ETSI GS ECI 001-5-1 V1.1.1 (2017-07)

Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 5: The Advanced Security System; Sub-part 1: ECI specific functionalities

Disclaimer

The present document has been produced and approved by the Embedded Common Interface (ECI) 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-001-5-1

Keywords

authentication, CA, DRM, encryption, 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

List of Figures

List of Tables

Intellectual Property Rights

Essential patents

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 (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 5, sub-part 1 of a multi-part deliverable covering the ECI specific functionalities of an advanced security system, 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:

Sub-part 1: "ECI specific functionalities";

Sub-part 2: "Key Ladder Block".

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

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 PayTVoperators. It is also essential for consumers 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 be achieved by the implementation of interoperable CA and DRM mechanisms inside CPEs, based on an appropriate security architecture.

As part of a security architecture the present document defines a security processing system for the authentication and verification of protected media content and of software images to be processed inside an ECI-compliant CPE. The core of the security architecture is built by a **Key Ladder Block** that supports secure processing with secret keys, targeting of keys to specific chips and authentication of the origin of key material.

Clause 4 gives an overview about the system architecture, defines robustness rules to fight attacks and describes the relation between the elements of the security architecture, **ECI Host** and **ECI Clients**.

Clause 5 describes the applications the **Key Ladder Block** can be used for, together with the associated functions.

For proper operations, the security processing system needs information about the state of each loaded **ECI Client.** This state information, as some of it needs to be secret, is handled with the help of an advanced security slot. The **ECI Host** assigns to each **ECI Client** such a slot that needs to be protected against malicious modifications. The definition of a slot and its configuration for several operations like decrypting or exporting content is described in clause 6.

In an **ECI**-compliant CPE content can be decrypted, it can be forwarded to standard outputs if permitted and it can be re-encrypted for export. The usage of an advanced security slot for these operations is specified in clause 7.

A **Certificate Processing Subsystem** that is realized as a special function of an advanced security slot is responsible for the authentication of items. Clause 8 specifies the rules that are applied for authentication.

The **ECI** system uses a loader mechanism that permits **ECI Clients** to securely verify the version of the **ECI Host** and **ECI Client** credentials that are loaded so as to detect any known security issue. The loader mechanism relies on robustness principles that are described in clause 9.

Clause 10 contains timing constraints for the operations described in the present document.

1 Scope

The present document defines a robust security processing subsystem for **ECI** called the **Advanced Security System**. The **Advanced Security System** provides a secure basis for software elements to be authenticated and loaded, performs security computations and verifications, manages the encryption and decryption of content and the exchange of content with associated rights and obligations. As such the **Advanced Security System** is part of a "secure video path" as it is referred to in contemporary specifications. The **Advanced Security System** applies the **ECI Key Ladder Block [**5**]** to perform secure calculations.

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 001-5-2: "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 5: The Advanced Security System; Sub-part 2: Key Ladder Block".

[6] ISO/IEC 9899:2011: "Information technology - Programming languages - C".

[7] NIST FIPS PUB 180-4: "Secure Hash Standard (SHS)".

[8] NIST Special Publication 800-90A revision 1: "Recommendation for Random Number Generation Using Deterministic Random Bit Generators", June 2015.

NOTE: Available at http://dx.doi.org/10.6028/NIST.SP.800-90Ar1.

[9] ETSI ETR 289 (CSA1/2): "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems".

[10] ETSI TS 100 289 (V1.2.1) (CSA3): "Digital Video Broadcasting (DVB); Support for use of the DVB Scrambling Algorithm version 3 within digital broadcasting systems".

[11] ETSI TS 103 127 (V1.1.1) (CISSA): "Digital Video Broadcasting (DVB); Content Scrambling Algorithms for DVB-IPTV Services using MPEG2 Transport Streams".

[12] ISO/IEC 23001-7 (2016) (CENC): "Information technology - MPEG systems technologies - Part 7: Common encryption in ISO base media file format files".

[13] ISO/IEC 23009-4 (2013): "Information technology - Dynamic adaptive streaming over HTTP (DASH) - Part 4: Segment encryption and authentication".

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: "Using the DVB CSA algorithm" (licencing arrangement).

NOTE: Available at http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/csa-licences.

[i.2] ETSI: "Using the DVB CSA3 algorithm" (licensing conditions).

NOTE: Available at http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/csa3-licences.

[i.3] 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 System (AS System): robust secure processing system providing basic and highly secure processing functions for **ECI Clients**

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

AS-API: application programming interface between the **ECI Client** and its **ECI Host** permitting the **ECI Client** to exchange information with and perform operations on its **AS Slot**

Authentication Mechanism: Key Ladder Block function as defined in [5] that permits an **AS Slot** to provide secure key applications for purposes other than content decryption and encryption, like authentication

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: sequence of **Certificates** where the next **Certificate** can be authenticated by the public key of the preceding one

NOTE: Typically, in **ECI Certificates** are accompanied by a **Revocation List** that excludes **Certificates** that cannot be validated.

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

Content Properties (CP): properties of the content that provide information on rights and obligations associated with subsequent applications or transformations of the content, like usage rights information, selective output control and parental control information

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 and thus provides interoperability of CPE devices with respect to this system

ECI Client (Embedded CI Client): implementation of a CA/DRM client which is compliant with the **ECI** specifications

ECI Client Loader: functionality of the **ECI Host** that uses the AS system to exclusively provide the function , verify and install a new **ECI Client** software image in an **ECI** container of the **ECI Host**

ECI Host: hardware and software system of a CPE, which covers **ECI** related functionalities and has interfaces to an **ECI Client**

ECI Host Loader: CPE bootloading functionality that uses the AS system to exclusively provide the function to verify and install **ECI Host** software into a CPE

ECI Root Key: public key providing the origin of authentication for **ECI** certified entities and **Certificates**

entity: organization (e.g. manufacturer, **Operator** or **Security Vendor**) or real world item (e.g. **ECI Host**, **Platform Operation** or **ECI Client**) identified by an ID in a **Certificate**

export connection: relation between an **AS Slot** decrypting content and an **AS Slot** subsequently re-encrypting the decrypted content indicating such re-encryption is permitted

Key Ladder: function of the **Key Ladder Block** as defined in ETSI GS ECI 001-5-2 [5] 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 [5], 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 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**

micro server: ECI Client that encrypts such that it can only be decoded by the targeted **Micro Client** or group of **Micro Clients**

operator: organization providing **Platform Operations** that is enlisted with the **ECI TA** for signing the **ECI** eco system

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

Provisioning Server: server, typically located in a secure back office location, that provisions keys and other secure information to facilitate an encryption or decryption function through an **AS Slot**

revocation: status of exclusion of an entity in accordance with its enumeration in a **Revocation List**

Revocation List (RL): list of **Certificates** that have been revoked and therefore should no longer be used

robustness: property of the implementation of a specified secure function representing the effort and/or cost involved to compromise the security of the implemented secure function

root certificate: trusted certificate that is the origin of authentication for a chain of certificates

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

3.2 Abbreviations

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

ACF	Advanced Security Control Field
AD	Input of the Key Ladder Block
AES	Advanced Encryption Standard
AK	Authentication Key
API	Application Programming Interface
ARK	Advanced Security Random Key
AS	Advanced Security
CA	Conditional Access
CBC	Cypher Block Chaining
CENC	Common Encryption
CISSA	Common IPTV Software-oriented Scrambling Algorithm
CP	Content Properties
CPE	Customer Premises Equipment
CPS	Certificate Processing Subsystem
CSA	Common Scrambling Algorithm
CTR	Counter Mode
CW	Control Word
DRM	Digital Rights Management
EAC	Export Authorization Certificate
EAOC	Export Authorization Operator Certificate
ECI	Embedded Common Interface
ECM	Entitlement Control Message
EGC	Export Group Certificate
ERC	Export Revocation Certificate
ESC	Export System Certificate
LK	Link Key
MPEG	Moving Picture Experts Group
MSCSK	Micro Server Chipset Secret Key
PES	Packetized Elementary Stream
PO	Platform Operator
POC	Platform Operation Certificate
POPK	Platform Operation Public Key
REAOC	Revocation Export Authentication Operator Certificate
RFU	Reserved for Future Use
RK	Random Key
RL	Revocation List
SPK	Sender Public Key
TA	Trust Authority
TPEGC	Third Party Export Group Certificate
TS	MPEG 2 Transport Stream
URI	Usage Rights Information
XT	eXTension field

4 Principles

4.1 Overview

The present document is part of the Multipart ISG Group Specifications ECI 001, based on the **ECI** architecture ETSI GS ECI 001-1 [1] and **ECI** basic requirements ETSI GS ECI 001-2 [2].

Figure 4.1-1 presents the main principles of the **Advanced Security System**. The core of the **Advanced Security System** is formed by the **Key Ladder Block** as defined in [5], allowing secure processing with secret keys, targeting of keys to specific chips and authentication of the origin of key material.

The basis for loading images is embodied in the **loader core**. It uses the **Certificate Processing Subsystem** to verify the **ECI** status of **ECI Host** images, **ECI Client** images and Platform Operator (PO) credentials using a recent **ECI Root Key** and **ECI** root **Revocation List**. The version numbers of the **ECI Root Key** and **ECI** root **Revocation List** used by the **ECI Host** and other **ECI Clients** can be checked by **ECI Clients** that are loaded. These can refuse to descramble content on detecting unacceptable versions in accordance with the **ECI** revocation enforcement principle. Encrypted **ECI Client** images are decrypted upon loading.

Each **ECI Client** uses an Advanced Security slot. The **AS Slot** is identified by the **Platform Operation** Public Key of the **ECI Client.** The **ECI Host** ensures that **ECI Client** interactions through the **AS-API** are directed to the **AS Slot** allocated to that **ECI Client**. Each **AS Slot** is described by a slot state and a session state per encryption/decryption operation. The **AS Slot** can be used either for decryption purposes or for encryption purposes. The **AS Slot** session state also includes a configuration (config) defining the details of the operation and how the session state should be authenticated. The **ECI Client** provides the configuration information and input for other state information. The **Key Ladder Block** is used to authenticate SPK, POPK and the configuration information. The **AS Slot** can supply random numbers to selected **Key Ladder Block** inputs so as to generate random keys or to use as a nonce to ensure freshly computed **Key Ladder Block** inputs. This mechanism can be used to prevent replay of encrypted content and to ensure always online provisioning of an **AS Slot** by a **Provisioning Server**.

When decrypting content the **Content Properties** can be authenticated along with computing the control words, thus creating a strong link with the decrypted content. **Content Properties** are forwarded with the content to any standard output to ensure the proper setting of protection mechanisms for such an output. These properties are compared to those with which the content is re-encrypted on an **Export Connection**. An **Export Connection** is permitted only through the appropriate export/import **Certificate Chain**s. These are verified by the **Certificate Processing Subsystem** on behalf of the **AS Slot**. Standard outputs can be disabled through the output control mechanism.

Computed control words can be synchronized to MPEG Transport Stream formatted content using the alternating bit protocol. For this purpose the content processing system uses a double buffering mechanism with a current/next control word for stream processing.

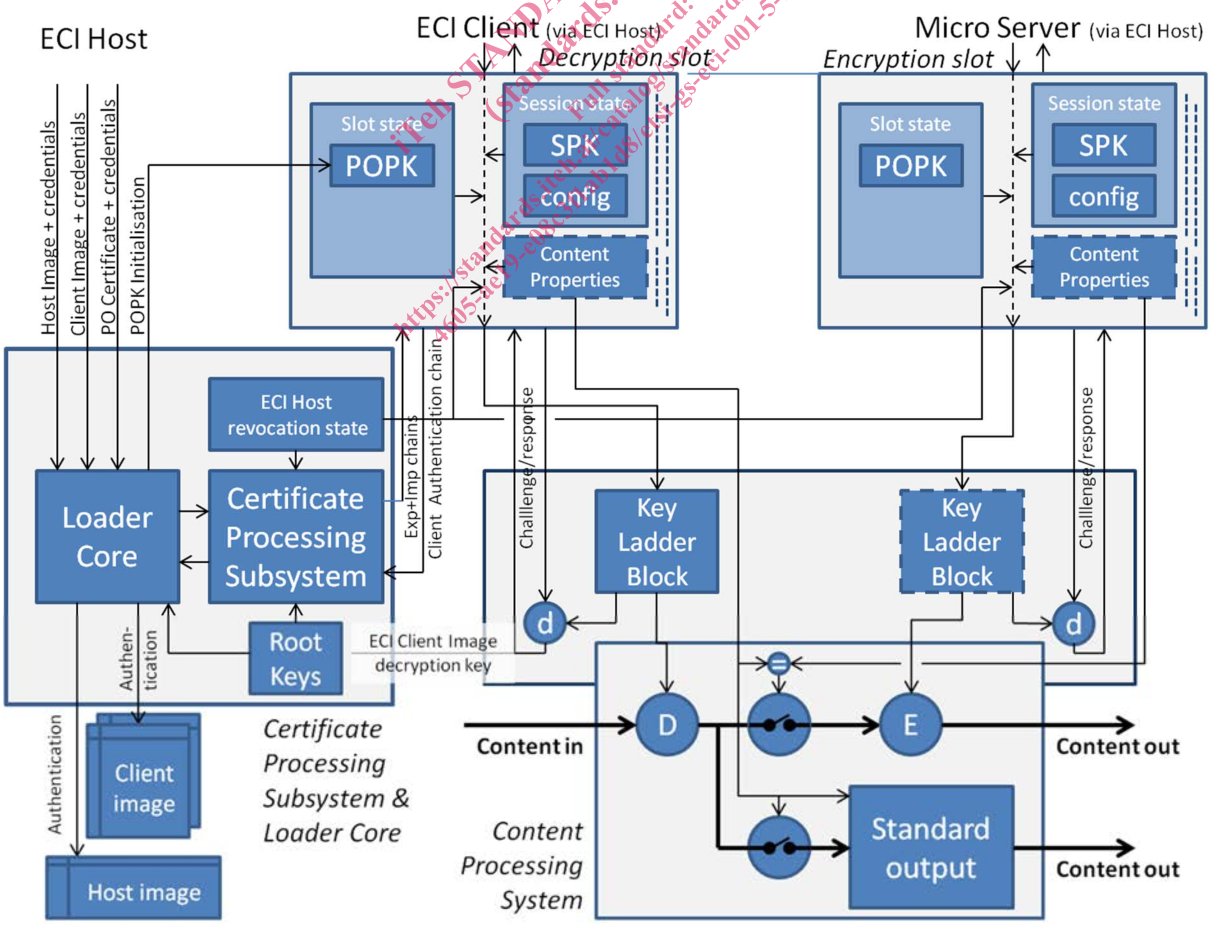

Figure 4.1-1: Block diagram of Advanced Security System