International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.1026

(01/2022)

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 a one-way downloadable conditional access system (DCAS) for unidirectional networks. A one-way DCAS protects broadcast content or 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 client of a CA system without changing the hardware. In particular, one-way DCAS can fully work in unidirectional cable television (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
2.0	ITU-T J.1026	2022-01-13	9	11.1002/1000/14868

Keywords

Downloadable conditional access system, DCAS, Requirements.

* 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

This Recommendation is the first in a series specifying requirements, system architecture and the terminal system, respectively, for a one-way downloadable conditional access system:

Part 1: "Requirements" [ITU-T J.1026]

Part 2: "System architecture" [ITU-T J.1027]

Part 3: "Terminal system" [ITU-T J.1028]

Recommendation ITU-T J.1026

Downloadable conditional access system for unidirectional networks - Requirements

1 Scope

This Recommendation specifies a set of basic requirements for a one-way downloadable conditional access system (DCAS) for unidirectional networks. This Recommendation is the first in a series specifying the whole one-way DCAS for unidirectional networks. [ITU-T J.1027] specifies a related system architecture and [ITU-T J.1028] specifies a related terminal system.

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 (2022), *Downloadable conditional access system for unidirectional networks – System architecture.*

[ITU-T J.1028] Recommendation ITU-T J.1028 (2022), *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 process of reversing the scrambling function (see "scrambling") to yield usable pictures, sound and data services.

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

3.1.3 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: A program for initiating hardware and loading software after a receiver boots up.

3.2.2 challenge-response: The process in which one-way 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 entitlement management message (EMM): A message containing actual authorization data that requires sending by a secure method to each piece of customer premises equipment.

NOTE – Based on [b-ITU-T J.290].

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

3.2.6 key ladder (KLAD): A structured multi-level key mechanism that ensures secure transport of a control word.

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

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

3.2.9 one-way DCAS client software: A terminal application composed of a one-way DCAS App and a one-way DCAS trusted App through joint work with the support of the DCAS manager embedded in the terminal software platform.

3.2.10 one-way DCAS manager: A software component of a terminal software platform responsible for registering one-way DCAS client software, supporting information exchange between the one-way DCAS App and the one-way DCAS trusted App, as well as receiving and forwarding one-way downloadable conditional access system (DCAS) entitlement control and management messages.

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

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

3.2.13 terminal security chipset: A stream-processing chipset with security functions such as secure key deriving and key ladder processing.

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

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

App Application

CA Conditional Access

CW Control Word

DCAS Downloadable Conditional Access System

ECM Entitlement Control Message

EMM Entitlement Management Message

HSM Hardware Security Module

KLAD Key Ladder

QR Quick Response

SAC Secure Authenticated Channel

STB Set-Top Box

TEE Trusted Execution Environment

TV Television

5 Conventions

In this Recommendation:

The phrase **"is required to"** indicates a requirement that must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The phrase **"is recommended"** indicates a requirement that is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

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

The phrase **"can optionally"** indicates an optional requirement that 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 or service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this Recommendation, 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 television 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;
- 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 one that is newer and more secure.

The currently proposed system provides two of the three elements in the preceding list: secure processing is done in the trusted execution environment (TEE), and since the CA trusted application and the CA application are downloadable over the network, a high degree of renewability is also achieved. Furthermore, the root-key derivation block in the key ladder (KLAD) also provides a means of renewability if the keys of a given CA vendor 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:

- robustness: a one-way DCAS shall be secure enough and have hardware level of security in order to withstand the increasingly sophisticated attacks now and in the future;
- renewability: the currently deployed DCAS shall be able to be replaced by a newly deployed DCAS via a simple software download to the terminals;
- neutrality: the security mechanism embedded in the terminal security chipset shall be equally accessed by the currently deployed DCAS and newly deployed DCAS.

6.3 General requirements

6.3.1 One-way DCAS headend system requirements

A one-way DCAS headend shall comply with the following requirements:

a) to implement EMM transmission via unidirectional channel;

b) to generate security data that can be used to derive a root key within a KLAD for a terminal security chipset and hardware security module (HSM);

c) for the EMM and ECM generated by a one-way DCAS headend to comply with the one-way DCAS key mechanism.

6.3.2 One-way DCAS client software requirements

One-way DCAS client software shall meet the following requirements:

a) Shall implement standard application programming interfaces (APIs) to interact with terminal software platform;

b) Shall implement CA functionality with a terminal software platform;

c) Shall support use of a terminal HSM;

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

6.3.3 Terminal security chipset requirements

The terminal security chipset shall meet the following requirements:

a) Shall contain a one time programmable area and support secure storage of security data;

b) Shall support de-obfuscation of the security chipset key;

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

d) Shall support a KLAD mechanism, to ensure secure transmission of control words (CWs) within a chipset;

e) Shall include an audio and video decoding module;

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

g) Shall support signature verification over bootloader;

h) Shall support a TEE.

6.3.4 Hardware security module requirements

The HSM shall meet the following requirements:

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

b) Shall contain a random number generator;

c) Shall support a KLAD mechanism;

d) Shall participate in CW operation;

e) Shall support data signature and verification;

f) Shall support data encryption and decryption;

g) Shall support a secure authenticated channel (SAC);

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

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

6.3.5 Terminal software platform requirements

The terminal software platform shall meet the following requirements:

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

b) Shall provide standard APIs for the 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 a TEE.

6.3.6 Terminal security requirements

A 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 Recommendation;

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

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

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

Appendix I

Activation of a hardware security module of a one-way downloadable conditional access system

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

This appendix describes the activation process of an HSM of a one-way DCAS. Note that this is the only moment two-way communication is needed during the activation of an HSM, after which it is never needed for one-way DCAS.

By activation, an HSM can register itself in a specific CA headend and retrieve dedicated CA information and keys. After that, the HSM can work with the corresponding conditional access system. Activation flow includes three basic operations. An HSM:

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

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

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

One-way DCAS client software makes a request to the HSM; as the response, the activation request message is generated and signed by the HSM. The message includes information about 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 a quick-response (QR) code when the terminal is first powered up when the QR code is scanned by a mobile device and sent to the headend.

There is only one moment when one-way DCAS needs two-way communication, which is the time 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 does not provide secure storage or cryptographic services.

The primary activation message is sent by the CA headend to the set-top box (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) that 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 one with an identical timestamp to that of 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 reception 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 in which 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, 2022