International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.1027

(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 – 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. 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 , to adapt to a new CA system by downloading and installing the new client of a CA system without changing the hardware. In particular, a 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.1027	2019-07-29	9	11.1002/1000/13973
2.0	ITU-T J.1027	2022-01-13	9	11.1002/1000/14869

Keywords

DCAS, downloadable conditional access system, system architecture.

* 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 second 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: “The terminal” [ITU-T J.1028].

Recommendation ITU-T J.1027

Downloadable conditional access system for unidirectional networks – System architecture

1 Scope

This Recommendation specifies the system architecture and related security mechanisms of a one-way downloadable conditional access system (DCAS) for unidirectional networks. This Recommendation is one of a series specifying the whole one-way DCAS for unidirectional networks: [ITU-T J.1026] specifies related requirements 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.1026] Recommendation ITU-T J.1026 (2022), *Downloadable conditional access system for unidirectional networks – Requirements*.

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

3.1.2 challenge-response [ITU-T J.1026]: 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.

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

3.1.4 downloadable conditional access system (DCAS) [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 a two-way network.

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

3.1.6 entitlement management message (EMM) [ITU-T J.1026]: A message containing actual authorization data that requires sending by a secure method to each piece of customer premises equipment.

3.1.7 hardware security module (HSM) [ITU-T J.1026]: A security chipset capable of control word processing, access control and secure storage, etc., which supports hardware security enhancement in a unidirectional receiver.

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

3.1.9 one-way DCAS [ITU-T J.1026]: A downloadable conditional access system (DCAS) operated especially in a one-way network.

3.1.10 one-way DCAS App [ITU-T J.1026]: 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.

3.1.11 one-way DCAS client software [ITU-T J.1026]: 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.

3.1.12 one-way DCAS manager [ITU-T J.1026]: 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.

3.1.13 one-way DCAS trusted App [ITU-T J.1026]: 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.

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

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

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

3.1.17 terminal software platform [ITU-T J.1026]: 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.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 one-way DCAS client software data: Data to be saved or updated, which include conditional access (CA) authorization information, CA private data and positioning information, when the one-way DCAS client software runs.

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

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

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
BOSS	Business Operation Support System
CA	Conditional Access
ChipID	Chipset Identifier
CW	Control Word
DCAS	Downloadable Conditional Access System
ECM	Entitlement Control Message
ECMG	Entitlement Control Message Generator
EMM	Entitlement Management Message
EMMG	Entitlement Management Message Generator
ESCK	Encrypted Security Chipset Key
HSM	Hardware Security Module
K*n*	Key *n*
KLAD	Key Ladder
SCKv	Security Chipset Key vendor
SDMP	Secure Data Management Platform
SIG	Service Information Generator
SMK	Secret Mask Key
SMS	Subscriber Management System
TEE	Trusted Execution Environment
TS	Transport Stream
TV	Television
Vendor_SysID	Vendor System Identifier

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 Recommendation 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 this Recommendation.

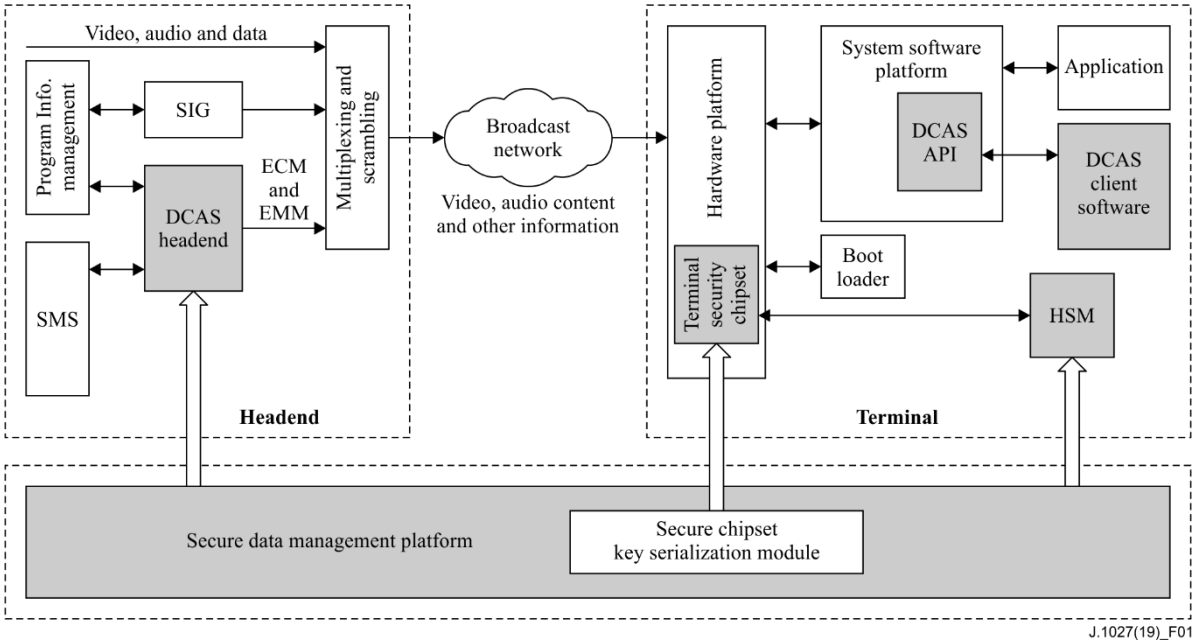
In the body of this Recommendation, the words *shall*, *shall not*, *should*, and *may* sometimes appear, in which case they are to be interpreted, respectively, as *is required to*, *is prohibited from*, *is recommended*, and *can optionally*. The appearance of such phrases or keywords in an appendix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

6 One-way DCAS architecture

6.1 One-way DCAS architecture

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

A one-way DCAS consists of the headend, the terminal and the SDMP. Figure 1 shows the one-way DCAS architecture defined in [b-GY/T 308].



SIG: service information generator; SMS: subscriber management System

Figure 1 – One-way DCAS architecture

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

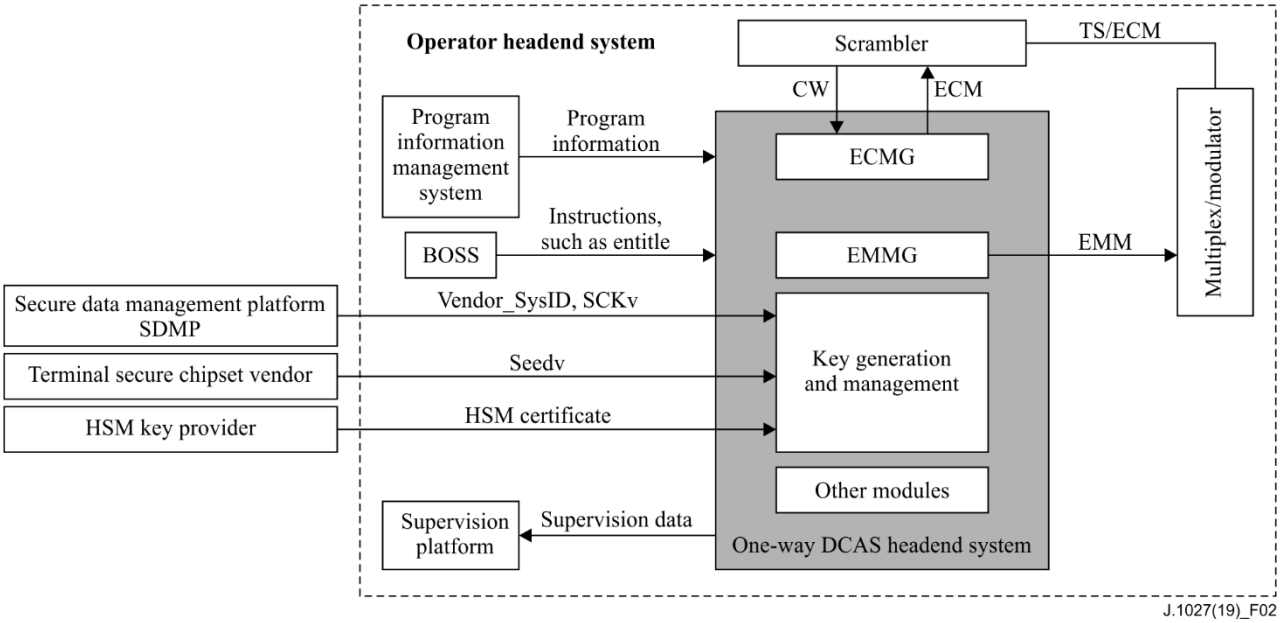
The one-way DCAS terminal validates a user's entitlement and descrambles protected services to implement CA of services. A terminal software platform can securely download, update and replace DCAS client software. The one-way DCAS terminal mainly includes a terminal security chipset, an HSM, a terminal software platform, which includes a DCAS application programming interface (API) and DCAS manager, and DCAS client software that includes a one-way DCAS app and one-way DCAS trusted app.

The one-way DCAS SDMP generates and manages keys used in one-way DCAS, provides the one-way DCAS headend with necessary information such as a security chipset key vendor (SCKv) and a

vendor system identifier (Vendor_SysID), and provides a terminal security chipset by using a key serializing module with the necessary information such as a chipset identifier (ChipID), encrypted security chipset key (ESCK) and BL_KEY0, and provides the HSM with a root certificate. Clauses 6.1.1 and 6.1.3 describe how a one-way DCAS SDMP works with a one-way DCAS headend and one-way DCAS terminals. The one-way DCAS SDMP provides the information previously mentioned to both a one-way DCAS headend and related one-way DCAS terminals before the deployment of headend and terminals, but it does not participate in any operation and get involved in any activity of both the one-way headend and related one-way terminals once they are deployed.

6.1.1 One-way DCAS headend system

Figure 2 shows the functional framework of a one-way DCAS headend also specified in [b-GY/T 308].



BOSS: business operation support system; TS: transport stream

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

A one-way DCAS headend consists of following main modules.

a) ECMG

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

b) EMMG

The EMMG generates and sends an EMM via the interface of the multiplex.

c) Secure key generation and management

This module generates and manages root key and KLAD keys according to the information about the terminal security chipset vendor and the terminal security chipset provided by the SDMP. This module encrypts and signs HSM-related data according to the HSM information provided by the SDMP and HSM key providers. The generation and management of KLAD keys are handled by the one-way DCAS headend system itself.

d) Other modules

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

6.1.2 One-way DCAS terminal system

Figure 3 shows the functional framework of a one-way DCAS terminal specified in [b-GY/T 308].

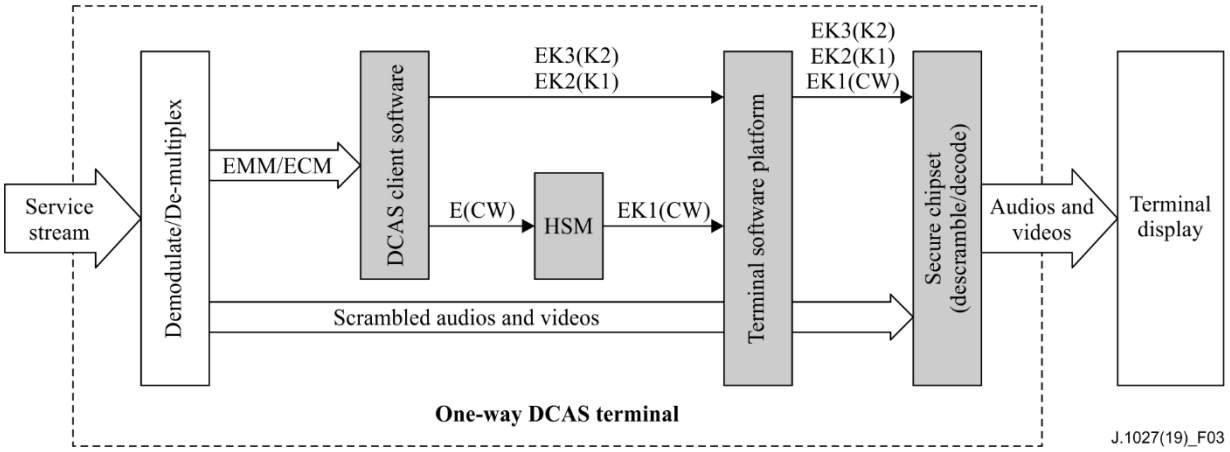


Figure 3 – The functional framework for the one-way DCAS terminal

The one-way DCAS terminal includes the following main modules.

a) The one-way DCAS client software

Th is application runs on a one-way DCAS terminal software platform, and communicates with the one-way DCAS terminal software platform and other modules via a standard API. One-way DCAS client software can be downloaded, updated and replaced through the one-way DCAS terminal software platform by the receiver. One-way DCAS client software is responsible for the analysis and processing of EMM data, and provides KLAD data to the terminal security chipset and HSM.

b) The terminal software platform

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

c) The 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

This independent security chipset provides secure storage and algorithm tools. It protects the CW with KLAD and re-encryption keys, and works together with the terminal security chipset to enhance the security of the one-way DCAS system.

6.1.3 One-way DCAS SDMP

The one-way SDMP performs keys and security data generation and serialization for the terminal security chipset, and maintains and manages the keys and security data that it generates. The main functions are as follows.

a) Key generation for a terminal security chipset

To generate security information of a terminal security chipset, this function: generates files for a ChipID and other security data, sends them in a secure way to a security chipset key serializing module and writes the security information data into the terminal security chipset.

To generate an intermediate key for root key derivation, this function: generates a ChipID and SCKv file and sends them in a secure way to a one-way DCAS of a CA vendor to generate root key K3.

To generate the bootloader verification key for a terminal security chipset, this function: generates BL_KEY0 key pairs and sends the public key to the terminal security chipset vendor 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 a ChipID and ESCK, which are saved in the key serializing module installed on the chipset vendor's production line with appropriate secure transfer protocols.

c) Signing the boot-up verification key

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

d) Management of the HSM certificate

This function generates the HSM root certificate and issues subordinate HSM vendor and CA vendor certificates.

6.2 Security mechanism

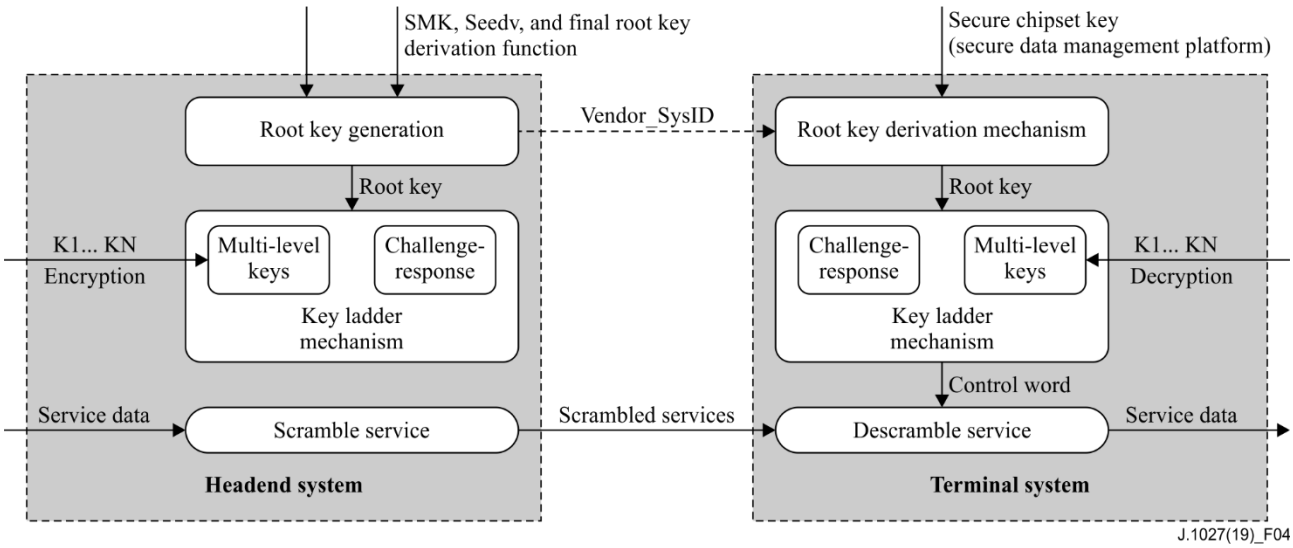
6.2.1 Key mechanism

6.2.1.1 Key model

The key mechanisms of a one-way DCAS system include those for root key derivation, KLAD, secure data management, and service scrambling and descrambling. Figure 4 shows the one-way DCAS key model also specified in [b-GY/T 308].

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 one-way DCAS systems can securely derive their personalized root key by using the respective and appropriate module based on the same terminal security chipset.

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



SMK: secret mask key

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 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 the terminal security chipset and derives the root key by the corresponding module embedded in the terminal security chipset.

6.2.1.3 Key ladder mechanism

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

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

The challenge-response function is used to send a value to a certain level of the KLAD 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, the CA vendor and chipset vendor, to ensure the security and neutrality of the one-way DCAS system.

6.2.1.5 Service scrambling and descrambling mechanism

The service scrambling and 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. [ITU-T J.1028] specifies 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 by digital signature technology on a bottom-to-top 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.

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 one-way DCAS client software before the one-way DCAS client software runs.

6.2.3.2 One-way DCAS client software data security

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

6.2.3.3 Terminal trusted execution environment

The one-way DCAS client trusted application runs in a trusted execution environment (TEE). A TEE provides a trusted computation environment for one-way DCAS based on the 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 KLAD processing module.

Trusted secure software includes a secure operating system and TEE hardware abstraction layer, which implements functions such as memory isolation, anti-rollback, secure storage, conditional access trusted application dynamic loading by using memory management, secure time, task scheduling, interruption, task communications, encryption and 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*.

[b-GY/T 308] GY/T 308-2017, *Technical specification of downloadable conditional access system for unidirectional network.*

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