International Telecommunication Union

ITU-T J.1031

(05/2020)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

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

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

Downloadable conditional access system for bidirectional networks – Requirements

Recommendation ITU-T J.1031

Recommendation ITU-T J.1031

Downloadable conditional access system for bidirectional network – Requirements

Summary

Recommendation ITU-T J.1031 specifies requirements for the two-way downloadable conditional access system (DCAS) for bidirectional networks. A two-way DCAS protects broadcast content/services and controls consumer entitlements in the same way as what traditional conditional access (CA) systems do, and enables a two-way terminal device, such as a set-top-box (STB), to adapt to a new CA system by downloading and installing the new CA system's client software without changing hardware. In particular, a two-way DCAS can work in bidirectional cable TV networks and other bidirectional networks such as broadband cable networks.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T J.1031	2020-05-29	9	11.1002/1000/14280

Keywords

Bidirectional network, CA, downloadable.

* 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

This Recommendation document is Part 1 of a multi-part deliverable covering the requirements for two-way DCAS specification, as identified below:

Part 1: Requirements;

Part 2: System architecture;

Part 3: The terminal.

Recommendation ITU-T J.1031

Downloadable conditional access system for bidirectional networks – Requirements

1 Scope

The object of this Recommendation is a set of basic requirements for a two-way downloadable conditional access system (DCAS) for bidirectional networks. This Recommendation is the first in a series of Recommendations, specifying the whole two-way DCAS for bidirectional networks. The other Recommendations for the two-way DCAS include the specification of the system architecture and related security mechanism for a two-way DCAS, and the terminal specification for a two-way DCAS.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 bootloader [b-ITU-T J.1026]: The program for initiating hardware and loading software after a receiver boots up.

3.1.2 DCAS [b-ITU-T J.1026]: A conditional access system that supports all the features of legacy conditional access (CA), and provides a CA-neutral mechanism to securely download CA client image and switch CA terminals without changing hardware through either a broadcasting or two-way network.

3.1.3 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).

3.1.4 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.

3.1.5 key ladder (KLAD) [b-ITU-T J.1026]: A structured multi-level key mechanism that ensures secure transport of control word.

3.1.6 root key [b-ITU-T J.1026]: The key used for the first level of a key ladder.

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

3.1.8 security chipset key de-obfuscation [b-ITU-T J.1026]: Algorithm used to de-obfuscate encrypted security chipset key.

3.1.9 terminal security chipset [b-ITU-T J.1026]: A stream processing chipset with security functions such as secure key deriving and key ladder processing, etc.

3.1.10 terminal software platform [b-ITU-T J.1026]: A software platform running on a receiver such as a terminal device, 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 trusted execution environment for terminal application.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 descrambling: The processes of reversing the scrambling functions (see "scrambling") to yield usable pictures, sound and data services.

NOTE – Based on the definition given in [b-ITU-T J.93].

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

3.2.3 two-way DCAS App: A two-way downloadable conditional access system (DCAS) application running on the terminal software platform of a receiver having two network functionalities. After a terminal device is deployed in the field, this application can be upgraded or replaced through online downloading or other methods.

3.2.4 two-way DCAS client software: A terminal application implemented by a two-way DCAS App and a two-way DCAS trusted App working together on the terminal software platform.

3.2.5 two-way DCAS trusted App: A two-way DCAS trusted application running in the trusted execution environment of a terminal software platform on a terminal device. After a terminal device is deployed in field, this application can be upgraded or replaced through online downloading or other methods.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
CA	Conditional Access
CAT	Conditional Access Table
CATA	Conditional Access Trusted Application
CAJS	Conditional Access JavaScript
CAS	Conditional Access System
ChipID	Chipset Identification
CPU	Central Process Unit
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
KDF	Key Derivation Function
KLAD	Key Ladder
NVM	Non-Volatile Memory
OTP	One-Time Programmable
PID	Packet Identification
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 Recommendation 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 Security challenges for a two-way DCAS in a two-way TV network

Figure 1 shows the two-way DCAS functional diagram consisting of a two-way DCAS headend and a two-way terminal.

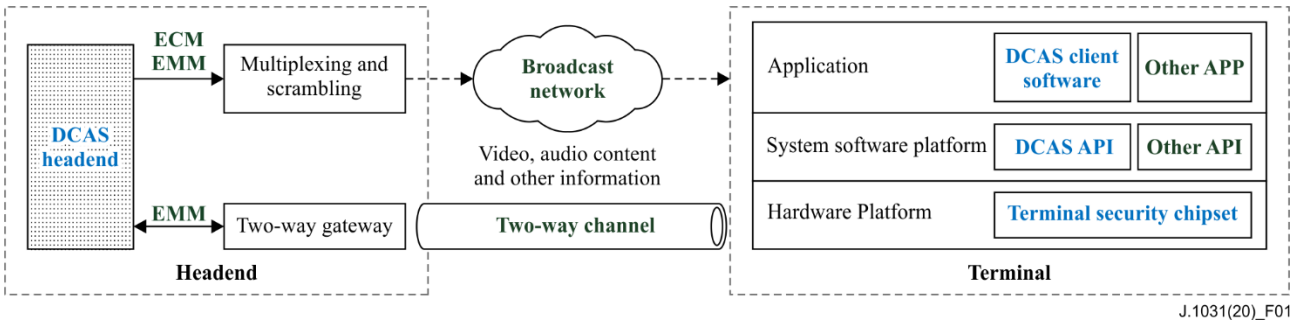

Figure 1 – Functional diagram of two-way DCAS

According to Figure 1, the two-way DCAS shall address its major security challenges, which include the authentication between the two-way DCAS headend and related two-way DCAS terminals, the data transmission security and the network stability.

The security challenge for the authentication between the two-way DCAS headend and related two-way DCAS terminals in a two-way DCAS is due to the fact that the two-way DCAS terminal has to face typical man-in-middle security problem, as the security data such as EMM are stored in the two-way DCAS headend, and two-way DCAS terminals have to retrieve the security data from the authentic DCAS headend. One of the solutions is for a two-way DCAS to use key ladder and challenge-response mechanism embedded in the terminal security chipset.

The security challenge for the transmission of security data is due to the fact that these data, when transmitted in a two-way network, may be leaked or tampered. One of solutions is to sign and encrypt these data with the security mechanism embedded in the security chipset.

The security challenge for network stability is due to the fact that in order for a two-way DCAS to perform normally when the two-way TV network is unstable and two-way DCAS terminals cannot obtain the necessary security data stored in a two-way DCAS headend in time, certain security data has to be maintained in related two-way DCAS terminals. One of the solutions is for two-way DCAS terminals to use the terminal software platform's trusted execution environment that supports the secure storage together with properly short-lived EMMs which are EMMs having properly short-lived authorizing rights.

7 Overall security requirements

A two-way DCAS shall meet following requirements:

- Robustness: A two-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.

8 General requirements

8.1 Headend requirements

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

a) Shall be able to implement EMM transmission via unidirectional or bidirectional network;

b) Shall be able to generate security data which can be used to derive a root key within a key ladder for a terminal security chipset;

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

8.2 Terminal requirements

A two-way DCAS terminal shall comply with the following requirements to efficiently protect the security of a two-way DCAS:

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

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 the terminal security chipset cannot be easily removed or replaced;

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

8.2.1 Terminal security chipset requirements

The terminal security chipset shall meet the following requirements:

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

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

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

d) Shall support key ladder mechanism, to ensure secure transmission of control words (CWs) within the 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 trusted execution environment (TEE).

8.2.2 Terminal software platform requirements

The terminal software platform shall meet the following requirements:

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

b) Shall provide standard application programming interfaces (APIs) for the two-way DCAS client software;

c) Shall ensure the integrity, reliability, and security about downloading, startup and running of the two-way DCAS client software.

8.2.3 Two-way DCAS client software requirements

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

a) Shall implement standard APIs to interact with the terminal software platform;

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

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

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*.

[b-ITU-T J.1026] Recommendation ITU-T J.1026 (2019), *Downloadable conditional access system for unidirectional networks – Requirements*.

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