# ETSI GS ECI 001-2 V1.1.1 (2014-09)




# Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 2: Use cases and requirements

***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-001-2

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

***Copyright Notification***

# 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 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";

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

The Group Specification on **ECI** basic requirements, as covered by the present document, is part of a multi-part deliverable 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. 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 content protection and to prevent unauthorized content access.
- 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 module is in software, no longer in hardware, hence no need for costs 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 deliverable consists of a group of specifications, including a Group Specification on Use cases and Requirements (the present document), in combination with the underlying specifications:

Part 1: Architecture, Definitions and Overview [1].

Part 2: Use cases and requirements (the present document).

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 use cases and requirements as basis 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].



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

## 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 (ECI) for exchangeable CA/DRM solutions; Part 3: The CA/DRM Container: Loader, Interfaces, Revocation".

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

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

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

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

[i.6] Recommendation ITU-T H.222.0 (2006)/ISO/IEC 13818-1:2007: "Information technology - Generic coding of moving pictures and associated audio information: Systems".

[i.7] ISO/IEC 14496-12:2012: "Information Technology - Coding of Audio-Visual Objects - Part 12: ISO Base Media file format".

[i.8] ISO/IEC 23001-7:2011: "Information technology - MPEG systems technologies - Part 7: Common encryption in ISO base media file format files".



# 3 Definitions and abbreviations

## 3.1 Definitions

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

**Embedded Common Interface (ECI):** architecture and system to be 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 Common Interface client (ECI client):** implementation of a CA/DRM client which is compliant with the planned Embedded CI specifications

NOTE: It is the software module in a CPE which provides all means to receive, in a protected manner, 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. An Embedded CI client may have an associated smart card.

**Embedded Common Interface (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.

**protected content:** all kinds of protected media, in particular A/V and associated metadata, delivered to the customer application either via linear or non-linear delivery means

**software container:** set of software interfaces to the host and to the client, which strictly separates the CA/DRM client from the host

NOTE: The provisioning of the interfaces enables the exchangeability of the CA/DRM clients.

## 3.2 Abbreviations

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

| | |
|---|---|
| AES | Advanced Encryption Standard |
| 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 |
| IP | Internet Protocol |
| IPTV | TV using the Internet Protocol (IP) |
| OMA | Open Mobile Access |
| OTT | Over The Top (over the open Internet) |
| PVR | Personal Video Recorder |
| TTP | Trusted Third Party |
| URI | Usage Rights Information |
| VM | Virtual Machine |



# 4 Requirements

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 eco system, GS ECI 001-1 [1] which has to be created by a Trust Authority, taking also into account a legal framework, device certification and other issues. The following requirements are based on the use cases as given in Annex A.

## 4.1 Generic Requirements

[R 01] **Embedded CI** 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] **Embedded CI** 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] **Embedded CI** shall provide Enhanced Security features comparable to those available with today's state of the art CA/DRM Systems.

[R 04] **Embedded CI** 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.