|  |  |  |
| --- | --- | --- |
| INTERNATIONAL TELECOMMUNICATION UNION | | **STUDY GROUP 17** |
| **TELECOMMUNICATION STANDARDIZATION SECTOR**  STUDY PERIOD 2013-2016 | | **TD 0241** |
| **English only**  **Original: English** |
| **Question(s):** | 11/17 | Geneva, 17-26 April 2013 |
| **TD** | | |
| **Source:** | Rapporteur Q.11/17 | |
| **Title:** | Draft amendment 2 for Rec. ITU-T X.509 | ISO/IEC 9594-8 | |

**TITLE:** Rec. ITU-T X.509 (2012) | ISO/IEC 9594-8 : 2012 Information Technology - Open systems Interconnection - The Directory: Public-key and attribute certificate frameworks – Working Draft for Adm. 2: Directory-IdM support

**SOURCE:** Collaborative ITU-T and ISO/IEC JTC1 meeting on the Directory, Geneva, Switzerland,  
17 - 26 April 2013

## 3.5 Public-key and attribute certificate definitions

Add the following new definitions:

**3.5.68 trust in a CA**: belief that the CA will act reliability and truthfully in the management of its public key certificates and will comply with its published certification practise statement and relevant legislation.

**3.5.69 trust in a public key certificate**: belief that the public key certificate is valid for a particular transaction.

**3.5.70 trust broker**: a trusted third party that helps relying parties to decide about the validity of a public key certificate for a particular transaction. Trust brokers are independent of certification authorities and have direct trust relationships with relying parties.

# 6 Frameworks overview

Add a new bullet to the first bullet list:

– optionally asking a trust broker if the certificate can be trusted for the intended purpose.

SECTION 2 – PUBLIC-KEY CERTIFICATE FRAMEWORK

Add new 1st level header right after SECTION 2 header and renumber subsequent clauses:

# 7 Trust Models

Update the third paragraph of the new 7 clause as shown:

A relying party needs to validate a public-key certificate prior to using that public-key certificate for a particular transaction in an application. Procedures for performing that validation are also defined here, including verifying the integrity of the public-key certificate itself, its revocation status, and its validity with respect to the intended use.

After this third paragraph add a level 2 header:

## 7.1 Three Cornered Model

At the start of what is now 7.1 delete the first paragraph together with the three bullet point.

Add the following:

The three cornered model is used in closed public key infrastructures where each user (certificate subject and relying party) has been issued with a public-key certificate by the CA.



Figure 2 – The three cornered trust model

In the three cornered trust model, the public-key certificate subject trusts the CA and has asked it to issue a public-key certificate. The CA trusts the public-key certificate subject and so issues it with a public key certificate. The relying party, being a public-key certificate subject, also trusts the CA. Consequently the relying party can indirectly trust the public-key certificate subject for the current transaction.

## 7.2 Four Cornered Model

The four cornered model may be used in open public key infrastructures, where the relying party does not have a public key certificate issued by the CA of the certificate subject.



Figure 3 – The four cornered trust model

In the four cornered model, the relying party trusts the trust broker. The trust broker has evaluated the CA and the public key certificate of the certificate subject, and has decided that the certificate can be used by the relying party for the transaction that the relying party is currently participating in with the certificate subject. Consequently the trust broker trusts the CA and the certificate for this transaction. The CA trusts the certificate subject. Hence the relying party can indirectly trust the public key certificate of the subject for this particular transaction.

# 8 Public-keys and public-key certificates

## 8.1 Introduction

In the old 7.1, which is now 8.1, change the first paragraph as shown:

In order for a relying partyuser to be able to trust a public-key offor another user, for instance to authenticate the identity of that user, the public-key shall be obtained from a trusted source, and a trust broker may be consulted. Such a source, called a Certification Authority (CA), certifies a public key by issuing a public-key certificate which binds the public-key to the entity which holds the corresponding private-key. The procedures used by a CA to ensure that an entity is in fact in the possession of the private key and other procedures related to the issuance of public-key certificates are outside the scope of this Directory Specification. However trust brokers are the entities that should review these procedures and make trust decisions based upon them. The certificate, the form of which is specified later in this clause, has the following properties:

Move clauses 18, 18.1 18.2 18.2.1, 18.2.2, 18.2.3, 18.3 to Rec. ITU-T X.511 | ISO/IEC 9594-3 after clause 7.

Move 18.2.4 and 18.2.5 to Rec. ITU-T X.520 | ISO/IEC 9594-6 after clause 13

Move 18.2.6 to Rec. ITU-T X.520 | ISO/IEC 9594-6 after clause 8.9

Merge clause 19 with clause 7.11 of Rec. ITU-T X.511 | ISO/IEC 9594-3

Merge clause 20 with 7.10 of Rec. ITU-T X.511 | ISO/IEC 9594-3

Move Annex K to Rec. ITU-T X.511 | ISO/IEC 9594-3 as Annex E

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_