International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.1001

(01/2012)

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

Conditional access and protection

Requirements for renewable conditional access system

Recommendation ITU-T J.1001

Recommendation ITU-T J.1001

Requirements for renewable conditional access system

Summary

Recommendation ITU-T J.1001 specifies functional and security requirements that should be considered for remotely renewing the conditional access client software in a conditional access system in cable networks.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T J.1001	2012-01-13	9

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 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

Since there are no conditional access systems in the real world that are secure permanently, almost all conditional access systems provide a way to renew conditional access client software (CACS) by replacing the conditional access module (CAM), which is a cryptographic functional module located within the set-top box.

The CACS remotely renewable security system is a new paradigm for renewing CACS by securely downloading a new CACS through the digital cable two-way environment. As a result, when the multiple system operator wants to upgrade the CACS in the CAM to a new one, the costs associated with the traditional approach of physically deploying and replacing the security hardware module can be avoided.

Recommendation ITU-T J.1001

Requirements for renewable conditional access system

1 Scope

1.1 Purpose

This Recommendation focuses on the architectural, functional, and security requirements that should be considered for remotely renewing the conditional access client software (CACS) within a conditional access system, which is supposed to be provided by a single vendor in cable networks. This Recommendation defines three major functional requirements for updating remotely the security systems of CACS:

- Authentication and secure download of CACS
- Association of the descrambler and the conditional access module (CAM)
- Countermeasures for CAM cloning attacks.

1.2 Reference architecture

Figure 1 shows the reference architecture for the CACS remotely renewable security system (CRS). CRS consists of a CRS headend and a CRS set-top box (STB) at the customer premises. The AC issues identification information to the CAM and descrambler, and authenticates them. The multiple system operator (MSO) headend establishes a CACS encryption key with the CAM and sends encrypted CACS to the CAM. Finally, the CRS STB, which is a two-way (e.g., DOCSIS) digital cable set-top box, downloads the CACS in the memory of the CAM, and descrambles the encrypted video streams at the descrambler. Here, CAM has a role to request CACS from a headend, and update the old conditional access client software with a new one.

CRS headend could be categorized into three parts: CAM authentication sub-system, Secure CACS download sub-system, and Authorization centre. The CAM authentication sub-system issues unique identification information to each CAM, and authenticates each CAM that requests a new conditional access client software. The Secure CACS download sub-system establishes a secure channel between itself and CAM. Then it downloads conditional access software to CAM after CAM authentication sub-system authenticates the CAM.

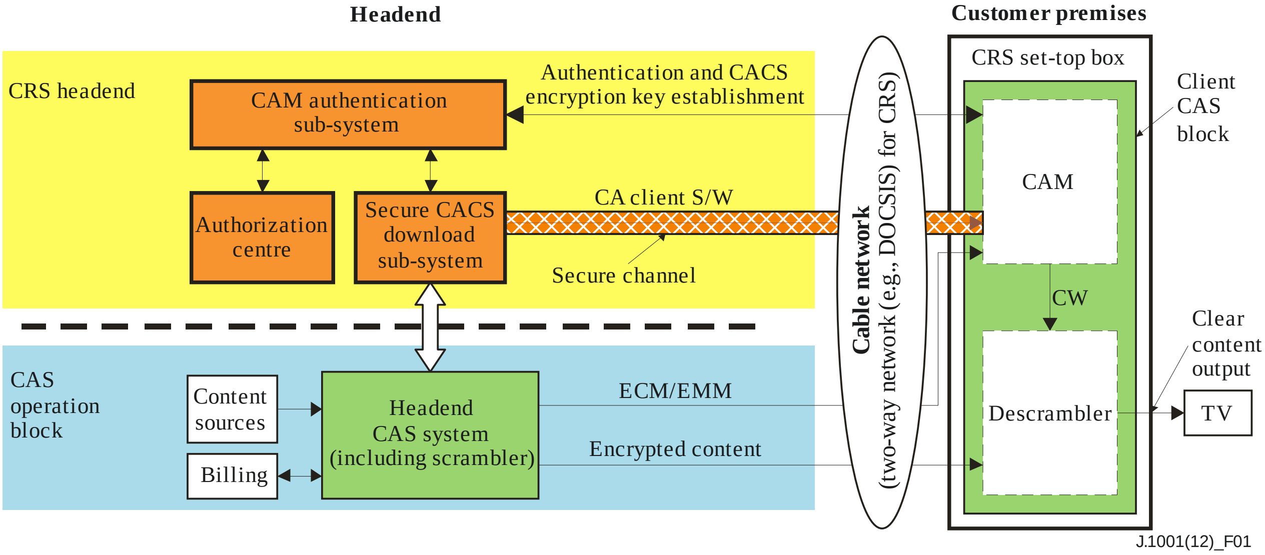

Figure 1 – Reference architecture of CRS

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 conditional access (CA) [b-ITU-T J.193]: The conditional granting of access to cable services and content based upon what service suite has been purchased by the customer.

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

3.1.3 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 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 authorization centre (AC): An entity which issues identification information of the conditional access module (CAM) and performs the authentication process when the CAM requests renewal of the conditional access client software.

3.2.2 conditional access module (CAM): A cryptographic functional module which is located in a set-top box with the main functions of entitlement validation, key management, and authentication. A set-top box can have one chip of secure hardware that includes the functions of CAM and descrambler, or a physically separated CAM in the form of a secure hardware IC or smart-card. The form of CAM can be determined by the policy of the multiple system operator or the conditional access client software vendor.

3.2.3 conditional access client software (CACS): An image of conditional access client software code downloaded onto the CACS remotely renewable security system.

3.2.4 control word (CW): The value which is used to scramble and descramble transport streams.

NOTE – The control word should be refreshed frequently during service operation to enhance security.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AC	Authorization Centre
CA	Conditional Access
CACS	Conditional Access Client Software
CAM	Conditional Access Module
CAS	Conditional Access System
CRS	CACS remote by Renewable Security System

CW	Control Word
ECM	Entitlement Control Message
EMM	Entitlement Management Message
MSO	Multiple System Operator
STB	Set-Top Box

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 Recommendation 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.

6 Architectural requirements

CRS is required to meet the following architectural requirements.

6.1 CRS headend

- [CRS-HE-01] The CRS headend is required to consist of Authorization centre (AC), CAM authentication sub-system, Secure CACS download sub-system and CAS, as shown in Figure 1.
- [CRS-HE-02] The AC is required to generate unique identification information for each CAM and descrambler, and securely deliver the generated identification information to their manufacturers using either an on-line or off-line method. The manufacturer is required to securely embed the received identification information.
- [CRS-HE-03] The identification information of the CAM and descrambler is recommended to be included in certificates.
- [CRS-HE-04] The AC is required to perform a CRS STB device authentication process based on the identification information received from the CAM via the CAM authentication sub-system in the MSO headend.
- [CRS-HE-05] The CAM authentication sub-system is a proxy of the AC and is required to perform a mutual authentication process through the CRS network protocol between the CAM authentication sub-system and CAM.
- [CRS-HE-06] While the CAM authentication sub-system performs the mutual authentication process through the CRS network protocol, CAM is required to send identification information of the CRS STB devices to the AC, and the AC is required to relay the authentication results to the CAM authentication sub-system.
- [CRS-HE-07] After the mutual authentication process is successfully performed, CAM authentication sub-system and CAM is required to establish symmetric CACS encryption key through the CRS network protocol.
- [CRS-HE-08] The Secure CACS download sub-system is required to contain the source of all CACS for distribution, downloading and management.
- [CRS-HE-09] If the mutual authentication process between the CAM authentication sub-system and CAM is successfully performed, the Secure CACS download sub-system is required to send the CACS to the CAM through the download servers after encrypting it with the CACS encryption key.

- [CRS-HE-10] The CAS is required to generate entitlements keys and control words for all for-fee programmes and securely deliver them via entitlement management messages (EMMs) and entitlement control messages (ECMs) to the CA client application in the CAM.

6.2 CRS STB

- [CRS-STB-01] The CRS STB is required to be a two-way digital cable set-top box that has not only downstream broadcast service receiving capability, but also downstream and upstream data communication capabilities.
- [CRS-STB-02] CAM and descrambler are required to protect security parameters stored in their memory from physical security attacks.
- [CRS-STB-03] The CAM is a highly secure chip that is required to perform a CRS network protocol for mutual authentication with the CAM authentication sub-system.
- [CRS-STB-04] The CAM device is required to be either an embedded chip on a set-top motherboard type or a removable device type.
- [CRS-STB-05] The CAM is required to securely store security parameters in its memory and to operate CAM client applications to decrypt control words and send them in encrypted form to the descrambler.
- [CRS-STB-06] The descrambler is required to receive encrypted control words from the CAM and decrypt the control words before using them for descrambling the encrypted video streams.
- [CRS-STB-07] Since the descrambler has no direct communication channel to the MSO headend and AC, the descrambler is required to receive any necessary data from the AC or MSO headend through the CAM.

7 Functional requirements

CRS is required to meet the following functional requirements:

7.1 Authentication and secure download of CACS

- [CRS-AUTH-01] When downloading CACS from headend to CAM, the headend is required to perform the authentication and CACS encryption key establishment processes through the CRS network protocol to prevent an illegitimate CACS downloading request from a pirate CAM that has a CAM authentication sub-system. When CACS is authenticated on a one-by-one basis between the headend and the CAM in a CRS STB, a surrogate authentication by each cable station could be allowed to make renewal effective in a large scale network.
- [CRS-AUTH-02] After headend successfully performs the authentication process and confirms that a CACS download request is from a legitimate CAM, the Secure CACS download sub-system is required to encrypt CACS using the CACS encryption key.

7.2 CAM and descrambler pairing

- [CRS-PAIR-01] Assume that there is a user who has a removable or detachable CAM, and subscribes to pay programmes after CACS has been loaded into a CAM. Then, that user can watch the subscribed pay programmes by inserting the removable CAM into any set-top box connected to the same MSO network. In other words, a group of users can watch pay programmes by sharing the removable CAM if just one member of the group subscribes to the pay programmes. However, this service leak caused by CAM sharing cannot be acceptable to the MSO from a subscriber management point of view. To prevent the service leak described above, the CRS is required to support a CAM and descrambler pairing function.

7.3 Countermeasure to CAM cloning attacks

- [CRS-CLN-01] One of the major concerns of the CACS remotely renewable security system is a CAM cloning attack. If there is a cloned CAM in an MSO network, the CRS cannot reject the authentication request from the cloned one. As a result, MSOs would suffer service leakage in proportion to the number of cloned CAMs existing in their networks. Therefore, the CRS is required to be equipped with a function of countermeasure to CAM cloning attacks.

8 Security Requirements

CRS is required to meet the following security requirements:

8.1 CACS encryption key establishment

The CRS key establishment protocol between the CAM authentication sub-system and CAM is required to follow the requirements below for establishing symmetric CACS encryption keys.

- [CRS-KEYEST-01] *Known key security*: An adversary must not be allowed to generate a key using knowledge that can be obtained from some other keys. For this type of security, the CRS key establishment protocol is required to generate a key that is unique for each session.
- [CRS-KEYEST-02] *Perfect forward secrecy*: Even when long-term private keys are compromised, an adversary must not be allowed to find previous keys established between entities. For this type of security, the CRS key establishment protocol is required to use a random value for key generation and guarantee that the random value cannot be extracted from the key.
- [CRS-KEYEST-03] *Key-compromised impersonation*: If a long-term private key of an entity, say A, is compromised, then clearly an adversary that knows this value can impersonate A to other entities. Despite this loss of key integrity, the CRS key establishment protocol is required not to allow an adversary to impersonate other entities to A.
- [CRS-KEYEST-04] *Unknown key-share attack*: From this unknown key-share attack, an adversary C can make one entity, say A, believe that the key is shared with C when it is in fact shared with a different entity, B. To counter this attack, the CRS key establishment protocol is required to provide a process of key confirmation between entities.
- [CRS-KEYEST-05] *Key control*: The CRS key establishment protocol is required to prevent either entity from forcing the key to a preselected value.

8.2 Operational encryption key enforcement

To enforce CACS encryption key security, the following functions of operational encryption key enforcement are necessary:

- [CRS-KEYOPR-01] CRS is required to specify creation, reproduction, distribution and life-time of a CACS encryption key.
- [CRS-KEYOPR-02] CRS is required to specify exception handling processes for authentication due to excessive time to respond and to excessive number of retries.
- [CRS-KEYOPR-03] CRS is required to specify the failure process of CACS renewal.

Appendix I

Overall CRS operation flows

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

The overall CRS operation flows based on the CRS entities are shown in Figure I.1 and are described as follows. It is assumed that, prior to starting CRS operations, CAM and the descrambler have unique identification information which is supposed to be assigned by AC. Note that off line delivery is recommended to securely issue identification information from AC to the manufacturers of CAM and the descrambler.

– Step 1: AC, CAM authentication sub-system and CAM perform the authentication and pairing process. In this process, the identification information of CAM itself and the descrambler are securely delivered to AC through the CAM authentication sub-system.

– Step 2: After CAM and the descrambler are properly authenticated and paired, then a CRS operation session is established. In this process, the CAM authentication sub-system and CAM set up a secure channel between them.

– Step 3: The CAM authentication sub-system and CAM establish a CACS encryption key between them through the CRS network protocol.

– Step 4: The Secure CACS download sub-system sends the encrypted CACS via download servers to the CAM.

– Step 5: The CAM boot-loader decrypts the CACS and loads the image into the CAM memory.

– Step 6: The CRS operation session is terminated and the CAS operation steps commence.

– Step 7: General CAS processes are started as follows:

  - The CAS in the MSO headend sends entitlement keys for the subscribed pay-programmes using an EMM and the encrypted control words using an ECM to the CA client application in the CAM.
  - The CA client application in the CAM decrypts control words with the entitlement keys and sends the control words to the descrambler in an encrypted form. Note that the CAM and descrambler establish the control words encryption key to provide confidentiality when they are sent from the CAM to descrambler.
  - The descrambler descrambles the encrypted video stream using the control words and sends the cleared video stream to a device on the user's premises, such as a television.

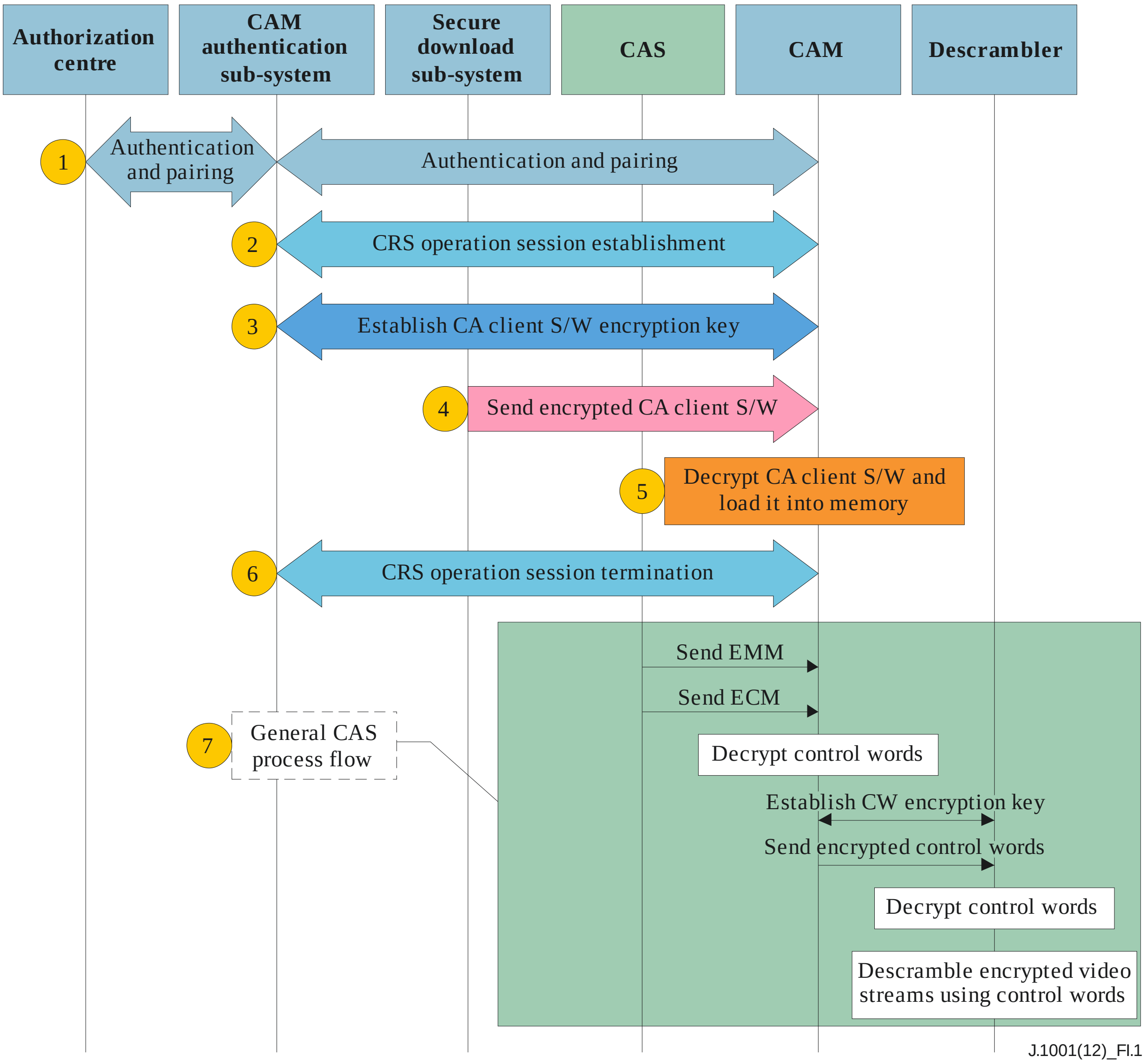
Authorization centre
CAM authentication sub-system
Secure download sub-system
CAS
CAM
Descrambler
1
Authentication and pairing
Authentication and pairing
2
CRS operation session establishment
3
Establish CA client S/W encryption key
4
Send encrypted CA client S/W
5
Decrypt CA client S/W and load it into memory
6
CRS operation session termination
7
General CAS process flow
Send EMM
Send ECM
Decrypt control words
Establish CW encryption key
Send encrypted control words
Decrypt control words
Descramble encrypted video streams using control words
J.1001(12)_FI.1

Figure I.1 – Overall CRS operation flows

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.193]	Recommendation ITU-T J.193 (2004), *Requirements for the next generation of set-top boxes*.
[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	General tariff principles
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	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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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 and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013