ETSI GS ECI 002 V1.1.1 (2018-04)

Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; System validation

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

DGS/ECI-002

Keywords

CA, DRM, validation

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

List of Figures

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 describes the validation of the ECI architecture that is specified in parts 1 to 6 of the ISG ECI multi-part document ETSI GS ECI 001 "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions". The titles of these parts are listed 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 5-1: "The Advanced Security System; ECI specific functionalities";

Part 5-2: "The Advanced Security System; Key Ladder Block";

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.

1 Scope

For implementations of an **ECI Ecosystem** as described in ETSI GS ECI 001-1 [1] the evaluation of the system architecture is of high importance with respect to verifying the correctness of the features described in the multi-part standard. The requirements for such a system are given in ETSI GS ECI 001-2 [2]. The present document contains a set of life-cycle oriented use cases reflecting the usage of components of an **ECI** system from its installation via its usage for content-protected media up to playout to an external device.

The **ECI** system aims at exchangeability of CA and DRM systems in the user's end device by defining appropriate interfaces between such systems and the device. End-users are enabled to install security clients on their devices to ensure interoperability with the services and devices of their choice. The platform operator, in collaboration with the content provider, can select the most suitable technology for a chosen application and can offer the corresponding application to his customers for download. The following features are supported by an **ECI** system:

- Provisioning of a software container for a CA respectively DRM kernel, called an **ECI Client**
- Implementation of multiple software containers in a device for the support of more than one protection scheme
- Installation of **ECI Clients** is separated from the installation of other CPE software
- Support for smartcard-less or smartcard-based protection systems
- Support for the user to discover and download the appropriate kernel
- Support for chip-set security, also known as Advanced Security
- Applicable to classical digital broadcasting, IPTV and OTT services

The fulfilment of these features is done via defined interfaces that are available for an **ECI Client**. The characteristics of these interfaces are described in clause 4 of the present document.

Afterwards, several test cases are described in order to show the correctness and the completeness of the **ECI** architecture as described in ETSI GS ECI 001-3 [3], ETSI GS ECI 001-4 [4], ETSI GS ECI 001-5.1 [5], ETSI GS ECI 001-5.2 [6] and ETSI GS ECI 001-6 [7]. Test cases described in clauses 5 to 8 include the installation of **ECI Host** and **ECI Client**, the installation of a second **ECI Client** and the decryption of protected content. Clause 9 shows the processing steps for a re-encryption of content whereas clause 10 describes the play-out of content to an external device. Besides these technically oriented tests cases the handling of security aspects and the provisioning of trust within an **ECI Ecosystem** is described in clause 11.

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 reference 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 (ECI) for exchangeable CA/DRM solutions; Part 1: Architecture, Definitions and Overview".

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

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

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

[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".

[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".

[7] 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 reference 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] ISO/IEC 13818-1: "Information technology -- Generic coding of moving pictures and associated audio information -- Part 1: Systems".

3 Definitions and abbreviations

3.1 Definitions

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

Advanced Security 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 ETSI GS ECI 001-5-1 [5].

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

Chipset-ID: non-secret number that is used to identify a chipset

Child, Children: entity (entities) referred to by a **Certificate** signed by a (common) **Father**

NOTE: **Father, Children, Brother** are referring to entities that manage **Certificates:** initialization data and software that is used to start the SoC of a **CPE**.

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.

Certificate Chain: list of certificates that authenticate each other including a Root **Revocation List**

Certificate Processing Subsystem: subsystem of the **ECI Host** that provides certificate verification processing and providing additional robustness against tampering

Control Word: secret key used to encrypt and decrypt content

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

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 Clients** 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 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 to download, verify and install new **ECI Client** software in an ECI Container of the **ECI Host**

ECI Ecosystem: real-world instantiation of a **Trust Environment** consisting of a **TA** and several platforms and **ECI** compliant **CPE**s in a commercial operation 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.

ECI Host Image: file with software and initialization data for an **ECI** environment

NOTE: It may also contain other software that does not cause interference with or permit undesirable observation of the **ECI Host.**

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**.

ECI Trust Authority (TA): organization governing all rules and regulations that apply to implementations of **ECI** and manages the interoperability and coexistence of CA and DRM systems within the **ECI Ecosystem** with respect to the establishment of a chain of trust

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.

Entity: organization (e.g. manufacturer, **Operator** or vendor) or real world item (e.g. **ECI Host**, **Platform Operation** or **ECI Client**) identified by an ID in a certificate

Export Connection: authenticated relation between an **ECI Client** that can decrypt content and a **Micro Server** that can re-encrypt content

Import Connection: approved connection from an **ECI Client** to a **Micro Server** that permits it to import decrypted content for subsequent re-encryption

Father: signatory of the certificate of an **Entity**

NOTE: The ID of the **Entity** is defined by and is unique in the context of the Father.

Key Ladder: function of the **Key Ladder Block** as defined in ETSI GS ECI 001-5-2 [6] for computing control words and associated control word usage information for application in the content decryption or re-encryption function of a CPE

Key Ladder Block: robust secure mechanism to compute decryption, encryption and authentication keys as defined in ETSI GS ECI 001-5-2 [6], both **Key Ladder** and **Authentication Mechanism**

Micro Client: ECI Client or non-**ECI** client that can decrypt content which was re-encrypted by a **Micro Server**

Micro Server: ECI Client that can import decrypted content, re-encrypt this content and authenticate a specific **ECI Client** or group of **ECI Clients** as the target for subsequent decryption

Micro DRM System: content protection system that re-encrypts content on a CPE with a **Micro Server** and that permits decoding of that re-encrypted content by authenticated **Micro Clients**

NOTE: **Micro Server** and **Micro Clients** being provisioned by a Micro DRM **Operator**.

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

NOTE: An **Operator** may operate multiple **Platform Operations**.

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

Re-encryption Session: process controlled by a **Micro Server** of importing content from an **Import Connection**, re-encrypting it and producing the decryption information necessary for the authenticated target to subsequently decrypt it

Revocation List (RL): list of certificates 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 certificates

Root Certificate: trusted certificate that is the single origin of a chain of certificates

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

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

3.2 Abbreviations

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

API	Application Programming Interface
AS	Advanced Security
BAT	Bouquet Association Table
CA	Conditional Access
CAT	Conditional Access Table
CI	Common Interface
CPE	Customer Premises Equipment
DRM	Digital Rights Management
DVB	Digital Video Broadcasting
ECM	Entitlement Control Message
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IPTV	Internet Protocol TeleVision
NIT	Network Information Table
NV	Non Volatile
OTT	Over The Top (over the open Internet)
PVR	Personal Video Recorder
SI	Service Information
SSU	System Software Update
TA	Trust Authority
URI	Usage Rights Information
URL	Uniform Resource Locator
VM	Virtual Machine

4 Characteristics of ECI interfaces

4.1 General remarks

Interfaces that are available for an **ECI Client** are classified in six groups of **Application Programming Interfaces** named as APIs. These APIs provide functions and attributes the **ECI Client** can benefit from. The classification is shown in **Figure 4-1**.

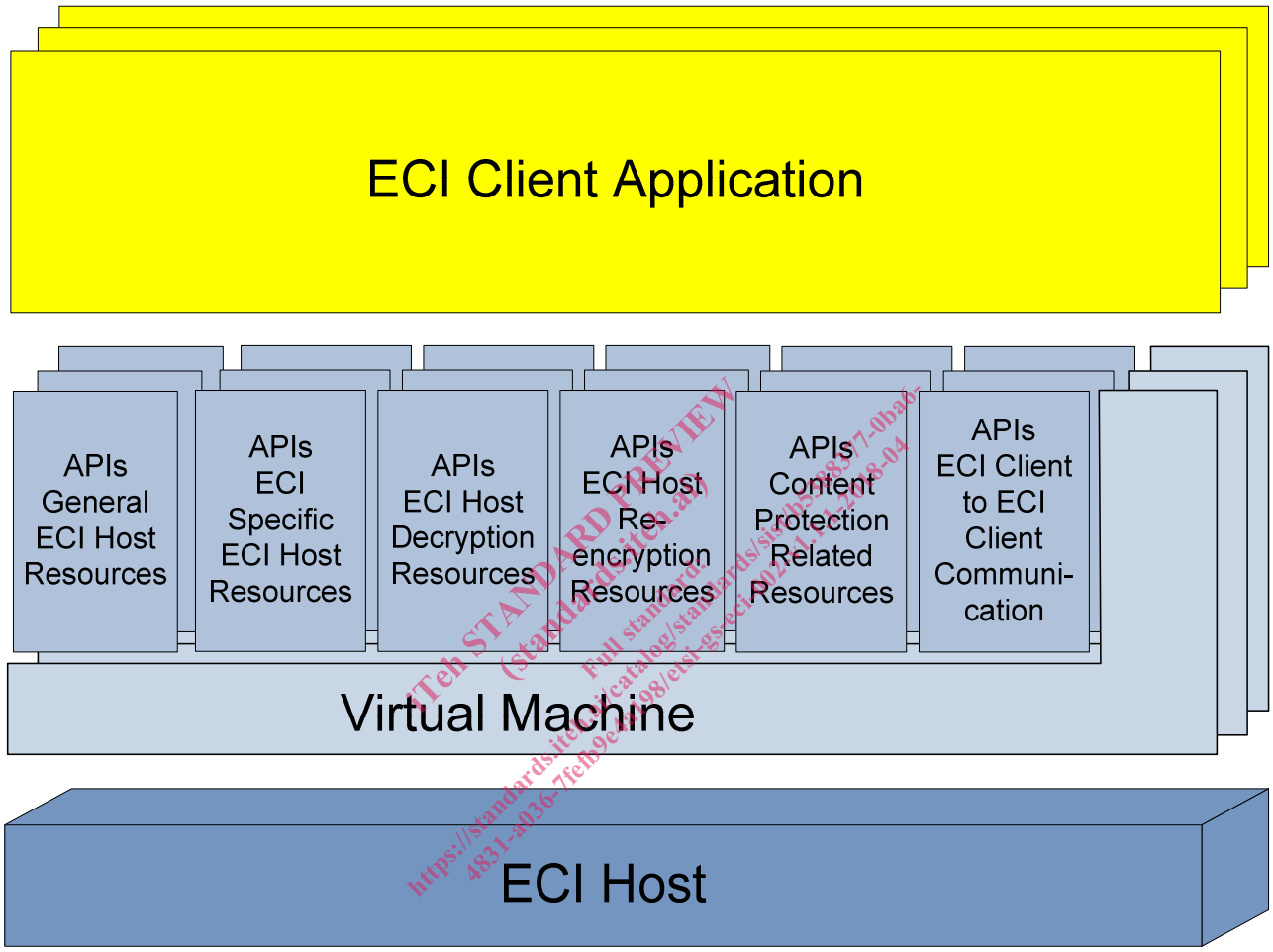

Figure 4-1: API classification of the ECI architecture

4.2 General ECI Host resources

This API class provides the **ECI Client** with functionalities allowing the discovery of interface resources the **ECI Host** has available. The messages that are exchanged between **ECI Client** and **ECI Host** are important to set up the features the **ECI Host** will be possible to offer to the end-user depending on the facilities of the device. This API class supports the communication with the user, can establish the IP connection to a device, allows the **ECI Client** to store data in the memory of the **ECI Host**, is responsible for the settings of time, data and languages and allows communication with the power management.

4.3 ECI specific ECI Host resources

This API class allows the **ECI Client** to gain access to the functionalities of the **Advanced Security System** of the **ECI Host** and it also handles the usage of a smart card reader. Taking into account that an **ECI Client** very likely will be active as part of a DVB environment, this API additionally allows to gain access to a data carousel according to the DVB standard.

4.4 ECI Host decryption resources

In the ECI architecture every media decryption is initiated and controlled by the **ECI Host**. This class supports the selection of an **ECI Client** following the content decryption requirements for the media to be decrypted. The **ECI** architecture supports two different types of media formats, the MPEG Transport Stream and the ISOBMFF file format. The request of an **ECI Host** to open a descrambling session includes the check whether all the resources needed for accessing the content and the accompanying metadata are available at both sides, for the **ECI Host** as well as for the **ECI Client**. Only if this is guaranteed, the decryption session will start.

4.5 ECI re-encryption resources

Content that is going to leave the protected environment of the **ECI** architecture needs to possess the possibility to be protected again by an encryption scheme. This API class supports such a protection by provisioning functionalities for re-encryption e.g. for further distribution or for storage. The **ECI Host** requests from the **ECI Client** some information about DRM servers that can deliver further information about re-encryption and this information is then used to set up appropriate sessions to start such a re-encryption process. The re-encryption system is called a **Micro DRM System** and the **ECI Client** that initially decrypted the content can control to which **Micro DRM System** the export of content is going to happen.

4.6 Content protection related resources

This API class supports CA/DRM providers in setting up a content property system according to their needs. Access to Usage Rights Information (URI) can be granted on several security levels. The URI is generated by the **ECI Client** and is used by the **ECI Host** to control applications possessing access to media content. This also includes the support for blocking the presentation or processing of media in a selective way. Outgoing content can be water-marked by the **ECI Client** and parental control permits the **ECI Client** to authorize the consumer before displaying the content.

4.7 ECI Client Communication related resources

This API class supports the communication between **ECI Clients**. Those may communicate amongst themselves in order to provide additional functionality. **ECI Clients** can register their principle ability and willingness to support inter client communication through a discovery resource. After system initialization, they can read the identities of other **ECI Clients** including the established **Import/Export Connections.**

5 Installation of an ECI Host

In order to make an end-user's device **ECI** compatible, this device needs to be prepared in such a way that one or more **ECI Clients** can be installed. This part of the preparation is done with the help of an **ECI Host** which itself is installed via an **ECI Host Loader**.

This test case is characterized by the following terms:

- Prerequisite: **ECI Host** not yet installed on the device or update of an existing **ECI Host** necessary.
- Status after activity: **ECI Host** installed on device.

The steps for the installation of an **ECI Host** are shown in the flow diagram in Figure 5-1.