

International Telecommunication Union

**ITU-T**

TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

**J.1002**

(03/2013)

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

Conditional access and protection

---

## **Pairing protocol specification for renewable conditional access system**

Recommendation ITU-T J.1002



International  
Telecommunication  
Union  
**Documents**

Document Sharing Hub

Copyright International Telecommunication Union/ITU Telecommunication Sector  
Provided by IHS Markit under license with ITU-T  
No reproduction or networking permitted without license from IHS

# Recommendation ITU-T J.1002

## Pairing protocol specification for renewable conditional access system

### Summary

Recommendation ITU-T J.1002 specifies the pairing protocol that supports the conditional access module (CAM) and descrambler (DSC) pairing function, which is specified in Recommendation ITU-T J.1001.

### History

| Edition | Recommendation | Approval   | Study Group |
|---------|----------------|------------|-------------|
| 1.0     | ITU-T J.1002   | 2013-03-01 | 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/>.

© ITU 2013

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

## Table of Contents

|     |                                                                  | Page |
|-----|------------------------------------------------------------------|------|
| 1   | Scope .....                                                      | 1    |
| 2   | References.....                                                  | 1    |
| 3   | Definitions .....                                                | 1    |
| 3.1 | Terms defined elsewhere .....                                    | 1    |
| 3.2 | Terms defined in this Recommendation.....                        | 1    |
| 3.3 | Security symbols .....                                           | 2    |
| 3.4 | Parameter definitions.....                                       | 2    |
| 3.5 | Security function definitions .....                              | 3    |
| 4   | Abbreviations and acronyms .....                                 | 3    |
| 5   | Conventions .....                                                | 3    |
| 6   | Overview of RCAS pairing protocol .....                          | 4    |
| 7   | Details of RCAS pairing protocol.....                            | 5    |
| 7.1 | Initialization.....                                              | 5    |
| 7.2 | Pairing.....                                                     | 6    |
| 7.3 | CWEK generation .....                                            | 10   |
| 8   | CAM and DSC interface message format and encryption.....         | 12   |
| 8.1 | DscCertReq message .....                                         | 13   |
| 8.2 | DscCertRsp message .....                                         | 13   |
| 8.3 | CWEKGenInfo message .....                                        | 14   |
| 8.4 | CWEKGenInfoCnfm message .....                                    | 14   |
|     | Appendix I – The functional structures for the CAM and DSC ..... | 16   |
| I.1 | Functional structure for CAM .....                               | 16   |
| I.2 | Functional structure for DSC.....                                | 17   |
|     | Bibliography.....                                                | 18   |

Copyright International Telecommunication Union/ITU Telecommunication Sector  
 Provided by IHS Markit under license with ITU-T  
 No reproduction or networking permitted without license from IHS  
 Full document details: ITU-T J.1002 2013

## Introduction

Recommendation ITU-T J.1001 specifies the requirements for renewable conditional access system (RCAS), and it identifies the pairing protocol that is one of the functional requirements.

The RCAS is a new paradigm technology for renewing conditional access (CA) client software by securely downloading the new version of software through the digital cable two-way environment. The benefit of RCAS is that no additional budget is required for issuing a new security hardware module when the multiple systems operator (MSO) wants to upgrade the old CA client software to a new one.

The pairing protocol is an authentication protocol between the conditional access module (CAM) and descrambler (DSC). The authentication process between the CAM and DSC is one of the most important security requirements for the RCAS. If the pairing is not performed properly, it may cause a control word (CW) disclosure problem. For example, a hacked DSC could intercept CWs transferred from the CAM through impersonation attack. As a result, a hacker could watch pay broadcasting programs without proper entitlement by taking advantage of the intercepted CW.

If the pairing is not performed properly, this may cause another problem – of managing paid-viewers. For example, a malicious user could remove the physically-implemented CAM from one set-top box that stores entitlement information, and connect the removed CAM to another set-top box. Then a malicious user could watch pay broadcasting programs on multiple set-top boxes with one CAM. As a result, MSO cannot properly manage pay subscribers, and undergoes unwanted business losses.

To prevent the above drawbacks, a pairing protocol is specified in this Recommendation, which can provide a mutual authentication and security channel establishment between the CAM and the DSC. Using the pairing protocol can efficiently prevent a hacked DSC from eavesdropping CWs, which are transferred from the CAM to DSC, as well as unwanted usage of one CAM to multiple set-top boxes.

# Recommendation ITU-T J.1002

## Pairing protocol specification for renewable conditional access system

### 1 Scope

This Recommendation specifies the pairing protocol that provides the conditional access module (CAM) and descrambler (DSC) pairing function of renewable conditional access system (RCAS), which is specified in [ITU-T J.1001].

### 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.1001] Recommendation ITU-T J.1001 (2012), *Requirements for renewable conditional access system*.

[ITU-T X.509] Recommendation ITU-T X.509 (2008) | ISO/IEC 9594-8:2008, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

### 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 function (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 CAM and performs authentication process when CAM requests renewing of CACS.

**3.2.2 conditional access module (CAM):** A cryptographic functional module which is located in set-top boxes, whose main function is entitlement validation, key management and authentication. Set-top boxes 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 the MSO or CAS vendor.

**3.2.3 conditional access client software (CACS):** An image of conditional access client software code downloaded onto the CRS CAM.

**3.2.4 control word (CW):** The value which is used to scramble and descramble transport streams; it is refreshed frequently during the service operation to enhance security.

### 3.3 Security symbols

| Security symbols    | Descriptions                                                                                                                                                                                               |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pub(X)              | RSA public key of 'X'                                                                                                                                                                                      |
| Prv(X)              | RSA private key of 'X'                                                                                                                                                                                     |
| E(k,m)              | Encryption of a message 'm' with key 'k'. RSAES-OAEP is used to encrypt a message when the encryption key is a public key. AES-ECB is used to encrypt a message when the encryption key is a symmetric key |
| S(k,m)              | Digital signature for a message 'm' with signing key 'k'. RSASSA-PSS is used for message signing                                                                                                           |
| H(m)                | SHA-256 hashing for a message 'm'                                                                                                                                                                          |
| HMAC(k,m)           | HMAC-SHA1 for a message 'm' with key 'k'                                                                                                                                                                   |
| X  Y                | Concatenation of 'X' and 'Y'                                                                                                                                                                               |
| Cert(X)             | ITU-T X.509 certificate of 'X'                                                                                                                                                                             |
| PRF(X)              | Pseudo random function having a seed value of 'X'                                                                                                                                                          |
| X <sub>msb(Y)</sub> | 'Y' bits from MSB of 'X'                                                                                                                                                                                   |

### 3.4 Parameter definitions

| Parameter names | Descriptions                                                                                                                                                                                                                                                                 |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DSC_ID          | The value of identification of DSC having a size of 40 bytes                                                                                                                                                                                                                 |
| CAM_ID          | The value of identification of CAM having a size of 8 bytes                                                                                                                                                                                                                  |
| KeyPairingID    | The value of concatenation with CAM_ID and DSC_ID, i.e., CAM_ID  DSC_ID                                                                                                                                                                                                      |
| CWEK            | The abbreviation of control words encryption key, and used to encrypt <i>control words</i><br>The CWEK generation method is<br>$CWEK = H(CWEK  CAM\_ID  DSC\_ID)_{msb(128)}$                                                                                                 |
| KPK             | The abbreviation of key pairing key. The AC generates the KPK if KeyPairingID is valid                                                                                                                                                                                       |
| HMAC_KEY        | An HMAC secret key. The CAM uses HMAC_KEY to generate an HMAC value for the message including <i>control words</i><br>The HMAC_KEY generation method is<br>$HMAC\_KEY = H(RAND_{HMAC}  CAM\_ID  DSC\_ID)_{msb(160)}$ , Here $RAND_{HMAC}$ is achieved by $PRF(X)_{msb(320)}$ |
| RAND            | A random number with 320 bits                                                                                                                                                                                                                                                |
| K <sub>i</sub>  | The pre-shared key having the size of 128 bits. AC uniquely assigns three K <sub>i</sub> to each CAM                                                                                                                                                                         |