International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.1032

(08/2020)

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 – System architecture

Recommendation ITU-T J.1032

Recommendation ITU-T J.1032

Downloadable conditional access system for bidirectional networks – System architecture

Summary

Recommendation ITU-T J.1032 specifies a system architecture 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 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 a 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.1032	2020-08-13	9	11.1002/1000/14355

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

The present Recommendation is part 2 of a multi-part deliverable covering the system architecture for two-way downloadable conditional access system (DCAS) specification, as identified below:

Part 1: "Requirements"

Part 2: "System architecture"

Part 3: "The terminal"

Recommendation ITU-T J.1032

Downloadable conditional access system for bidirectional networks – System architecture

1 Scope

The object of this Recommendation is to specify the system architecture and related security mechanisms of a two-way downloadable conditional access system (DCAS) for bidirectional networks. This Recommendation is one in a series of two-way DCAS Recommendations, specifying the whole downloadable conditional access system for bidirectional networks. The other parts of the two-way DCAS Recommendations include the requirement for two-way DCAS as defined in [ITU-T J.1031] and the terminal specification for two-way DCAS as defined in [ITU-T J.1033].

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.1031] Recommendation ITU-T J.1031 (2020), *Downloadable conditional access system for bidirectional networks – Requirements.*

[ITU-T J.1033] Recommendation ITU-T J.1033 (2020), *Downloadable conditional access system for bidirectional networks – The terminal.*

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.

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

3.1.6 downloadable conditional access system (DCAS) [b-ITU-T J.1026]: 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 two-way network.

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

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

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, 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.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

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

NOTE – Definition adapted from [b-ITU-T J.1026].

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

NOTE – Definition adapted from [b-ITU-T J.1026].

3.2.3 secure data management platform (SDMP): Platform that generates and manages some basic and root information, such as keys and IDs used in a downloadable conditional access system (DCAS), including information to DCAS headend to terminal security chipset.

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

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

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

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

3.2.8 two-way DCAS client software data: Data that needs to be saved or updated when two-way DCAS client software runs, which include CA authorization information, CA private data, positioning information, etc.

3.2.9 two-way DCAS manager: Software module responsible for registering two-way DCAS client software, supporting information interaction between two-way DCAS App and two-way DCAS trusted App, as well as receiving and forwarding two-way DCAS entitlement control and management messages.

3.2.10 two-way DCAS SDMP: The two-way secure data management platform (SDMP) performs key and security data generation and serialization for the terminal security chipset as well as maintains and manages the keys and security data which are generated by itself.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
CA	Conditional Access
CAS	Conditional Access System
CATA	Conditional Access Trusted Application
ChipID	Chipset Identification
CPE	Customer Premises Equipment
CW	Control Word
DCAS	Downloadable Conditional Access System
ECM	Entitlement Control Message
ECMG	Entitlement Control Message Generator
ECW	Encrypted Control Word
EMM	Entitlement Management Message
EMMG	Entitlement Management Message Generator
ESCK	Encrypted Security chipset Key
PID	Packet Identification
SCK	Security chipset Key
SCKv	Security chipset Key Vendor
SDMP	Secure Data Management Platform
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 Two-way DCAS architecture

6.1 System architecture

A two-way downloadable conditional access system (DCAS) is a complete end-to-end service protection system, which has all entitlement control and management functions of a traditional conditional access (CA) system. A two-way DCAS can coexist with traditional CA systems and is highly flexible. By downloading the two-way DCAS client software, a terminal can switch flexibly among different two-way DCASes. This is to say, a terminal will no longer need to change hardware or upgrade its entire software to support CA headend from different CA system vendors and different versions of the CA headend from the same CA system vendor.

A two-way DCAS consists of the headend, the terminal and the secure data management system (SDMP). Figure 1 shows the two-way DCAS architecture defined in [b-GY/T 255].

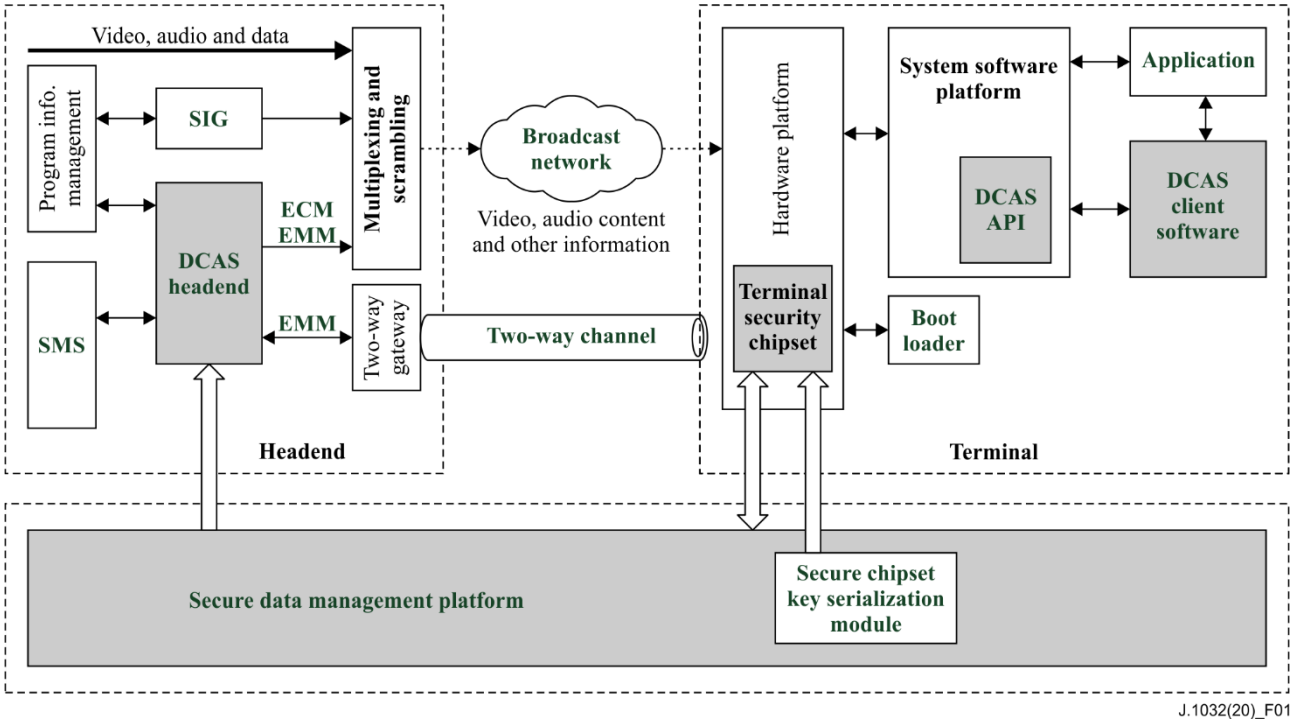

Figure 1 – The two-way DCAS architecture

The two-way DCAS headend scrambles the input audio/video stream and sends conditional access system (CAS) messages via a broadcast channel or bidirectional channel to implement encrypted transmission of services. The two-way DCAS headend includes mainly entitlement control message generator (ECMG), entitlement management message generator (EMMG), key management and other modules, etc.

The two-way DCAS terminal validates a user's entitlement and descrambles protected services to implement conditional access of services. The terminal software platform can securely download, update, and replace the DCAS client software. The two-way DCAS terminal mainly includes a terminal security chipset, the terminal software platform which includes DCAS API and DCAS manager, and DCAS client software which includes two-way DCAS App and two-way DCAS trusted App.

The two-way DCAS SDMP generates and manages keys used in two-way DCAS, provides two-way DCAS headend with necessary information such as SCKv and Vendor_SysID, and provides a terminal security chipset by using a key serializing module with the necessary information such as ChipID, encrypted security chipset key (ESCK), and BL_KEY0, etc. Clause 6.1.1 and clause 6.1.3

of this Recommendation describe how a two-way DCAS SDMP works with a two-way DCAS headend and two-way DCAS terminals. The two-way DCAS SDMP provides the above mentioned information to both a two-way DCAS headend and related two-way DCAS terminals before the deployment of the two-way headend and related terminals, but it does not participate in any operation and involve in any activity of both the two-way headend and related two-way terminals once they are deployed.

6.1.1 The two-way DCAS headend

Figure 2 shows the functional framework of a two-way DCAS headend also defined in [b-GY/T 255].

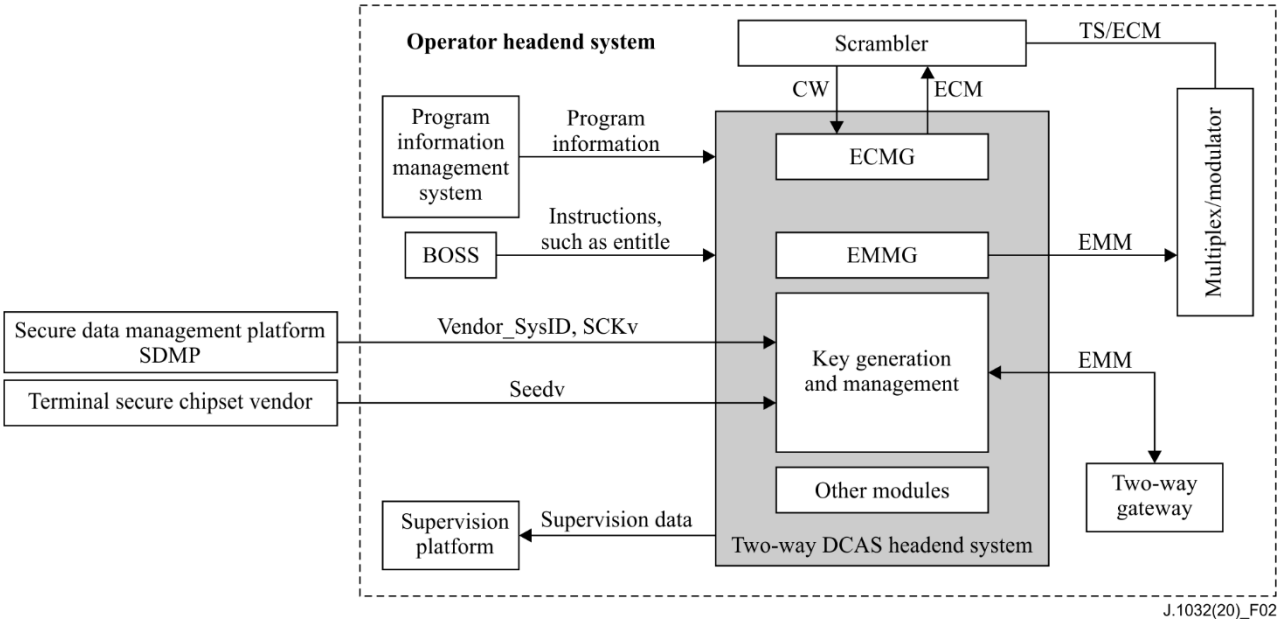

Figure 2 – The functional framework of a two-way DCAS headend

A two-way DCAS headend consists of following main modules:

a) ECMG

ECMG connects to the scrambler, to receive a CW sent from the scrambler, generates the ECM, and returns it to scrambler.

b) EMMG

EMMG generates the entitlement management message (EMM), and sends the EMM via the multiplex's interface.

c) Secure key generation and management

To generate and manage root key and key ladder keys according to the information of the terminal security chipset vendor and the terminal security chipset provided by SDMP. The generation and management of key ladder keys are handled by the two-way DCAS headend itself.

d) Other modules

The two-way DCAS headend also includes other modules such as a network management module, a monitoring module and external interfaces, etc.

6.1.2 The two-way DCAS terminal

Figure 3 shows the functional framework of a two-way DCAS terminal also defined in [b-GY/T 255].

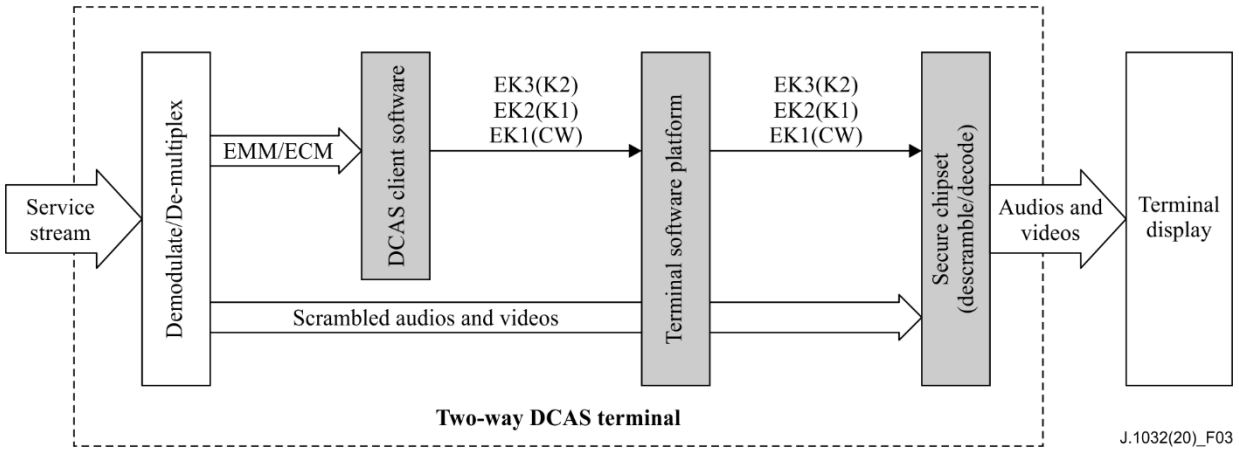

Figure 3 – The functional framework for the two-way DCAS terminal

The two-way DCAS terminal includes the following main modules:

a) The two-way DCAS client software

The two-way DCAS client software is an application running on the two-way DCAS terminal software platform, and communicating with the two-way DCAS terminal software platform and other modules via a standard API. A two-way DCAS client software can be downloaded, updated, and replaced through the two-way DCAS terminal software platform by the receiver. A two-way DCAS client software is responsible for analyzing and processing the EMM data, and providing the key ladder data to the terminal security chipset.

b) The terminal software platform

The terminal software platform is a public software running on the terminal security chipset hardware. It provides a standard API required by the two-way DCAS client software to ensure integrity, reliability, and security of the downloading, booting and running of the two-way DCAS client software.

c) The terminal security chipset

The terminal security chipset receives key ladder keys and scrambled service streams, decrypts key ladder keys, descrambles scrambled service streams and decodes them to output decoded videos and audios.

6.1.3 The two-way DCAS SDMP

The two-way SDMP performs key and security data generation and serialization for the terminal security chipset, and maintains and manages the keys and security data which are generated by itself. The two-way SDMP has following main functions:

a) Key generation for a terminal security chipset

To generate security information of a terminal security chipset: generate files for ChipID and other security data, and send them in a secure way to a security chipset key serializing module as well as write the security information data into the terminal security chipset.

To generate an intermediate key for root key derivation: generate ChipID and SCKv file, and send them in a secure way to a two-way DCAS of a CA vendor to generate root key K3.

To generate the bootloader verification key for a terminal security chipset: generate BL_KEY0 key pairs, send the terminal security chipset vendor the public key to be written into the terminal security chipset.

b) Key serialization for a terminal security chipset

The SDMP writes the terminal security chipset, the secure information data such as ChipID and ESCK, etc., which are saved in the key serializing module by using the key serializing module installed on chipset vendor's production line with appropriate secure transfer protocols.

c) Signing the bootup verification key

Uses BL_KEY0 to sign the public key of BL_KEY1 held by BL_KEY1's holder, so that terminal security chipset can verify BL_KEY1's holder.

6.2 Security mechanism

6.2.1 Key mechanism

6.2.1.1 Key model

The key mechanisms of a two-way DCAS include the root key derivation mechanism, the key ladder mechanism, the secure data management mechanism and the service scrambling/descrambling mechanism. Figure 4 shows the two-way DCAS key model also defined in [b-GY/T 255].

The root key derivation mechanism enables a terminal security chipset to derive a personalized root key in real time by using its built-in root key derivation module; a secure data management mechanism uses data separation security management to safeguard the security of root key generation management; the root key derivation mechanism works closely with the secure data management mechanism, so that different two-way DCAS systems can securely derive their personalized root key respectively by using the root key derivation module based on the same terminal security chipset.

The key ladder mechanism protects the control word during its transmission, by using the root key derived from the root key derivation mechanism as the first level key to encrypt/decrypt the CW level by level, the root key and other keys in the key ladder are also used for challenge-response function. Contents are protected by a service scrambling/descrambling mechanism implemented with the control word output from key ladder.

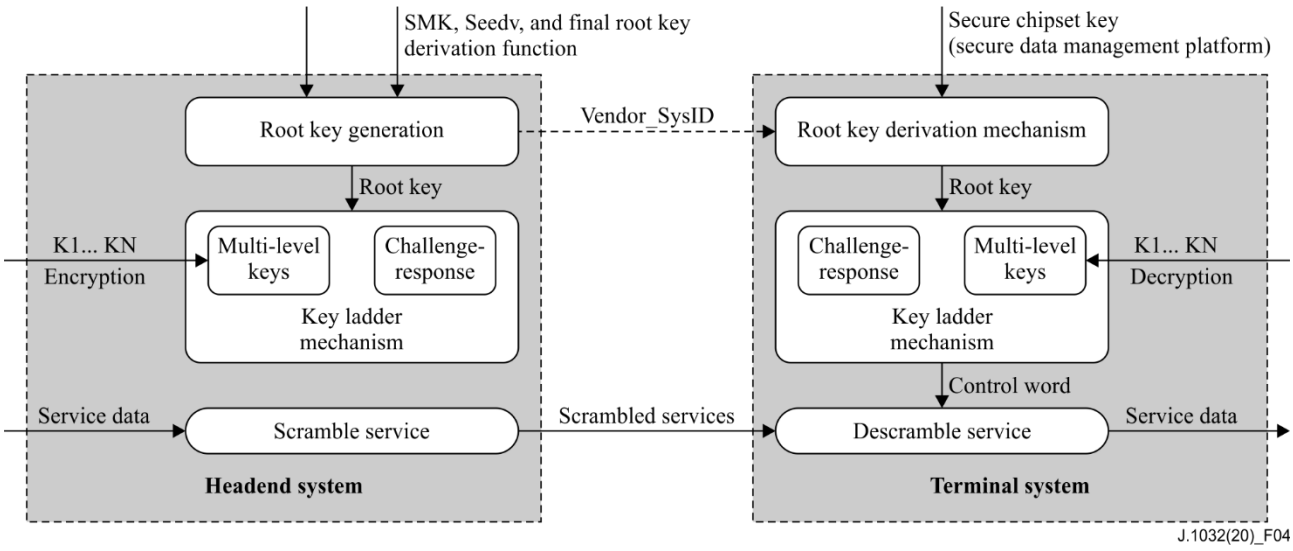

Figure 4 – Key model

6.2.1.2 Root key derivation mechanism

The mechanism of root key derivation includes headend root key derivation and terminal root key derivation:

a) Generation of headend root key

Two-way DCAS headend uses necessary data and related algorithms provided by the terminal security chipset vendor and SDMP, to derive the root key for each terminal security chipset of every terminal before using the chipset.

b) Derivation of terminal root key

Two-way DCAS terminal uses DCAS client software to provide necessary information for the terminal security chipset, and derive the root key with the root key derivation module embedded in the terminal security chipset.

6.2.1.3 Key ladder mechanism

The key ladder mechanism includes a multi-level key function and challenge-response function.

The multi-level key function is used to decrypt CW level by level, to ensure the security of CW when being used and transferred.

The challenge-response function is used to send a value to a certain level of the key ladder for computation, and then the terminal security chipset computes the result with a specified algorithm.

6.2.1.4 Secure data management

The secure data management mechanism is the core component of the two-way DCAS key mechanism. It utilizes the method of separation management of the secure information including those required in headend and terminal root key derivation, separately managed by SDMP, the CA vendor and chipset vendor, to ensure the security and neutrality of the two-way DCAS system.

6.2.1.5 Service scrambling/descrambling mechanism

The service scrambling/descrambling mechanism implements secure delivery of service data from headend to terminal.

6.2.2 Two-way DCAS terminal hardware security mechanism

Two-way DCAS terminal hardware security mechanism is secured by the terminal security chipset. Part 3 [ITU-T J.1033] describes detailed technical requirements.

6.2.3 Two-way DCAS terminal software security mechanism

6.2.3.1 Chain of trust

A two-way DCAS client software security mechanism is established on a bottom-to-top chain of trust, in which digital signature technology is used to establish a chain of trust from terminal security chipset to boot loader, terminal software platform, and two-way DCAS client software. Only if the signature of each link of the chain is validated can the following link be launched. In addition to passing the signature verification, two-way DCAS client software shall have a run-time data security protection mechanism.

The terminal security chipset performs a data source reliability check and integrity check on the boot loader before the boot loader runs.

The boot loader performs a data source reliability verification and integrity check on the terminal software platform locally before the terminal software platform runs.

The terminal software platform performs a data source reliability check and integrity check on the two-way DCAS client software before the two-way DCAS client software runs.

6.2.3.2 Two-way DCAS client software data security

The two-way DCAS client software data security shall be ensured if it is stored in the terminal.

6.2.3.3 Terminal trusted execution environment

The two-way DCAS client trusted application runs in a trusted execution environment (TEE). A TEE provides a trusted computing environment for two-way DCAS based on the secure trusted hardware and secure trusted software.

Secure trusted hardware provides a trusted secure hardware environment by using functions such as secure memory access control, secure bus connection, secure interruption, secure clock, secure random number and secure key ladder processing module, etc.

Secure trusted software includes secure OS and TEE HAL, which implements functions such as memory isolation, anti-rollback, secure storage, conditional access trusted application (CATA) dynamic loading by using memory management, secure time, task scheduling, interruption, task communications, encryption/decryption, and provides trusted secure software environment.

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.*

[b-GY/T 255] GY/T 255 (2012), *Technical specification of downloadable conditional access system.*

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