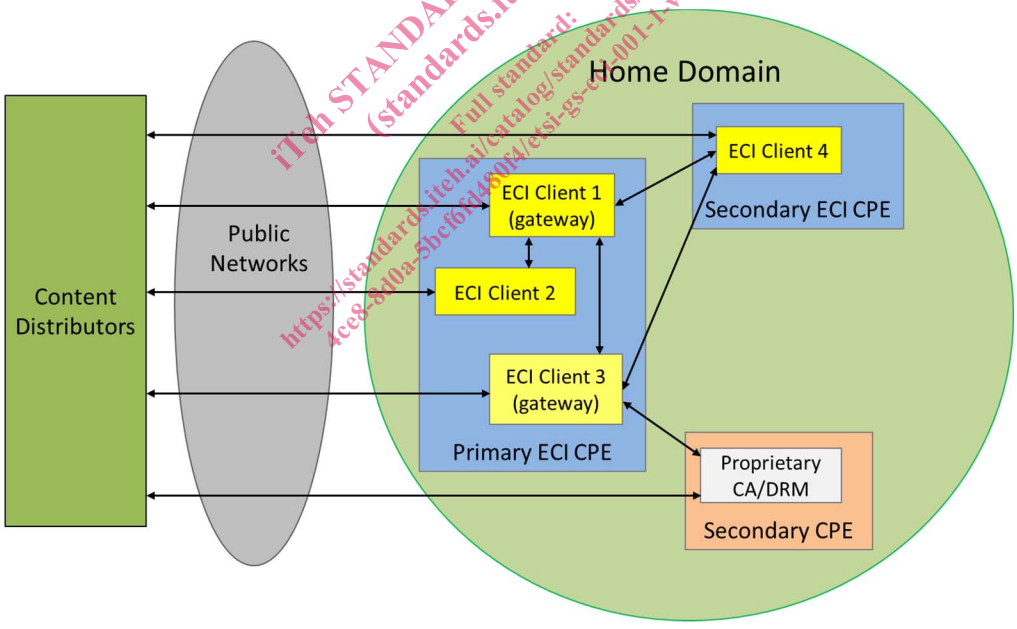

Figure 1: Multiple ECI Clients within a single Home Domain

The **ECI** specifications define, amongst others, the interface between an **ECI Client** and the **ECI Host.** Figure 2 shows the block diagram of a CPE with **ECI Clients**, and the other functions in the **ECI Host** that the **ECI Clients** may make use of. Some of these functions are optional. During the installation of an **ECI Client** and during launch of an **ECI Client**, the **ECI Host** specifies which relevant functions it has available to the **ECI Client**.