|  |  |  |
| --- | --- | --- |
| INTERNATIONAL TELECOMMUNICATION UNION | | **STUDY GROUP 17** |
| **TELECOMMUNICATION STANDARDIZATION SECTOR**  STUDY PERIOD 2013-2016 | | **TD 0631** |
| **English only**  **Original: English** |
| **Question(s):** | 11/17 | Geneva, 26 August - 4 September 2013 |
| **TD** | | |
| **Source:** | Rapporteur Q11/17 | |
| **Title:** | 2nd 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,  
26 August - 4 September April 2013

# General

Make a global change of the term "this Directory Specification" to just "this Specification"

# Summary

New to be provided

# Introduction

Delete the two first two paragraphs, including the four bullet list.

Delete the paragraph saying:

This Recommendation | International Standard also defines a framework for the provision of authentication services by the Directory to its users.

Move the paragraph saying:

Annex K, which is not an integral part of this Recommendation | International Standard, provides a suggested technique for Bind protected password.

to Rec. ITU-T X.511 | ISO/IEC 9594-3 changing Annex K to Annex E. Change the letter-numbering of the follragraphs.

# 1 Scope

Remove the last bullet of the bullet list right after first paragraph.

Delete the third paragraph after the above bullet list (starting with "The Directory makes use ...")

Remove the last bullet of the second bullet list.

Change the paragraph after the second bullet list as shown:

This Recommendation | International Standard describes two levels of authentication: simple authentication, using a password as a verification of claimed identity; and strong authentication, involving credentials formed using cryptographic techniques. While simple authentication offers some limited protection against unauthorized access, only strong authentication should be used as the basis for providing secure services. It is not intended to establish this as a general framework for authentication, but it can be of general use for applications which consider these techniques adequate.

## 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.

## 6.3 Distinguished Encoding of Basic Encoding Rules

Change the first paragraph as shown:

In order to enable the validation of SIGNED and SIGNATURE types in a distributed environment, either the original signed message or, in its absence a canonical distinguished encoding is required. The canonical encoding that shall be used by this Specification is called the A distinguished encoding of a SIGNED or SIGNATURE data value shall be obtained by applying the Basic Encoding Rules defined in Rec. ITU-T X.690 | ISO/IEC 8825-1, with the following restrictions:

At then of the subclause add the following note:

NOTE ‑ These restrictions are the same as the Distinguished Encoding Rules specified in Rec. ITU-T X690 | ISO/IEC 8825-1.

## 6.4 Applying Distinguished Encoding

Change the first paragraph as shown:

Generating a distinguished encoding requires the abstract syntax of the data to be encoded to be fully understood. An entity may be required to sign data or check the signature of data that is already signed or contains unknown protocol extensions or unknown attribute syntaxes. The entity shall follow these rules:

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. In the three cornered trust model described below, the relying party acts on its own behalf. In the four cornered trust model the relying party engages the services of a trust broker to validate certificates on its behalf. When the term relying party is used in this specification, if the four cornered trust model is being employed, then it is assumed that the trust broker is acting on behalf of the relying party.

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 acts on behalf of the relying party in validating certificates and certificate chains. The trust broker evaluates the CA and the public key certificate of the certificate subject, and decides if the certificate can be used by the relying party for the transaction that the relying party is currently participating in with the certificate subject. If the decision is positive, this means that 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.

In the remainder of this specification, where relying party is mentioned, this also implies the trust broker acting on behalf of the relying party in the case of the four cornered trust model.

# 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. 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:

## 8.6 Cross-certificates

In the old 7.6, which is now 8.6, delete the last sentence of the second paragraph (Starting with: The public-key certificates issued for CA ...)

Delete all the paragraphs after the second paragraph

## 8.7 Certification path

In the old 7.7, which is now 8.7, delete the third and fourth paragraphs. (should the next paragraph also be deleted?)

Change the first paragraph after Figure 5 (old Figure 3) as shown:

Figure 53 illustrates the situation where a relying party needs to check the validity of an end-entity public-key certificate and the relying party is able to construct a certification path between the end-entity and a one of its trust anchors and the end-entity's public-key certificaterecognised by the relying party.

Delete the paragraph starting with "The following ASN.1 data types can ..." down to and including the CrossCertificate data type

Update the lat paragraph as shown:

Each public-key certificate in a PKI certification path shall be unique. No public-key certificate may appear more than once in a value of the theCACertificates component of CertificationPath or in a value of Certificate in the CrossCertificates component of ForwardCertificationPath or a value of Certificate in PkiPath.

## 8.10 Certification path

In the old 7.10, which is now 8.10,change the fourth paragraph as shown:

Certificates, including public-key certificates as well as attribute certificates, shall have a lifetime associated with them, at the end of which they expire. In order to provide continuity of service, the authority shall ensure timely availability of replacement certificates to supersede expired/expiring certificates. Revocation notice date is the date/time that a revocation notice for a certificate first appears on a CRL, regardless of whether it is a base or dCRL. In the CRL, revocation notice date is the value contained in the thisUpdate field. Revocation date is the date/time the CA actually revoked the certificate, which could be different from the first time it appears on a CRL. In the CRL, revocation date is the value contained in the revocationDate component. Invalidity date is the date/time at which it is known or suspected that the private key was compromised or that the certificate should otherwise be considered invalid. This date may be earlier that the revocation date. In the CRL, invalidity date is the value contained in the invalidityDate entry extension.

# 9 Public-key certificate and CRL extensions

In the old clause 8, which is now clause 9,change the first paragraph as shown:

The certificate extensions defined in this clause are for use with public-key certificates, unless otherwise stated. Extensions for use with attribute certificates are defined in clause 15. CRL extensions defined in this clause may be used in CRLs,and CARLs. Extensions for use with and also for ACRLs and AARLs are defined in clause 17.

## 9.1 Policy handling

### 9.1.1 Certificate policy

In the old 8.1.1, which is now 9.1.1, change the subclause as shown:

This framework contains three four types of entity: the relying party, the CA, the trust broker and the certificate subject (or end-entity). Each entity operates under obligations to some of the other two entities and, in return, enjoys limited warranties offered by them. These obligations and warranties of a CA are defined in its certificate policy. A certificate policy is a document (usually in plain-language, but it could be machine readable). It may be referenced by an object identifier and a URL, which may be included in the certificate policies extension of the certificate issued by the CA, to the end-entity and upon which the relying party relies. A certificate may be issued in accordance with one or more than one policy. Definition of the policy, and assignment of the identifier, is performed by a policy authority. The set of policies administered by a policy authority is called a policy domain. All certificates are issued in accordance with a policy, even if the policy is neither recorded anywhere nor referenced in the certificate. This Directory Specification does not prescribe the style or contents of the certificate policy.

The trust broker relying party may be bound to any relying party its obligations under the certificate policy by the act of importing an authority public key and using it as trust anchor information, or by informing a relying party that it may relying on a certificate that includes the associated policy identifier. The CA may be bound to its obligations under the policy by the act of issuing a certificate that includes the associated policy identifier. The certificate subject, and any relying party who is also a certificate subject, end-entity may be bound to its obligations under the policy by the act of requesting and accepting a certificate that includes the associated policy identifier and by using the corresponding private key. Implementations that do not use the certificate policies extension should achieve the required binding by some other means.

The relying party and trust broker may be bound by any contractual agreement that they have or by any trust policy that the trust broker issues.

For an entity simply to declare conformance to a policy does not generally satisfy the assurance requirements of the other entities in the framework. They require some reason to believe that the other parties operate a reliable implementation of their policy. However, if explicitly so stated in the certificate policy, relying parties may accept the CA's assurances that its subjects end-entities agree to be bound by their obligations under the policy, without having to confirm this directly with them. This aspect of certificate policy is outside the scope of this Directory Specification.

A CA may place limitations on the use of its certificates, in order to control the risk that it assumes as a result of issuing certificates. For instance, it may restrict the community of relying parties, the purposes for which they may use its certificates and/or the type and extent of damages that it is prepared to make good in the event of a failure on its part, or that of its end-entities. These matters should be defined in the certificate policy.

Additional information, to help affected entities understand the provisions of the certificate policy, may be included in the certificate policies extension in the form of policy qualifiers.

### 9.1.2 Cross-certificates

In the old 8.1.2, which is now 9.1.2, change the second paragraph as shown:

A certification path is said to be valid under the set of certificate policies that are common to all public-key certificates in the path.

### 9.3.2 Certificate and CRL extension fields

#### 9.3.2.3 Subject directory attributes extension

In the old 8.3.3.3, which is now 9.3.3.2, change the first paragraph as shown:

This field conveys any desired privilege Directory attributes associated with the subject of the certificate (see clause 13.2 for further details). This field is defined as follows:

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

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