International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.1027

(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 – System architecture

Recommendation ITU-T J.1027

Recommendation ITU-T J.1027

Downloadable conditional access system for unidirectional networks – System architecture

Summary

Recommendation ITU-T J.1027 specifies a system architecture for a 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 hardware changing. 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.1027	2019-07-29	9	11.1002/1000/13973

Keywords

CA, conditional access system, downloadable, unidirectional network.

* 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 of one-way DCAS specification, as identified below:

Part 1: "Requirements"

Part 2: "System architecture"

Part 3: "The terminal"

Recommendation ITU-T J.1027

Downloadable conditional access system for unidirectional networks – System architecture

1 Scope

The object of this Recommendation is to specify the system architecture and related security mechanisms of a one-way downloadable conditional access system for unidirectional networks. This Recommendation is one in a series of one-way DCAS Recommendations, specifying the whole downloadable conditional access system for unidirectional networks. The other parts of the one-way DCAS Recommendations include the requirements for one-way DCAS as defined in [ITU-T J.1026] and the terminal system 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.1026] Recommendation ITU-T J.1026 (2019), *Downloadable conditional access system for unidirectional networks – Requirements.*

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

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

3.2.3 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 field, this application can be upgraded or replaced through online pushing or other methods.

3.2.4 one-way DCAS trusted App: A one-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.

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

3.2.6 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, and which includes conditional access (CA) authorization information, CA private data, positioning information, etc.

3.2.7 one-way DCAS manager: A software module responsible for registering one-way 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.

3.2.8 security chipset key de-obfuscation: An algorithm used to de-obfuscate an encrypted security chipset key.

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

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

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

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

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

3.2.14 challenge-response: The process in which one-way DCAS client software performs calculations using the key ladder of a terminal security chipset through a one-way DCAS manager.

3.2.15 nonce: A random or repetitive data sent from a one-way DCAS headend system for challenge-response.

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

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 a terminal application.

3.2.19 secure data management platform (SDMP): A secure data management platform generates and manages some basic and root information, such as keys and IDs used in a DCAS, including information to the DCAS headend, to the terminal security chipset and to the HSM.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
App	Application
CA	Conditional Access
CAT	Conditional Access Table
CATA	Conditional Access Trusted Application
CAJS	Conditional Access Javascript
CAS	Conditional Access System
ChipID	Chipset Identification
CPE	Customer Premises Equipment
CPU	Central Process 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
ECMG	Entitlement Control Message Generator
ECW	Encrypted Control Word
EMM	Entitlement Management Message
EMMG	Entitlement Management Message Generator
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
OS	Operating System
OTP	One Time Programmable
PairK	Pairing Key
PID	Packet Identification
SAC	Secure Authenticated Channel
SCK	Security chipset Key
SCKv	Security Chipset Key Vendor

SDMP	Secure Data Management Platform
Seedv	Seed Vendor
SI	Service Information
SIG	Service Information Generator
SMK	Secret Mask Key
SMS	Subscriber Management System
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 One-way DCAS architecture

6.1 One-way DCAS architecture

One-way DCAS is a complete end-to-end service protection system, which has all the entitlement control and management functions of a traditional CA system. One-way DCAS can coexist with traditional CA systems and is highly flexible. By downloading one-way DCAS client software, a receiver can switch flexibly among different one-way DCAS systems, which means a receiver will no longer need hardware changes or an entire software upgrade to support CA headend systems from different CA system vendors and support different versions of CA headend system from the same CA system vendor.

One-way DCAS consists of a headend, a terminal and a secure data management platform (SDMP). Figure 1 shows the one-way DCAS architecture.

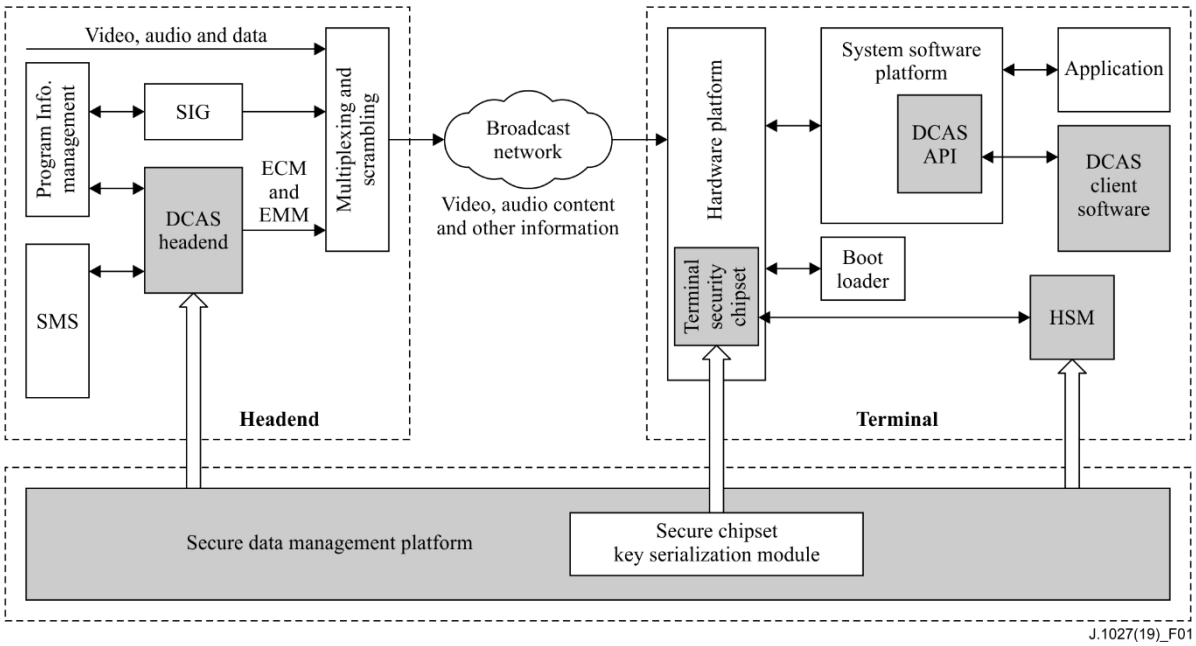

Figure 1 – One-way DCAS architecture

A one-way DCAS headend scrambles the input audio/video stream and sends conditional access system (CAS) messages via a broadcast channel to implement encrypted transmission of services and entitlement control and management, which is the fundamental function of the various one-way DCAS functions. One-way DCAS headend includes mainly an entitlement control message generator (ECMG), an entitlement management message generator (EMMG), key management and other modules, etc.

A one-way DCAS terminal validates user's entitlement and descrambles protected services to implement conditional access of services. A terminal software platform can safely download, update and replace DCAS client software. The one-way DCAS terminal mainly includes a terminal security chipset, a hardware security module (HSM), DCAS client software and DCAS API of the terminal software platform.

A one-way DCAS SDMP generates and manages keys used in a one-way DCAS, provides necessary information such as the security chipset key vendor (SCKv) and vendor system identification (Vendor_SysID) to a one-way DCAS headend, provides necessary information such as ChipID, encrypted security chipset key (ESCK), and BL_KEY0, etc., to a terminal security chipset using a key serializing module and provides aroot certificate to a HSM (please refer to clause 6.1.1 and clause 6.1.3). The one-way DCAS SDMP provides the information before the deployment of headend and terminals and is not involved in the system running after the deployment.

6.1.1 One-way DCAS headend system

Figure 2 shows the functional structure of a one-way DCAS headend.

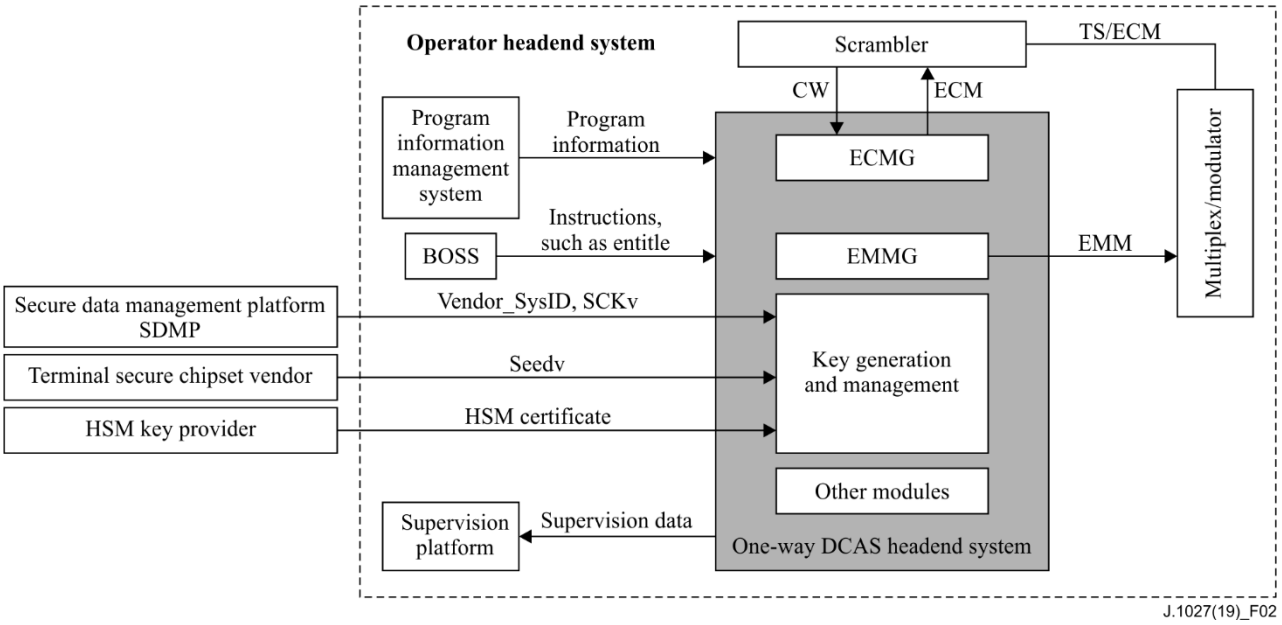

Figure 2 – The functional structure of one-way DCAS headend

The main modules are:

a) ECMG

The ECMG connects to a scrambler, to receive a control word (CW) sent from the scrambler, generates an entitlement control message (ECM), and returns it to scrambler.

b) EMMG

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

c) Secure key generation and management

To generate and manage the root key and key ladder keys according to the information of the terminal security chipset provided by the secure data management platform (SDMP) and terminal security chipset vendor. To encrypt and sign HSM related data according to HSM information provided by the SDMP and HSM key providers. Generation and management of KLAD keys are handled by the one-way DCAS headend system itself.

c) Other modules

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

6.1.2 One-way DCAS terminal system

Figure 3 shows the functional structure of a one-way DCAS terminal.

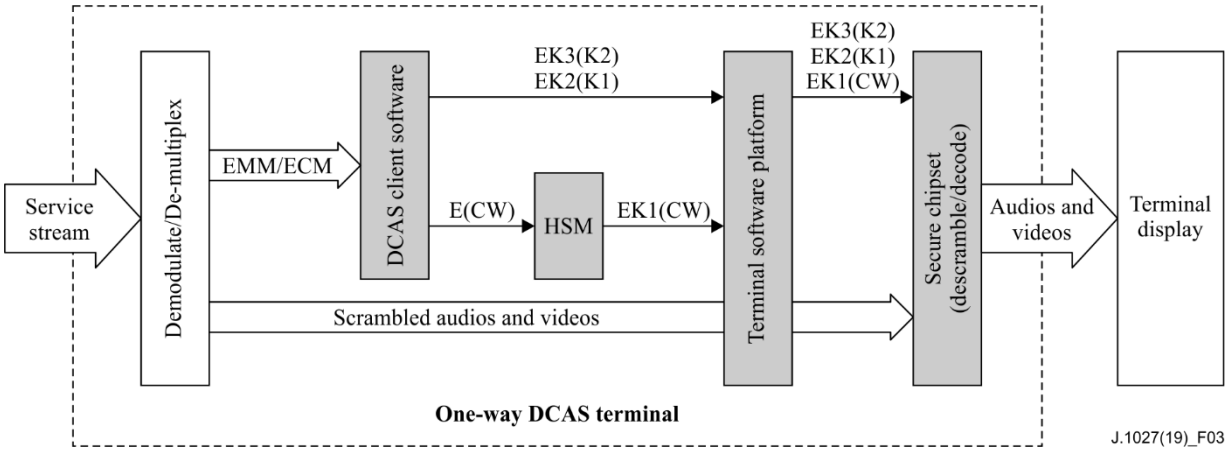

Figure 3 – One-way DCAS terminal functional structure

The main modules are:

a) One-way DCAS client software

One-way DCAS client software is an application running on a one-way DCAS terminal software platform, communicating with a platform and other modules via standard API. One-way DCAS client software can be downloaded, updated and replaced. One-way DCAS client software is responsible for analyzing and processing the EMM data, to provide key ladder data to the terminal security chipset and HSM.

b) Terminal software platform

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

c) Terminal security chipset

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

d) HSM

The HSM is an independent security chipset providing secure storage and algorithm tools. It protects the control word with key ladder and re-encryption keys and works together with terminal security chipset to enhance the security of the unidirectional one-way DCAS system.

6.1.3 One-way DCAS SDMP

The SDMP generates terminal security chipset keys and security data and serializes them to a terminal security chipset. It also maintains and manages the keys and security data. The main functions are:

a) Generating terminal security chipset keys

To generate keys of the terminal security chipset: generate ChipID and ESCK file and send them in a secure way to a security chipset key serializing module, to write the keys 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 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 public key to the terminal security chipset vendor and write the key into the terminal security chipset.

b) Serializing terminal security chipset key.

Using the key serializing module installed on the chipset vendor's production line through the secure transfer protocol of the production line, SDMP writes the terminal security chipset key saved in the key serializing module, including ChipID and ESCK, etc., to the terminal security chipset.

c) Signing the bootup verification key

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

d) Managing the HSM certificate

To generate the HSM root certificate and issue subordinate HSM vendor and CA vendor certificates.

6.2 Security mechanism

6.2.1 Key mechanism

6.2.1.1 Key model

The key mechanisms of a one-way DCAS system 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 key model of a one-way DCAS system.

The root key derivation mechanism enables the terminal security chipset to derive a personalized root key in real time by using its built-in root key derivation module; the 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 one-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 transfer, by using the root key derived from the root key derivation mechanism as the first level key to encrypt/decrypt CW level by level, the key ladder also includes a challenge-response function to implement operations by using a terminal security chipset key ladder. Contents are protected by the service scrambling/descrambling mechanism implemented with the control word output from key ladder.

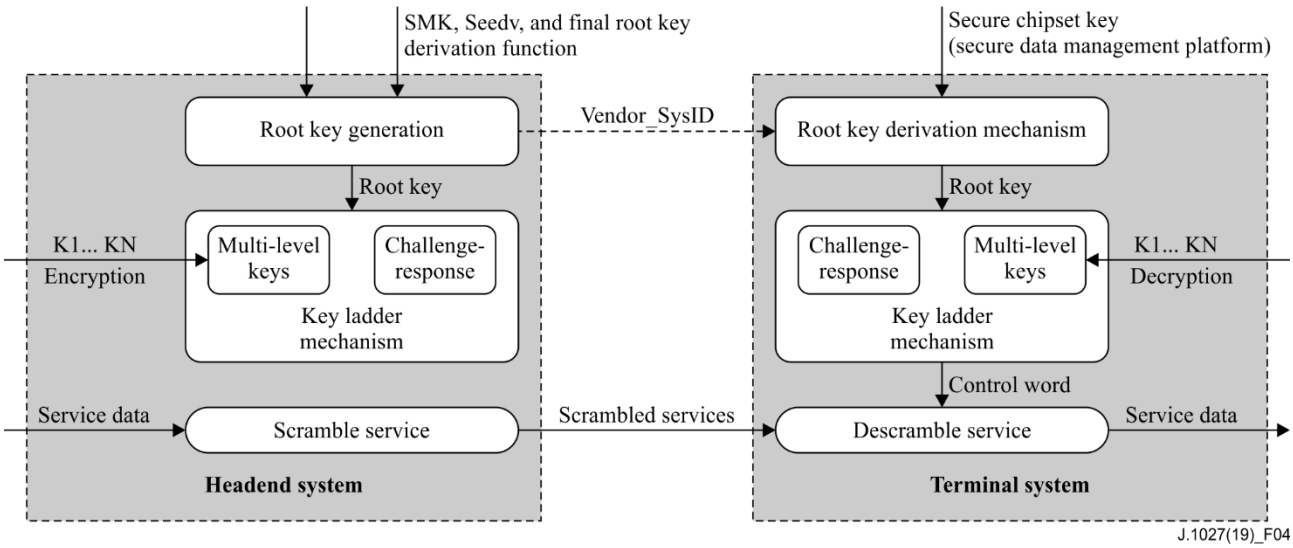

Figure 4 – Key model

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

A one-way DCAS headend system uses necessary data and a related algorithm 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

A one-way DCAS terminal uses DCAS client software to provide necessary information for a terminal security chipset and derives the root key with a 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 one-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, CA vendor and chipset vendor, to ensure the security and neutrality of the one-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 One-way DCAS terminal hardware security mechanism

A one-way DCAS terminal hardware security mechanism is secured by the terminal security chipset and HSM. See [ITU-T J.1028] for detailed technical requirements.

6.2.3 One-way DCAS terminal software security mechanism

6.2.3.1 Chain of trust

A one-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 one-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, one-way DCAS client software shall have a run-time data security protection mechanism.

Terminal security chipset performs a data source reliability check and integrity check on the boot loader before running it.

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

The terminal software platform performs a data source reliability check and integrity check on one-way DCAS client software before downloading and running it.

6.2.3.2 One-way DCAS client software data security

A terminal shall ensure the security of data storage when one-way DCAS client software stores data on the terminal.

When storing critical data, one-way DCAS client software shall use the secure storage function provided by the HSM via a secure authenticated channel (SAC).

6.2.3.3 Terminal trusted execution environment

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

Trusted secure 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.

Trusted secure software includes secure operating system (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 a 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*.

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