ETSI GS ECI 001-1 V1.1.1 (2014-09)

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

Disclaimer

This 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-001-1

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

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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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 (http://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.

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";

Part 7: "Extended Requirements".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**may not**", "**need**", "**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, including content, services, networks and customer premises equipment (CPE), to protect business models of content owners, network operators and PayTV operators. While conceptually CA focuses on mechanisms to access protected content distributed by a service provider over a network, DRM originally describes type and extent of the usage rights, according to the subscriber's contract.

PayTV operators have established Digital TV platforms, which implement standards for basic functions, extended with proprietary elements. Most CA and DRM systems used for classical digital broadcasting, IPTV or new OTT (over-the-top) services capture consumer premises equipment (CPE) by binding it with proprietary security related elements. As a result, consumer premises equipment configured for use in network or platform A cannot be used in network or platform B or vice versa. Thus, the consumer electronics market for digital TV is still fragmented, as specifications differ not only per country, but also per platform. Detachable CA/DRM modules only offer a partial solution: the modules are again proprietary to the CA/DRM system, they are not cheap either, and they are used primarily for cable or satellite TV and are not usable in modern-type equipment such as tablets due to lack of appropriate physical interfaces.

Currently implemented solutions, whether embedded or as detachable hardware, result in "Lock-in" effects. This seriously restricts the freedom of many players in digital multimedia content markets. Due to technological advances, innovative, software-based CA/DRM solutions become feasible. Maximizing interoperability while maintaining a high level of security, they promise to meet upcoming demands in the market, allow for new businesses, and broaden consumer choice.

It is in consumers' interest that they are able to continue using the CPEs they bought e.g. after a move or a change of network provider or even utilize devices for services of different commercial video portals. This can only be achieved by interoperability of CPEs regarding CA and DRM, based on an appropriate security architecture. Further fragmentation of the market for CPEs can only be prevented and competition encouraged by ensuring a consumer-friendly and context-sensitive exchangeability of CA and DRM systems.

1 Scope

ECI Architecture, Definitions and Overview, as covered by this framework document, is part of a multi-part standard specifying a system architecture for general purpose, software-based, embedded and exchangeable CA/DRM systems which would be the most appropriate and future-proof solution for overcoming market fragmentation and enabling interoperability**.** Key benefits of the envisaged approach for content security are:

- Flexibility and scalability due to software-based implementation
- Exchangeability fostering future-proof solution and enabling innovation
- Applicability to content distributed via broadcast and broadband, including OTT
- Support of multi-screen environment
- Stimulation of the market for platform operators, network/service providers, and consumers by avoiding "Lock-in"
- The specification of an open eco-system fostering market development

The **ECI** system aims at exchangeability of CA and DRM systems in CPEs on all relevant levels and aspects, at lowest possible costs for the consumers and at minimal restrictions for CA or DRM vendors to develop their target products for the PayTV market. The core element of ECI is to specify the interface between the software-based CA/DRM –client and the host system. Therefore, amongst others, the ECI has the following functionalities:

- A software container for the CA respectively the DRM kernel – hereafter called **ECI Client** - with:
  - standardized interfaces to all relevant functionalities of the CPE
  - a standardized **Virtual Machine (VM)** to run upon
- Support of smartcard-less systems as well as use in smartcard-based systems
- Inclusion of a multitude of such software containers in a CPE, each container running on its own instance of the **VM**
- Installation of the **ECI Client** independently from other CPE software by a secure and standardized loader concept
- **Advanced Security**, also known as Chip Set Security, to support state-of-the-art content protection
- Provisions to leverage hardware-assisted security functionalities
- Methods for the user to discover the right **ECI Client** to download
- Methods for revocation of (parts of) the **ECI Client's** functionality and CPE's functionality
- Suited for classical digital broadcasting, IPTV or modern OTT-based systems

Although ECI shows some similarity with already deployed solutions, there are substantial differences:

1) The CA/DRM client module is in software and no longer in hardware. Hence, no costs are incurred at the consumer side to swap a CA or DRM system.
2) Several parallel **ECI Clients** can be implemented in one and the same CPE, without adding relevant cost.
3) These clients can run concurrently in the one device.

As a result, a CA or DRM component can be exchanged much easier, allowing the end-user to change operator or get services from a variety of operators on his CPE, without having to exchange expensive modules.

The complete multi-part standard consists of a group of specifications, including a Framework specification (the present document), in combination with the underlying specifications:

Part 1: Architecture, Definitions and Overview (the present document)

Part 2: Use cases and requirements [1]

Part 3: CA/DRM Container, Loader, Interfaces, Revocation [i.1]

Part 4: The Virtual Machine (VM) [i.2]

Part 5: The Advanced Security System [i.3]

Part 6: Trust Environment [i.4]

Part 7: Extended Requirements [i.5]

which together describe a solution allowing replacement of **ECI Clients** at any time by just downloading the **ECI Clients** requested by an end customer. The **ECI Clients** are installed in a standard software container in the CPE by a separate loader, with separate security algorithms and keys to protect the **ECI Clients** against integrity and substitution attacks independently from all other software in the CPE. The container's interfaces with the CPE are generic and defined in GS ECI 001-3 [i.1], enabling the **ECI Client** to interact with the various functions in the CPE and beyond.

The **ECI Clients** run upon a virtual machine instance that is defined in GS ECI 001-4 [i.2].

GS ECI 001-5 [i.3] specifies an Advanced Security mechanism to protect the key to the content during its travel into the CPE processor chip's content decryption facility.

The present document addresses an architecture and an overview of the relevant interface specifications for the implementation of interoperable CA/DRM systems in CPEs.

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 scrambled 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, GS ECI 001-6 [i.4].

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

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 http://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.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

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

2.2 Informative references

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.

NOTE: The following references are intended to become normative references once these Group Specifications are completed.

[i.1] ETSI GS ECI 001-3: "Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 3: CA/DRM Container, Loader, Interfaces, Revocation".

[i.2] ETSI GS ECI 001-4: "Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 4: The Virtual Machine".

[i.3] ETSI GS ECI 001-5: "Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 5: The Advanced Security System".

[i.4] ETSI GS ECI 001-6: "Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 6: Trust Environment".

[i.5] ETSI GS ECI 001-7: "Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 7: Extended Requirements".

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 [i.3].

ECI (Embedded CI): the 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 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 Container (Embedded CI Container): abstract concept which provides an isolated environment comprised of a virtual machine and a single ECI client

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 (new) 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.

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.

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

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
MPEG	Motion Picture Experts Group
OS	Operating System
OSD	On Screen Display
OTT	Over The Top
PIN	Personal Identification Number
ROM	Read Only Memory
SI	Service Information
TA	Trust Authority
TTP	Trusted Third Party
TV	Television
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 and 7 of the specifications ([1], [i.1], [i.2], [i.3] and [i.5]), 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 host, the host CPE's system software or applications running on that 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, at least two. The **ECI Clients** in a host have to run in parallel, enabling simultaneous decryption or re-encryption of different content streams from different operators.

The technical concept described in the present document and specified in [1], [i.1], [i.2] and [i.3], 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 [i.1].

Concerning this technical concept, each **ECI Client** is installed in a separate software container, with an own **Virtual Machine** instance (**VM** instance), which is specified in [i.2]. The **ECI Container** is specified for CA/DRM functionality only, which is reflected in [i.1]. The interface with the CPE, detailed in [i.1], 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 host, between two **ECI Clients** in the same host or two **ECI Clients** in different 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. GS ECI 001-5 [i.3] 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, the specification [i.1] includes methods for the **ECI Client** to obtain the relevant parameters of the host's technical capabilities and functionalities, as far as relevant, including possible support of the Advanced Security as specified in [i.3].

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**. [i.1] gives further details.

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 hooks therefore are specified in [i.3]. The specific protocols and implementations of proprietary clients are out of scope of the ECI specifications.