INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.509

Corrigendum 3
(10/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Directory

Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

Technical Corrigendum 3

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/.

INTERNATIONAL STANDARD ISO/IEC 9594-8:2014
RECOMMENDATION ITU-T X.509 (2012)

Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

Technical Corrigendum 3

(Covering resolution to defect reports 421, 422, 423, 424 and 425)

1) Correction of the defects reported in defect report 421.

In clause 13, replace item e) with

e) When identity and/or privilege information is conveyed within the **`subjectDirectoryAttributes`** extension of a public-key certificate, the AA is then responsible for those aspects of the CA that relate to assigning identity and/or privilege information. The AA may either be a separate entity or and integrated part of the CA.

Update 13.2 as shown:

13.2 Privilege in public-key certificates

In some environments,~~ privileges are associated with the subject through the practices of a CA. Such~~ privilege may be added directly to public-key certificates (thereby reusing much of an already-established infrastructure), rather than issuing attribute certificates. In such cases, the privilege is included in the **`subjectDirectoryAttributes`** extension of the public-key certificate.

This mechanism is suitable in environments where one or more of the following are true:

- ~~The same physical entity is acting both as a CA and an AA;~~
- the lifetime of the privilege is aligned with that of the public-key ~~included in the~~ certificate;
- delegation of privilege is not permitted; or
- delegation is permitted, but for any one delegation, all privileges in the certificate (in the **`subjectDirectoryAttributes`** extension) have the same delegation parameters and all extensions relevant to delegation apply equally to all privileges in the certificate.

2) Correction of the defects reported in defect report 422

In clause 8.3.2.1, replace the paragraph right after the bullet list with the following:

For every name form used in an instance of the **`GeneralName`** data type, the issuing CA shall assure that it does not allocate the same name to different entities. A name of a particular type together with the identity of the issuing CA shall uniquely identify a particular entity.

3) Correction of the defects reported in defect report 423

Update first paragraph of clause 15.3.2.1.1 as shown:

This extension may only be present in a public-key certificate issued to an SOA. It shall not be included in attribute certificates or public-key certificates issued to other AAs.

The SOA identifier extension indicates that the public-key certificate subject may act as an SOA for the purposes of privilege management. As such, the public-key certificate subject may define attributes that assign privilege, issue attribute descriptor certificates for those attributes and use the private key corresponding to the certified public key to issue attribute certificates that assign privileges to holders. If the public key certificate is a CA certificate, the subject of that CA certificate may also issue ~~Those subsequent certificates may be attribute certificates or~~ public-key certificates with a **`subjectDirectoryAttributes`** extension containing the privileges.

Delete the second paragraph after the ASN.1

~~This field may only be present in a public-key certificate issued to an SOA. It shall not be included in attribute certificates or public-key certificates issued to other AAs or to end-entity privilege holders.~~

4) Correction of the defects reported in defect report 424

Add the following two new definitions to clause 3.5:

3.5.x **intermediate CA**: A CA is acting as an intermediate CA within a certification path when it is the issuer of the next public-key certificate on that certification path.

3.5.x **subject CA:** A CA for which another CA has issued a CA certificate.

5) Correction of the defects reported in defect report 425

Change the first paragraph of 8.2.2.5 as shown:

This ~~field~~ extension indicates the period of use of the private key corresponding to the certified public key. It is applicable only for private ~~digital signature~~ keys used for creating digital signatures. This ~~field~~ extension is defined as follows:

Change NOTE 1 of 8.2.2.5 as shown:

> NOTE 1 – The period of valid use of the private key may be different from the certified validity of the public key as indicated by the public-key certificate validity period. ~~With digital signature keys, t~~The usage period for the ~~signing~~ private key used for signing is typically shorter than that for the ~~verifying~~ public key used for verifying the signature.

Replace NOTE 2 of 8.2.2.5 with the following

> NOTE 2 – The period of use of the private key corresponding to a public key can only be enforced if both the private key and the corresponding public-key certificate are placed in a tamper resistant hardware module that contains a reliable clock synchronized with UTC. When this is not the case, a signer may avoid using a signing private key up to the very end of the validity period of the public-key certificate. This is one possible use of this extension

Add a new NOTE 3 to 8.2.2.5:

> NOTE 3 – In general, this Specification does not associate any semantic with this extension. Any particular use of this extension will have to specify the semantic associated with that usage.