ETSI GS ECI 001-6 V1.1.1 (2018-02)

GROUP SPECIFICATION

Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 6: Trust Environment

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-001-6

Keywords

CA, DRM, trust

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 6 of a multi-part deliverable covering the Trust Environment 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".

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 "**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

The **ECI** system combines security with interoperability to provide a flexible and future-proof content protection system. It is an open, standardized system, which allows CA/DRM vendors to implement a wide range of products and consumers to readily switch between vendors on **ECI** compliant **CPEs**. The openness of the **ECI** system requires specific security elements in a compliant **CPE** to be swappable. In addition to the technical aspects of the standard there exist certain operational and commercial aspects which need to be handled in order for the security of the system, and the trustworthiness for all stakeholders to be provisioned and maintained. These aspects are addressed by creating a **Trust Environment** that consists of a contractual framework, policies, and technical specifications required for creating an **ECI Ecosystem**.

1 Scope

The present document specifies the basic technical principles and tasks for defining an **ECI** compliant **Trust Environment** intended for establishing an **ECI Ecosystem** as specified in [1], [2] and [3]. The present document therefore also provides guidance for a party that intends to serve as an **ECI Trust Authority** for an **ECI Ecosystem**.

The present document covers specification details in the following clauses: clause 4 addresses the **Trust Environment** and its stakeholders, clause 5 addresses the role of the **ECI Trust Authority**, clause 6 describes the tasks of the **ECI Trust Authority**, and clause 7 deals with critical workflows within the **ECI Ecosystem**. An annex gives some additional background information on the security aspects.

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

[2] ETSI GS ECI 001-2: "Embedded Common Interface (ECI) for exchangeable CA/DRM 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 002: "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; System validation".

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

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 chains: list of **certificates** that authenticate each other up to and including a Root Revocation List

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

content protection system: systems that employs cryptographic techniques to manage access to content and services

NOTE: The term may be interchanged frequently with the alternate Service Protection system. Typical systems of this sort are either Conditional Access Systems, or Digital Rights Management systems.

Customer Premises Equipment (CPE): media receiver which has implemented **ECI**, allowing the user to access digital media services

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

digital signature: data (byte sequence) that decrypted with the public key of the signatory of another piece of data can be used to verify the integrity of that other piece of data by making a digest (hash) of the other piece of data and comparing it to the decrypted data

Embedded Common Interface (ECI): 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** devices with respect to **ECI**

ECI chip manufacturer: company providing Systems on a Chip that implement **ECI** specified chipset functionality

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 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(s) with software and initialization data for an ECI environment

NOTE: An **ECI host** image may consist of a number of **ECI host image** files.

ECI root certificate: certificate which issues to verify items approved by an **ECI TA**

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

entity, entities: organization(s) (e.g. manufacturer, **operator** or **security vendor**) or real world item(s) (e.g. **ECI host**, **platform operation** or **ECI client**) identified by an ID in a **certificate**

manufacturer: entity which develops and sells **CPEs**, which accommodate an implementation of the **ECI** system and allow **ECI hosts** and **ECI clients** to be installed per software download

operator: organization that provides **platform operation**s that is enlisted with the **ECI TA** for sing the **ECI** ecosystem

NOTE: An **operator** may operate multiple **platform operations.**

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

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 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): 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.

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

Trusted Third Party (TTP): external company that fulfils operational roles and tasks of the **Trust Authority** and on its behalf, such as issuing certificates

3.2 Abbreviations

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

API	Application Program Interface
AS	Advanced Security
CA	Conditional Access
CA/DRM	Conditional Access/Digital Rights Management
CI	Common Interface
COBIT	Control Objectives for Information and Related Technologies
CPE	Customer Premises Equipment
CPS	Certificate Processing Subsystem
DRM	Digital Rights Management
ECI	Embedded Common Interface
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
PO	Platform Operation
TA	Trust Authority
TTP	Trusted Third Party

4 Overview

4.1 Introduction

The technical **ECI** specifications [1], [2], [3], [4], [5], [6], and [7] provide significant freedom for making technical implementations, enabling ecosystems to make their own choices on how to implement certain features. In addition, the openness of the **ECI** system allows for certain components to be interchangeable. These properties require mutual trust between parties participating in the system and compliance to a common set of rules. These rules are collected in a **Trust Environment** and created and maintained by an **ECI Trust Authority** (**TA**).

The **Trust Environment** is defined by the **Trust Authority** and consists of the contractual framework, policies, and technical specification required for creating a real-world **ECI Ecosystem**. The **TA** is a legal entity that governs all rules and regulations for a specific **Trust Environment** and enforces them through legal and technical means**.** In addition, the **Trust Authority** serves as trusted root for the chain of certificates use to authenticate **Entities** of the ecosystem.

4.2 Trust Environment and ecosystem

The **Trust Environment** is a formal construct that combines all mandatory aspects described in the present document as well as the other **ECI** specifications. The **Trust Environment** is therefore the sum of all technical and contractual aspects needed for creating a real-world ecosystem.

The **ECI Ecosystem** is the real-world instantiation of a **Trust Environment**. An ecosystem is always created on the basis of a **Trust Environment**. However, the concrete shape of the ecosystem is also affected by regulatory, legal, and economic factors that are outside of the scope of the present document.

4.3 ECI Certificates and trust

Within the **ECI Ecosystem**, trust is established and managed through the use of **ECI** specific **Certificates** and **Certificate Chains** as defined in ETSI GS ECI 001-3 [3]. This allows all parties involved with an **ECI Ecosystem**, from key stakeholders to end users, to verify that each certified **Entity** has been directly or indirectly certified by the **Trust Authority**. Examples that illustrate the possibilities and properties of the certificate system and show how such a process may be implemented can be found in ETSI GS ECI 002 [7].

4.4 ECI export groups and trust

One unique feature within the **ECI Ecosystem** is the ability to securely transfer purchased content between **Clients**, as long as certain technical and contractual prerequisites are met. The technical basis for this process is a special API and **Certificates** as specified in clause 9.7 of ETSI GS ECI 001-3 [3]. But since the transfer of protected content from one **Client** to another implies a transfer of responsibility and liability between stakeholders, it is recommended that the **Trust Authority** provides the necessary rules and requirements within the **Trust Environment** to facilitate the creation of export groups between different stakeholders.

4.5 Stakeholders of the ECI-Ecosystem

4.5.1 Definition

A stakeholder of an **ECI Ecosystem** is any legal entity that commits itself to the contractual framework of the ecosystem by entering a contract3ual relationship with the **Trust Authority**. In addition to the contractual relationship with the **TA**, stakeholders may also have relationships with each other. Any relationship of a stakeholder with a third party outside of the ecosystem (e.g. subcontractors) is subject to the contractual framework of the **ECI Ecosystem**.

The following key stakeholders exist in an **ECI Ecosystem:**

- Platform **Operator** / Service Provider