International Telecommunication Union

ITU-T J.1026

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(07/2019)

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

Conditional access and protection – Downloadable conditional access system for unidirectional networks

Downloadable conditional access system for unidirectional networks – Requirements

Recommendation ITU-T J.1026

Recommendation ITU-T J.1026

Downloadable conditional access system for unidirectional networks – Requirements

Summary

Recommendation ITU-T J.1026 specifies requirements for one-way downloadable conditional access system (DCAS) for unidirectional networks. One-way DCAS protects broadcast content/services and controls consumer entitlements like traditional conditional access (CA) systems, and enables a terminal, such as a set-top-box (STB), to adapt to a new CA system by downloading and installing the new CA system's client without changing the hardware. In particular, one-way DCAS can fully work in unidirectional cable TV networks and other unidirectional networks such as satellite TV networks.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T J.1026	2019-07-29	9	11.1002/1000/13972

Keywords

CA, downloadable, unidirectional networks.

* 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

Introduction

The present Recommendation is part 1 of a multi-part deliverable covering the requirements for a one-way downloadable conditional access system (DCAS) specification, as identified below:

Part 1: "Requirements"

Part 2: "System architecture"

Part 3: "Terminal system".

Recommendation ITU-T J.1026

Downloadable conditional access system for unidirectional networks - Requirements

1 Scope

The object of this Recommendation is a set of basic requirements for a one-way downloadable conditional access system for unidirectional networks. This Recommendation is one in a series of Recommendations, specifying the whole downloadable conditional access system for unidirectional networks. The other parts of one-way DCAS Recommendations include the specification of system architecture and related security mechanisms for one-way DCAS as defined in [ITU-T J.1027] and the terminal specification for one-way DCAS as defined in [ITU-T J.1028].

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.1027] Recommendation ITU-T J.1027 (2019), *Downloadable conditional access system for unidirectional networks – System architecture*.

[ITU-T J.1028] Recommendation ITU-T J.1028 (2019), *Downloadable conditional access system for unidirectional networks – Terminal system.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 descrambling [b-ITU-T J.93]: The processes of reversing the scrambling functions (see "scrambling") to yield usable pictures, sound and data services.

3.1.2 entitlement control messages (ECMs) [b-ITU-T J.290]: An ECM is an encrypted message that contains access criteria to various service tiers and a control word (CW).

3.1.3 entitlement management messages (EMMs) [b-ITU-T J.290]: The EMM contains the actual authorization data and shall be sent in a secure method to each CPE device.

3.1.4 scrambling [b-ITU-T J.93]: The process of using an encryption function to render television and data signals unusable to unauthorized parties.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 bootloader: The program for initiating hardware and loading software after a receiver boots up.

3.2.2 challenge-response: The process in which one-way downloadable conditional access system (DCAS) client software performs calculations using a key ladder of a terminal security chipset through a one-way DCAS manager.

3.2.3 Downloadable conditional access system (DCAS): A conditional access (CA) system that supports all the features of legacy conditional access and provides a CA-neutral mechanism to securely download CA client image and switch CA terminals without changing hardware through either a broadcasting or a two-way network.

3.2.4 hardware security module (HSM): A security chipset capable of control word processing, access authorizing and secure storage, etc., which supports hardware security enhancement of a unidirectional receiver.

3.2.5 hash value: The result calculated on any value by using hashing algorithms.

3.2.6 key ladder: A structured multi-level key mechanism that ensures the secure transport of control word.

3.2.7 nonce: Random or repetitive data sent from a one-way downloadable conditional access system (DCAS) headend system for challenge-response.

3.2.8 one-way DCAS: A downloadable conditional access system (DCAS) operated especially in a one-way network.

3.2.9 one-way DCAS App: One-way downloadable conditional access system (DCAS) application running on the terminal software platform. After a terminal device is deployed in field, this application can be upgraded or replaced through online pushing or other methods.

3.2.10 one-way DCAS trusted App: One-way downloadable conditional access system (DCAS) trusted application running in the trusted execution environment of terminal device. After a terminal device is deployed in field, this application can be upgraded or replaced through online pushing or other methods.

3.2.11 one-way DCAS client software: Terminal application implemented by one-way downloadable conditional access system (DCAS) App and one-way DCAS trusted App working together on the terminal software platform.

3.2.12 one-way DCAS client software data: Data that needs to be saved or updated when one-way downloadable conditional access system (DCAS) client software runs, which includes conditional access (CA) authorization information, CA private data, positioning information, etc.

3.2.13 one-way DCAS manager: Software module responsible for registering downloadable conditional access system (DCAS) client software, supporting information interaction between one-way DCAS App and one-way DCAS trusted App, as well as receiving and forwarding one-way DCAS entitlement control and management messages.

3.2.14 root key: The key used for the first level of a key ladder.

3.2.15 security chipset key de-obfuscation: Algorithm used to de-obfuscate encrypted security chipset key.

3.2.16 transport stream filtering: A filtering mechanism that is used to extract data matching filter rules from a transport stream.

3.2.17 terminal security chipset: A stream processing chipset with security functions such as secure key deriving and key ladder processing, etc.

3.2.18 terminal software platform: A software platform running on a receiver, integrated with various hardware drivers, having various terminal application APIs, capable of downloading and running terminal applications according to specified security requirements and providing a secure execution environment for terminal application.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
App	Application
CA	Conditional Access
CAJS	Conditional Access Javascript
CAT	Conditional Access Table
CATA	Conditional Access Trusted Application
CAS	Conditional Access System
ChipID	Chipset Identification
CPU	Central Processing Unit
CREEK	Crypto-toolkit Re-encryption Key
CSA	Common Scrambling Algorithm
CW	Control Word
DCAS	Downloadable Conditional Access System
DVB	Digital Video Broadcasting
ECM	Entitlement Control Message
ECW	Encrypted Control Word
EMM	Entitlement Management Message
EPG	Electronic Program Guide
ESCK	Encrypted Security Chipset Key
GP	Global Platform
HSM	Hardware Security Module
HSMID	Hardware Security Module Identification
KDF	Key Derivation Function
KLAD	Key Ladder
NVM	Non-Volatile Memory
OTP	One Time Programmable
PairK	Pairing Key
PID	Packet Identification
RNG	Random Number Generator
SAC	Secure Authenticated Channel
SCK	Security chipset Key
SCKv	Security chipset Key Vendor
Seedv	Seed Vendor
SI	Service Information
SMK	Secret Mask Key
SoC	System on Chip
TEE	Trusted Execution Environment

Vendor SysID Vendor System Identification

5 Conventions

In this Recommendation:

The keywords **"is required to"** indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords **"is recommended"** indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords **"is prohibited from"** indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords **"can optionally"** indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this document and its annexes, the words *shall*, *shall not*, *should*, and *may* sometimes appear, in which case they are to be interpreted, respectively, as *is required to*, *is prohibited from*, *is recommended*, and *can optionally*. The appearance of such phrases or keywords in an appendix or in material explicitly marked as *informative* are to be interpreted as having no normative intent.

6 Requirements for one-way downloadable conditional access system for unidirectional networks

6.1 Security challenges in a one-way TV environment

A one-way broadcast environment poses particular security challenges stemming from the inability to communicate with and thereby gain knowledge of the devices that are active on the network.

Around the world, CA vendors have typically dealt with the security needs of one-way TV systems by relying on a smart card. There are three primary security elements in the smart card:

- Secure processing in the smart-card central processing unit (CPU);
- Secure storage via memory on the smart card. This storage cannot be easily read or written to by an unauthorized party;
- Renewability both via software downloading to the smart card and the ability to replace the smart card in the field with a newer, more-secure smart card.

The currently proposed system provides two of above three elements: the trusted execution environment (TEE) provides an environment for secure processing, and since the conditional access trusted application (CATA) and the conditional access Javascript (CAJS) are downloadable over the network, a high degree of renewability is also achieved. Besides, the root-key derivation block in the key ladder (KLAD) also provides a means of renewability if a given CA vendor's keys are exposed.

However, there is no means for secure storage in the current architecture. The only non-volatile storage available is either a memory chip or a hard disk, both of which are prone to physical attacks by a hacker attempting to read or write sensitive data.

6.2 System security requirements

The design is intended to meet several goals:

- Renewability: In the event that one CA vendor is breached, it shall be possible to replace it with a different CA vendor via a simple software download to the STB;
- Openness: All CA vendors shall have equal access to the security blocks in the STB;
- Security: The system shall be secure enough to withstand the increasingly sophisticated attacks in today's world.

6.3 General requirements

6.3.1 One-way DCAS headend system requirements

One-way DCAS headend shall comply with the following requirements:

a) Shall be able to implement entitlement management message (EMM) transmission via unidirectional channel;

b) Shall be able to generate root key and key ladder for terminal security chipset and hardware security module (HSM);

c) The EMM and ECM generated by one-way DCAS headend shall comply with one-way DCAS key mechanism.

6.3.2 Security chipset key serializing module requirements

Used on production lines, the security chipset key serializing module is responsible for serializing necessary information needed for deriving root key, such as ChipID, encrypted security chipset key (ESCK), BL_KEY0, etc., to terminal security chipset. The requirements are:

a) Shall support import and export of necessary information such as ChipID, ESCK and BL_KEY0, etc.;

b) Shall support secure storage of sensitive data;

c) Shall have sufficient security and anti-attack ability.

6.3.3 One-way DCAS client software requirements

One-way DCAS client software is a downloadable and replaceable terminal software module that controls users in their receiving of digital broadcast services, including video, audio, and data. It shall meet the following requirements:

a) Shall implement standard application programming interface (API) interacting with terminal software platform;

b) Shall implement CA functionality with terminal software platform;

c) Shall support using of terminal HSM;

d) Shall have sufficient security and anti-attack ability.

6.3.4 Terminal security chipset requirements

A terminal security chipset is a chipset integrated to a receiver, to implement key ladder decryption and stream processing. For a functional diagram of a terminal security chipset please refer to Figure 2 of [ITU-T J.1028]. The requirements are:

a) Shall contain OTP area and support secure storage of important data such as ChipID and ESCK, etc.;

b) Shall support de-obfuscation of root secure key SCK;

c) Shall support the generation of final root key K3 by derivation;

d) Shall support key ladder mechanism, to ensure secure transmission of control word (CW) within chipset.

e) Shall include audio/video decoding module;

f) Shall include a descrambling module compliant with the digital video broadcasting DVB standard;

g) Shall support signature verification over bootloader;

h) Shall support TEE.

6.3.5 HSM requirements

Independent to terminal security chipset, HSM is a security chipset integrated to receiver providing algorithm tools and secure storage services. HSM basic architecture is shown in Figure 6 of [ITU-T J.1028]. The requirements are:

a) Shall support activation, more details see Appendix I;

b) Shall contain random number generator (RNG);

c) Shall support key ladder mechanism;

d) Shall participate CW operation;

e) Shall support data signature and verification;

f) Shall support data encryption and decryption;

g) Shall support secure authenticated channel (SAC);

h) Shall contain lockable storage area, which becomes read-only area after lock;

i) Shall contain CA storage area and support SAC access control.

6.3.6 Terminal software platform requirements

Terminal software platform is a common collection of software running on a terminal security chipset. The requirements are:

a) Shall support download, update and replacement of one-way DCAS client software;

b) Shall provide standard API for one-way DCAS client software;

c) Shall ensure the integrity, reliability, and security in downloading, startup and running of one-way DCAS client software;

d) Shall support TEE.

6.3.7 Terminal security requirements

One-way DCAS terminal shall comply with the following requirements to efficiently protect the security of a one-way DCAS system:

a) Shall be able to ensure confidentiality and integrity of secret keys, certificates and software pertaining to this standard;

b) Shall be able to ensure decrypted content is not disclosed, intercepted, re-distributed or duplicated;

c) Shall be able to ensure hardware integrity that terminal security chipset and HSM cannot be easily removed or replaced;

d) Shall be able to ensure software/hardware interface cannot be easily damaged or circumvented.

Appendix I

Activation of a HSM of a one-way DCAS

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

This appendix describes the activation process of a hardware security module (HSM) of a one-way DCAS. It is important to note that this is the only moment two-way communication is needed during the activation of a HSM. After this moment two-way communication is never needed for one-way DCAS.

By activation, a HSM can register itself into a specific CA headend and retrieve dedicated CA information and keys. After that, the HSM can work with the corresponding CAS. Activation flow includes 3 basic operations:

a) HSM generates an activation request message and delivers it to headend;

b) HSM receives and processes the primary activation message from headend;

c) HSM receives and processes the auxiliary activation message from headend.

One-way DCAS client software makes a request to the HSM, as the response, the ctivation request message will be generated and signed by the HSM. It includes a group of information of the client device and is signed by the private key serialized inside the HSM. The activation request message is then passed to the headend for further processing via any available two-way communication. For example, the activation request message is shown using QR code when the terminal is first powered on and the QR code is scanned by a mobile device and sent to headend.

There is only one moment that one-way DCAS needs two-way communication, which is the time when the activation request message is delivered to the headend. Activation of the HSM depends on receiving two distinct messages: the primary activation message and the auxiliary data message. Until a valid pair has been received, the HSM is not activated and will not provide secure storage or cryptographic services.

The primary activation message is sent by the CA headend to the STB and one-way DCAS client software then passes it to the HSM. The primary activation message contains critical key material for "pairing" the HSM to the host STB, as well as key material to be used for CW processing. The primary activation message also contains information (e.g., location information), which is used by the main CA application on the STB.

After the primary activation message has been received, validated and processed, the HSM is still not active, it waits for a matching auxiliary data message. A "matching" auxiliary data message is the one with an identical timestamp to the primary activation message and the same vendor ID. Once a valid pair of messages has been received and processed, the HSM is activated and begins to provide its essential security services. Prior to the receiving of a valid pair, requests to use these services are denied by the HSM.

One-way DCAS is designed to be renewable, the pair of activation messages may be received more than once.

Receiving the primary activation message is not dependent on having previously issued an activation request message. There are use-cases where a primary activation message is sent from the headend without an activation request message being generated.

Bibliography

[b-ITU-T J.93] Recommendation ITU-T J.93 (1998), *Requirements for conditional access in the secondary distribution of digital television on cable television systems.*

[b-ITU-T J.290] Recommendation ITU-T J.290 (2006), *Next generation set-top box core architecture*.

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, 2019