International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.1015.1

(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: Authentication of control word-usage rules information and associated data 1

Recommendation ITU-T J.1015.1

Recommendation ITU-T J.1015.1

Embedded common interface for exchangeable CA/DRM solutions: The advanced security system – Key ladder block: Authentication of control word-usage rules information and associated data 1

Summary

Recommendation ITU-T J.1015.1 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.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T J.1015.1	2020-04-23	9	11.1002/1000/13837

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 not 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/.

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	2
6	Authentication of control word-usage rules information and associated data 1	3
	6.1 Authentication of control word-usage rules information	4
	6.2 Authentication of associated data 1	4
Appendix I – Areas for further development		5
Bibliography		7

Introduction

The objective of this Recommendation[1] 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**[2] 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.

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 (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 provider**s who wish to make use of the key ladder and/or the authentication mechanism. Next, **content provider**s use the certificates and certificate revocation information as input to their compliant **content protection system**; as detailed in clause 7 of [ITU-T J.1015]; 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.

---

[1] Several areas for further development have been identified in Appendix I

[2] 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.1015.1

Embedded common interface for exchangeable CA/DRM solutions: The advanced security system – Key ladder block: Authentication of control word-usage rules information and associated data 1

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 word**s (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.

[ITU-T J.1015] Recommendation ITU-T J.1015 (2020), *Embedded common interface for exchangeable CA/DRM solutions; The advanced security system – Key ladder block.*

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.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AD1 Associated Data 1

AK Authentication Key

CA Conditional Access

CW Control Word

DRM Digital Rights Management

ECI Embedded Common Interface

ID Identifier

LK Link Key

SHA Secure Hash Algorithm

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 Authentication of control word-usage rules information and associated data 1

Concerning specification details in clause 7 of [ITU-T J.1015], several inputs to the key ladder block are specified, covering among others: CW-URI, AD1, τ_b, SPK-URI, SPK_i, encrypted LK as well as signed Chipset-ID. Some of these inputs, such as LK and Chipset-ID, are encrypted and applied with a digital signature scheme. On the other hand, CW-URI, AD1, τ_b, SPK-URI and SPK_i are delivered without any cryptographic schemes applied. The authentication of these inputs relies on the implicit authentication; in case that a non-authentic value for any of the key ladder inputs is provided, an invalid value of CW is computed and the content cannot be descrambled successfully.

It is possible that a sender can send SPK_i, SPK-URI and τ_b without any cryptographic schemes applied when considering the nature of input characteristics. Especially, τ_b can be verified using the Associated Data verification routines and thus applying an explicit authentication scheme is not required.

If it is required by service providers, they can introduce an additional explicit authentication method for CW-URI and AD1 inputs of the key ladder block. Such functionality could allow to achieve an increase of convenience for users as well as operational advantages for service providers.

This Recommendation specifies a way to apply such an authentication scheme to the CW-URI and AD1 when they are inputs to a key ladder block. This can be achieved by applying a digital signature scheme that is already used for Chipset-ID || E(SPK, LK) with SSK. Service operators can individually or collectively authenticate the CW-URI or AD1.

If service operators wish to protect the CW-URI or AD1, then the use of the scheme specified in this Recommendation is required.

See Figure 1.

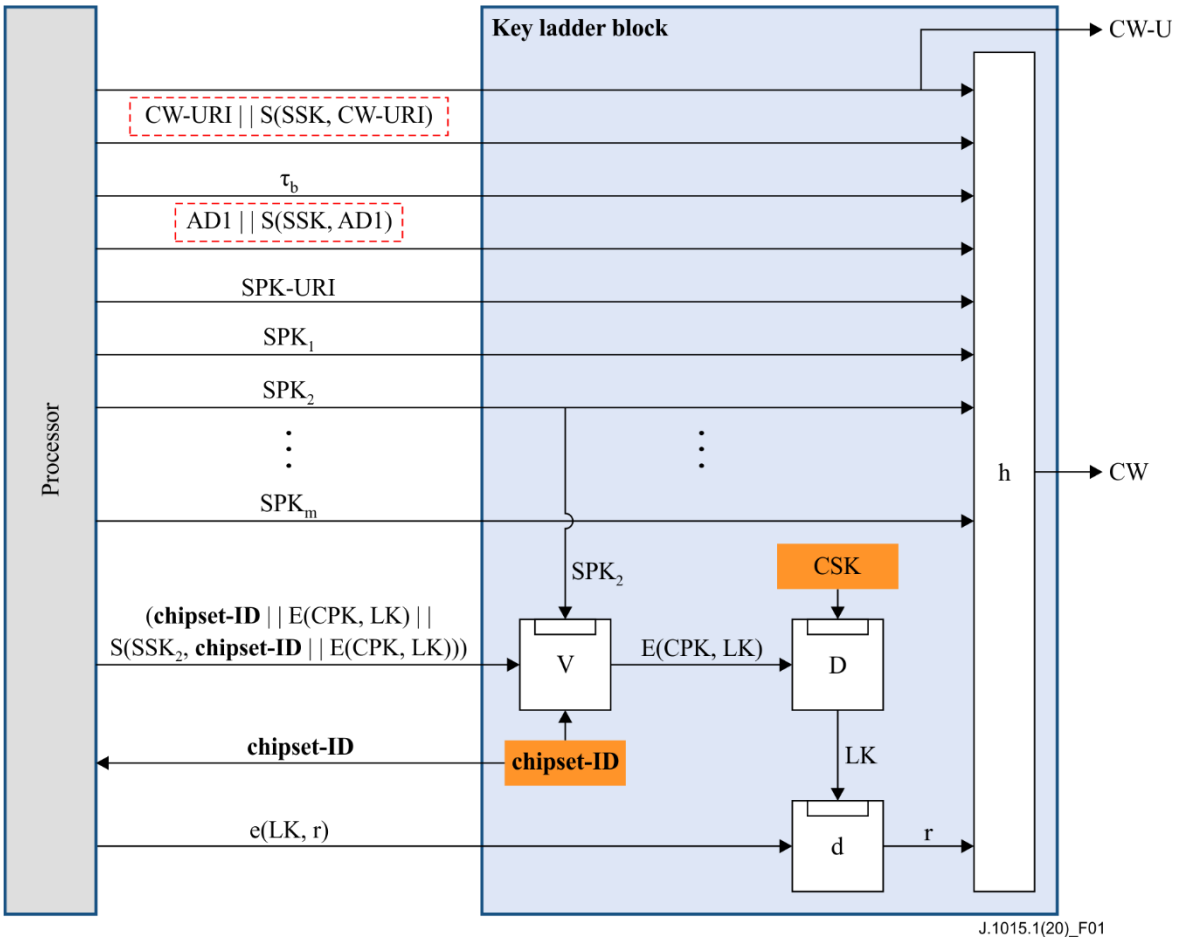

Figure 1 – Authentication of control word-usage rules information and associated data 1

6.1 Authentication of control word-usage rules information

Compute CW-URI ||signature (sender)

1) Sign the bit string CW-URI using SSK_i; the signature is denoted by S(SSK_i, CW-URI).
2) Append this signature to the bit string CW-URI

Retrieve CW-URI (key ladder block)

1) Check the length of the input data. If the length of the CW-URI is 64 bits, then the key ladder block shall perform the normal process specified in clause 7.3.1 of [ITU-T J.1015] and abort the CW-URI authentication process. Otherwise, i.e., if the length is more than 64 bits, then take the CW-URI authentication process and go to the next step.
2) Check whether the SPK-URI and the usage rule as specified in clause 7.3.2 of [ITU-T J.1015] allow V to use SPK_i to verify the signature. If this is not allowed, then the key ladder block shall abort the computations.
3) Use the received (CW-URI ||signature) and SPK_i to verify the signature. If the signature is invalid, then the key ladder block shall abort the computations.
4) Retrieve CW-URI.

6.2 Authentication of associated data 1

Compute AD1 ||signature (sender)

1) Sign the bit string AD1 using SSK_i; the signature is denoted by S(SSK_i, AD1).
2) Append this signature to the bit string AD1.

Retrieve associated data 1 (key ladder block)

1) Check the length of input data. If the length of the AD1 is 256 bits, then the key ladder block shall perform the normal process specified in clause 7.3.1 of [ITU-T J.1015] and abort the AD1 authentication process. Otherwise, i.e., if the length is more than 256 bits, then take the AD1 authentication process and go to the next step.
2) Check whether the SPK-URI and the usage rule as specified in clause 7.3.2 of [ITU-T J.1015] allow V to use SPK_i to verify the signature. If this is not allowed, then the key ladder block shall abort the computations.
3) Use the received (AD1 ||signature) and SPK_i to verify the signature. If the signature is invalid, then the key ladder block shall abort the computations.
4) Retrieve AD1.

Appendix I

Areas for further development

(This appendix does not form an integral part of this Recommendation.)

It has been identified that this Recommendation needs further development and validation for it to meet the requirements set out in [b-ITU-T J.1010], and that [b-ITU-T J.1010] needs to be updated to reflect the requirements of the MovieLabs Enhanced Content Protection (ECP) specification [b-ECP]. Recommendations [b-ITU-T J.1011], [b-ITU-T J.1012], [b-ITU-T J.1013], [b-ITU-T J.1014], [ITU-T J.1015] and ITU-T J.1015.1 should in the future be updated to reflect those updates to [b-ITU-T J.1010].

A number of ITU Member States, as well as stakeholders from a variety of industries – including manufacturers of devices and electronic components, owners and licensees of copyrighted content, providers of over-the-top (OTT) and linear television services, and providers of conditional access system (CAS) and digital rights management (DRM) solutions – based all around the world have expressed concern that the Embedded Common Interface (ECI) does not fully meet the requirements of ECP, nor wider industry content protection requirements.

More specifically, their concerns were raised in contributions to the ITU-T Study Group 9 (SG9) meeting (16-23 April 2020). Contributions from Israel, Australia, ITU-T Sector Member Samsung, and SG9 Associates Sky Group and MovieLabs proposed that a number of changes be included in the ECI Recommendations, but agreement on them was not reached. These items are inventoried in [b-SG9 Report 17 Ann.1].

They include proposals to:

1) Simplify the ECI system by reducing its scope;
2) Remove DRM;
3) Remove the re-encryption of content;
4) Remove software management;
5) Add APIs for secure storage and cryptographic operations;
6) Allow vendor-specific key ladders;
7) Use ITU-T J.1207 TEE requirements;
8) Include TEE implementation for VM;
9) Upgrade the strength of the cryptographic algorithms, e.g., using SHA-384;
10) Use standard certificates, like ITU-T X.509;
11) Reconsider communications between clients;
12) Perform additional liaisons with ETSI;
13) Perform additional peer-review;
14) Explore alternatives to the Trust Authority model;
15) Define further the technical aspects of ECI compliance and robustness rules;
16) Add requirements for diversity, e.g., address space randomization;
17) Add requirements on runtime integrity checking.

These proposals reflect that content protection and the threats of its compromise are continuously evolving. ECI was originally conceived nearly a decade before approval of this ITU-T Recommendation. Systems like ECI need to be assessed on a regular basis against the current state-of-the-art in both attack techniques and industry protection requirements.

Other mechanisms exist to enable interoperability. In particular for the DRM use case, most internet video services have deployed other solutions to provide interoperability and to address their needs.

Further clarity is important as many Member States regard ITU standards as influential sources of guidance for the development of their markets and industries. The list of concerns ensures ECI's implementation in their domestic markets can involve a full appreciation of implications of this ITU-T Recommendation and ensure that the issues are considered when legislation, regulation or market need requiring consumer digital television equipment to be interoperable are being considered. It also ensures that technology equipment manufacturers, who may prefer to use a unique set of requirements or other standards to design the products, can consider these issues in developing products for different markets.

Bibliography

[b-ITU-T J.1010] Recommendation ITU-T J.1010 (2016), *Embedded common interface for exchangeable CA/DRM solutions; Use cases and requirements*.

[b-ITU-T J.1011] Recommendation ITU-T J.1011 (2016), *Embedded common interface for exchangeable CA/DRM solutions; Architecture, definitions and overview*.

[b-ITU-T J.1012] Recommendation ITU-T J.1012 (2020), *Embedded common interface for exchangeable CA/DRM solutions; CA/DRM container, loader, interfaces, revocation*.

[b-ITU-T J.1013] Recommendation ITU-T J.1013 (2020), *Embedded common interface for exchangeable CA/DRM solutions; The virtual machine*.

[b-ITU-T J.1014] Recommendation ITU-T J.1014 (2020), *Embedded common interface for exchangeable CA/DRM solutions; Advanced security – ECI-specific functionalities*.

[b-SG9 Report 17 Ann.1] ITU-T SG9 meeting report, SG9-R17-Annex 1 (2020), Annex 1 to Report 17 of the SG9 fully virtual meeting held 16-23 April 2020. https://www.itu.int/md/T17-SG09-R-0017/en

[b-ECP] MovieLabs Specification for Enhanced Content Protection – Version 1.2 Available at: https://movielabs.com/ngvideo/MovieLabs_ECP_Spec_v1.2.pdf

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	**Cable networks and transmission of television, sound programme and other multimedia signals**
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020