ETSI GS ECI 001-5-2 V1.1.1 (2017-07)

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

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-001-5-2

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/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

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 2 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".

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

A **content provider** encrypts their digital content and uses a **content protection system** in order to protect the content against unauthorized access. A consumer uses a **content receiver** to access protected content. To this end, the **content receiver** contains a chipset that implements one or more content decryption operations. A cryptographic key establishment protocol is used to secure the transport of content decryption keys from the **content protection system** to the chipset. The steps of the protocol that are implemented within the chipset are referred to as a key ladder in the present document. The present document specifies a key ladder for the key establishment protocol presented in [i.1].

The key ladder and the protocol may also be used to secure the transport of content encryption keys to the chipset. Such keys are required for use cases in which the chipset re-encrypts content. The chipset may implement one or more content encryption operations for this purpose. Personal video recording and exporting protected content to a different **content protection system** are typical examples of content re-encryption use cases. Content decryption keys and content encryption keys are both referred to as **control word**s throughout the present document.

The present document also specifies an authentication mechanism. This mechanism is closely related to the key ladder and may be used for entity authentication; in other words, this mechanism may be used to authenticate the chipset.

The key ladder and authentication mechanism specified in the present document are agnostic to both the **content protection system** and the **content provider**. This enables a **content provider** to use any compliant **content protection system**, and it enables a consumer to use the **content receiver** for accessing content of any **content provider** that uses a compliant **content protection system**.

A **certification authority** manages a public-key certificate of each chipset in the mechanisms specified in the present document. In particular, the **certification authority** distributes such certificates and certificate revocation information to **content provider**s that want to make use of the key ladder and/or the authentication mechanism. Next, the **content provider**s use the certificates and certificate revocation information as input to their compliant **content protection system**; as detailed later, the knowledge of the public key in the certificate of a chipset enables the **content protection system** to generate suitable input messages for the chipset's key ladder and authentication mechanism.

1 Scope

The present document specifies a key ladder block for implementation in a **content receiver**'s chipset. The key ladder block comprises a key ladder for securing the transport of **control word**s to the chipset and an authentication mechanism. The present document also specifies aspects of the personalization of a compliant chipset.

The present document is intended for use by chipset manufacturers.

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] IEEE Standards Association™: "Guidelines for Use Organizationally Unique Identifier (OUI) and Company ID (CID)".

NOTE: Available at https://standards.ieee.org/develop/regauth/tut/eui.pdf.

[2] RSA Laboratories: "PKCS #1 v2.2: RSA Cryptography Standard".

[3] NIST FIPS PUB 197: "Specification for the Advanced Encryption Standard (AES)".

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

[5] NIST SP 800-107 Revision 1: "Recommendation for Applications Using Approved Hash Algorithms".

[6] ISO/IEC 9797-1:2011: "Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher".

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] P. Roelse: "A new key establishment protocol and its application in pay-TV systems".

[i.2] ETSI TS 100 289: "Digital Video Broadcasting (DVB); Support for use of the DVB Scrambling Algorithm version 3 within digital broadcasting systems".

[i.3] ETSI TS 103 127: "Digital Video Broadcasting (DVB); Content Scrambling Algorithms for DVB-IPTV Services using MPEG2 Transport Streams".

[i.4] ATSC Standard A/70 Part 1:2010: "Conditional Access System for Terrestrial Broadcast".

[i.5] ISO/IEC 23001-7:2016: "Information technology -- MPEG systems technologies -- Part 7: Common encryption in ISO base media file format files".

[i.6] Radio, Film and Television Industrial Standard of the People's Republic of China GY/T 277 - 2014: "Technical Specification of Digital Rights Management for Internet Television".

NOTE: This reference is only available in Chinese.

3 Definitions and abbreviations

3.1 Definitions

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

certification authority: party that is responsible for managing public-key certificates

NOTE: A **certification authority** is trusted by all other parties in the system to perform operations associated with certificates.

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

content protection system: system that uses cryptographic techniques to manage access to digital content

NOTE: Typically, a **content protection system** is either a conditional access system or a digital rights management system.

content provider: party that distributes digital content to a **content receiver**

content receiver: device that is used to access digital content

NOTE: A **content receiver** contains a chipset with a **content descrambler**.

content descrambler: component in the chipset that is capable of decrypting content

NOTE: A **content descrambler** may also be capable of encrypting content (for the purpose of content re-encryption). In the present document, content encryption/decryption uses a **symmetric encryption scheme**. For MPEG-2 content, content encryption and decryption are also referred to as scrambling and descrambling, respectively.

control word: secret key used to encrypt and decrypt content

NOTE: In digital rights management systems, a **control word** is typically referred to as a content key.

cryptographic hash function: unkeyed cryptographic function that takes data of arbitrary size, referred to as the message, as input and produces an output data block of fixed size, referred to as the message digest

NOTE: Assumed properties of the **cryptographic hash function** in the present document are:

1) the **cryptographic hash function** behaves as a random function; and

2) the **cryptographic hash function** is second preimage resistant.

digital signature scheme: keyed asymmetric cryptographic scheme that is used to protect the authenticity of data

NOTE: A **digital signature scheme** consists of a key generation algorithm, a signature generation operation and a signature verification operation. Keys are generated as (secret/private key, public key) pairs. The data is signed using a secret/private key and the corresponding public key is used to verify the signature. The **digital signature scheme** specified in the present document is used to protect the authenticity of messages as defined in [i.1]; in particular, the scheme is not used to provide non-repudiation or source authentication in the present document.

message authentication code algorithm: keyed symmetric cryptographic algorithm that is used to protect the authenticity of data

NOTE: A **message authentication code algorithm** takes a message and a secret key as inputs, and produces an output data block referred to as the MAC. The **message authentication code algorithm** as specified in the present document is used to cryptographically bind a ciphertext message to its associated data; in particular, the algorithm is not used to provide source authentication in the present document.

public-key encryption scheme: keyed asymmetric cryptographic scheme that is used to protect the confidentiality of data

NOTE: A **public-key encryption scheme** consists of a key generation algorithm, an encryption operation and a decryption operation. Keys are generated as (public key, secret/private key) pairs. Data is encrypted using a public key and the data is recovered from the ciphertext using the corresponding secret/private key.

symmetric encryption scheme: keyed symmetric cryptographic scheme that is used to protect the confidentiality of data

NOTE: A **symmetric encryption scheme** consists of a key generation algorithm, an encryption operation and a decryption operation. The encryption and decryption operations of a **symmetric encryption scheme** use the same secret key as input.

3.2 Abbreviations

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

AES	Advanced Encryption Standard
AD1	Associated Data 1
AD2	Associated Data 2
AK	Authentication Key
ATSC	Advanced Television Systems Committee
CA/DRM	Conditional Access/Digital Rights Management
CID	Company IDentifier
CISSA	Common IPTV Software-oriented Scrambling Algorithm
CPU	Central Processing Unit
CSA	Common Scrambling Algorithm
CPK	Chipset Public Key
CSK	Chipset Secret/private Key
CW	Control Word
DVB	Digital Video Broadcasting
ECB	Electronic Code Book
ID	IDentity
Len	Length
LK	Link Key
MAC	Message Authentication Code
MK	MAC Key
MPEG	Moving Pictures Expert Group
OUI	Organizationally Unique Identifier
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SIM	Signed Input Message
SPK	Sender Public Key
SSK	Sender Secret/private Key
T	Tag
URI	Usage Rules Information