



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 conditional access client software remote renewable security system

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

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/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/>.

© ITU 2012

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Recommendation ITU-T J.1001 (J.rcas-req)

Requirements for conditional access client software remote renewable security system

Summary

This recommendation 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.

Introduction

Since there are no permanent secure conditional access systems in the real world, 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 in set-top box.

The CACS remote renewable security system (CRS) is a new paradigm technology for renewing CACS by securely downloading a new CACS through the digital cable two-way environment. As a result there is no additional budget required for issuing a new security hardware module when the Multiple System Operator (MSO) wants to upgrade the old CACS in CAM to a new one.

1. Scope

1.1. Purpose

This recommendation focuses on the architectural, functional, and security requirements that should be considered for remotely renewing the 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, which are ‘Authentication and secure download of CACS’, ‘CAM and descrambler pairing’, and ‘CAM cloning-attack countermeasure’, for CACS remote renewable security system.

1.2. Reference architecture

Figure 1 shows the CRS reference architecture. CRS consists of CRS headend, and CRS STB at the customer premises. The AC issues identification information to the CAM and descrambler and authenticates them. The 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 to a headend, and update the old conditional access client software into a new one.

CRS headend could be categorized into three parts such as ‘CAM Authentication Sub-system’, ‘Secure CACS Download Sub-system’, and ‘Authorization Center’. The ‘CAM Authentication Sub-system’ issues unique identification information to each CAMs, and authenticates a CAM if it requests a new conditional access client software. The ‘Secure CACS Download Sub-system’ establishes secure channel between itself and CAM. Then it downloads conditional access software to CAM after ‘CAM Authentication Sub-system’ authenticates the CAM.

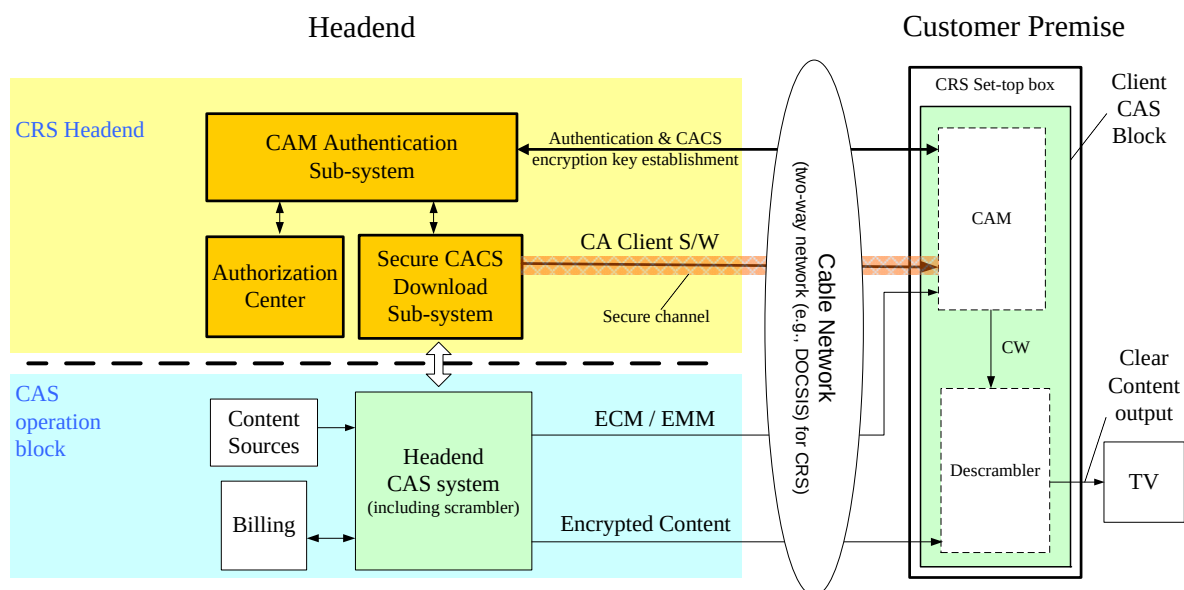


Figure 1 Reference architecture of CRS

2. References

None.

3. Definitions

3.1. Terms defined in this Recommendation

- 3.1.1. **Authorization Centre (AC):** An entity which issues identification information of CAM and performs authentication process when CAM requests renewing of CACS.
- 3.1.2. **Conditional Access Module (CAM):** A cryptographic functional module which is located in set-top box with the main function of entitlement validation, key management, and authentication. Set-top box can have one chip of secure hardware that includes the functions of CAM and descrambler, or 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 MSO or CAS vendor.
- 3.1.3. **Conditional Access Client Software (CACS):** An image of conditional access client software code downloaded onto the CRS CAM.
- 3.1.4. **Control Word (CW):** The value which is used to scramble and descramble transport streams, and it is refreshed frequently during the service operation to enhance security.

3.2. Terms defined elsewhere

- 3.2.1. **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.
- 3.2.2. **Descrambling [b-ITU-T J.93]:** The processes of reversing the scrambling function (see “scrambling” to yield usable pictures.
- 3.2.3. **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).
- 3.2.4. **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.