

# ITU-T

TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

## J.1015

(04/2020)

SERIES J: CABLE NETWORKS AND TRANSMISSION  
OF TELEVISION, SOUND PROGRAMME AND OTHER  
MULTIMEDIA SIGNALS

Conditional access and protection – Exchangeable  
embedded conditional access and digital rights  
management solutions

---

**Embedded common interface for exchangeable  
CA/DRM solutions: The advanced security  
system – Key ladder block**

Recommendation ITU-T J.1015



## Recommendation ITU-T J.1015

### Embedded common interface for exchangeable CA/DRM solutions: The advanced security system – Key ladder block

#### Summary

Recommendation ITU-T J.1015 is part of a series covering the advanced security system key ladder block for the embedded common interface for exchangeable conditional access/digital rights management (CA/DRM) solutions specification.

This ITU-T Recommendation is a transposition of ETSI standard [b-ETSI GS ECI 001-5-2] and is a result of collaboration between ITU-T SG9 and ETSI ISG ECI.

#### History

| Edition | Recommendation | Approval   | Study Group | Unique ID*                                                                   |
|---------|----------------|------------|-------------|------------------------------------------------------------------------------|
| 1.0     | ITU-T J.1015   | 2020-04-23 | 9           | <a href="http://handle.itu.int/11.1002/1000/11830-en">11.1002/1000/13576</a> |

#### Keywords

Conditional access, CA, digital rights management, DRM, swapping.

---

\* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2020

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

## Table of Contents

|    |                                                  | Page |
|----|--------------------------------------------------|------|
| 1  | Scope .....                                      | 1    |
| 2  | References.....                                  | 1    |
| 3  | Definitions .....                                | 1    |
|    | 3.1 Terms defined elsewhere .....                | 1    |
|    | 3.2 Terms defined in this Recommendation.....    | 1    |
| 4  | Abbreviations and acronyms .....                 | 2    |
| 5  | Conventions .....                                | 3    |
| 6  | Chipset-ID and chipset master key pair.....      | 3    |
| 7  | Key ladder.....                                  | 4    |
|    | 7.1 Overview .....                               | 4    |
|    | 7.2 Key ladder computations .....                | 6    |
|    | 7.3 Usage rules information .....                | 7    |
|    | 7.4 Additional key layers.....                   | 9    |
|    | 7.5 Associated data 2.....                       | 10   |
| 8  | Authentication mechanism .....                   | 11   |
|    | 8.1 Overview .....                               | 11   |
|    | 8.2 Authentication mechanism computations.....   | 12   |
| 9  | Data conversion primitives .....                 | 13   |
|    | 9.1 BS2OSP.....                                  | 13   |
|    | 9.2 OS2BSP.....                                  | 13   |
|    | 9.3 I2BSP.....                                   | 14   |
| 10 | Cryptographic operations .....                   | 14   |
|    | 10.1 Symmetric encryption scheme .....           | 14   |
|    | 10.2 Public-key encryption scheme.....           | 14   |
|    | 10.3 Digital signature scheme .....              | 14   |
|    | 10.4 Function h.....                             | 15   |
|    | 10.5 Message authentication code algorithm ..... | 16   |
|    | Appendix I – Areas for further development.....  | 17   |
|    | Bibliography.....                                | 19   |

## Introduction

This ITU-T Recommendation<sup>1</sup> is a transposition of ETSI standard [b-ETSI GS ECI 001-5-2] and is a result of a collaboration between ITU-T SG9 and ETSI ISG ECI.

The objective of this Recommendation is to facilitate interoperability and competition in electronic communications services and, in particular, in the market for broadcast and audio-visual devices. However other technologies are available and may also be appropriate and beneficial depending on the circumstances in Member States.

A content provider encrypts their digital content and uses a **content protection system**<sup>2</sup> 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 this Recommendation, which specifies a key ladder for the key establishment protocol presented in [b-ROEL].

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 words** (CWs) throughout this Recommendation.

This Recommendation 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 this Recommendation 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 this Recommendation. In particular, the **certification authority** distributes such certificates and certificate revocation information to **content providers** who wish to make use of the key ladder and/or the authentication mechanism. Next, **content providers** use the certificates and certificate revocation information as input to their compliant **content protection system**; as detailed in clause 7; knowledge of the public key in the certificate of a chipset enables the **content protection system** to generate suitable input messages for the key ladder and authentication mechanism of the chipset.

---

<sup>1</sup> Several areas for further development have been identified in Appendix I.

<sup>2</sup> The use of boldface in the text of this Recommendation indicates terms with definitions specific to the context of the embedded common interface that may differ from common use.

# Recommendation ITU-T J.1015

## Embedded common interface for exchangeable CA/DRM solutions: The advanced security system – Key ladder block

### 1 Scope

This Recommendation specifies a key ladder block for implementation in a chipset of a **content receiver**. The key ladder block comprises a key ladder to secure the transport of **control words** (CWs) to the chipset and an authentication mechanism. This Recommendation also specifies aspects of the personalization of a compliant chipset.

This Recommendation is intended for use by chipset manufacturers.

### 2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [ISO/IEC 9797-1] ISO/IEC 9797-1:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*.
- [IETF RFC 8017] IETF RFC 8017 (2016), *PKCS #1: RSA cryptography specifications version 2.2*.
- [NIST FIPS 180-4] NIST FIPS PUB 180-4 (2015), *Secure Hash Standard (SHS)*.
- [NIST FIPS 197] NIST FIPS PUB 197 (2001), *Specification for the Advanced Encryption Standard (AES)*.
- [NIST SP 800-107] NIST SP 800-107 Revision 1 (2012), *Recommendation for applications using approved hash algorithms*.

### 3 Definitions

#### 3.1 Terms defined elsewhere

None.

#### 3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

**3.2.1 certification authority:** Party that is responsible for managing public-key certificates in an embedded common interface (**ECI**) **ecosystem**. A certification authority is trusted by all other parties in the system to perform operations associated with certificates.

**3.2.2 chipset-ID:** Non-secret number that is used to identify a chipset within an **ECI ecosystem**.

**3.2.3 content protection system:** System in an **ECI ecosystem** that employs cryptographic techniques to manage access to content and services. The term may be interchanged frequently with

the alternate Service Protection system. Typical systems of this sort are either conditional access (CA) systems or digital rights management (DRM) systems.

**3.2.4 content provider:** Party that distributes digital content to a **content receiver** in an **ECI ecosystem**.

**3.2.5 content receiver:** Device that is used to access digital content within an **ECI ecosystem**. A **content receiver** contains a chipset with a **content descrambler**.

**3.2.6 content descrambler:** Component in the chipset of an **ECI ecosystem** that is capable of decrypting content. A content descrambler may also be capable of encrypting content (for the purpose of content re-encryption). In this Recommendation 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.

**3.2.7 control word:** Secret key used to encrypt and decrypt content within an **ECI ecosystem**. In digital rights management systems, a control word is typically referred to as a content key.

**3.2.8 cryptographic hash function:** Unkeyed cryptographic function in an **ECI ecosystem** 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. Assumed properties of the **cryptographic hash function** in this Recommendation are that the **cryptographic hash function** behaves as a random function and is second preimage resistant.

**3.2.9 digital signature scheme:** Keyed asymmetric cryptographic scheme that is used to protect the authenticity of data in an **ECI ecosystem**. 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 this Recommendation is used to protect the authenticity of messages as defined in [b-ROEL]; in particular, the scheme is not used to provide non-repudiation or source authentication in this Recommendation.

**3.2.10 ECI ecosystem:** A commercial operation consisting of a trust authority and several platforms and **ECI** – compliant customer premises equipment in the field.

**3.2.11 message authentication code algorithm:** Keyed symmetric cryptographic algorithm that is used to protect the authenticity of data in an **ECI ecosystem**. 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 this Recommendation is used to cryptographically bind a ciphertext message to its associated data; in particular, the algorithm is not used to provide source authentication in this Recommendation.

**3.2.12 public-key encryption scheme:** Keyed asymmetric cryptographic scheme that is used to protect the confidentiality of data in an **ECI ecosystem**. 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.

**3.2.13 symmetric encryption scheme:** Keyed symmetric cryptographic scheme that is used to protect the confidentiality of data in an **ECI ecosystem**. 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.

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES                      Advanced Encryption Standard

|       |                                                    |
|-------|----------------------------------------------------|
| AD1   | Associated Data 1                                  |
| AD2   | Associated Data 2                                  |
| AK    | Authentication Key                                 |
| CA    | Conditional Access                                 |
| 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                                       |
| DRM   | Digital Rights Management                          |
| DVB   | Digital Video Broadcasting                         |
| ECB   | Electronic Code Book                               |
| ECI   | Embedded Common Interface                          |
| ECP   | Enhanced Content Protection                        |
| ID    | Identifier                                         |
| LK    | Link Key                                           |
| MAC   | Message Authentication Code                        |
| MK    | MAC Key                                            |
| 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                            |

## 5 Conventions

The use of boldface in the text of this Recommendation indicates terms with definitions specific to the context of the embedded common interface that may differ from those in common use.

## 6 Chipset-ID and chipset master key pair

This clause specifies aspects of the personalization of a compliant chipset. Each compliant chipset is associated with a bit string identifier (ID) for the chipset, referred to as the **chipset-ID**, and a chipset master key pair.

A globally unique 64-bit **chipset-ID** shall be allocated to every compliant chipset. If the bits of **chipset-ID** are numbered 0 to 63 from left to right and if the  $i$ th bit ( $0 \leq i \leq 63$ ) is denoted by  $b_i$ , then  $(b_0, b_1, b_2, b_3)$  shall contain a registration authority ID. Each value of the registration authority ID shall be associated with at most one registration authority. The **chipset-ID** shall also contain a chipset manufacturer ID. The value of the registration authority ID and the chipset manufacturer ID of a compliant chipset's **chipset-ID** shall uniquely identify the chipset manufacturer that produced the