INTERNATIONAL STANDARD ISO/IEC 9594-8:2014
TECHNICAL CORRIGENDUM 3

Published 2016-12-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Information technology — Open Systems Interconnection — The Directory —

Part 8:
Public-key and attribute certificate frameworks

TECHNICAL CORRIGENDUM 3

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'annuaire —

Partie 8: Cadre général des certificats de clé publique et d'attribut

RECTIFICATIF TECHNIQUE 3

Technical Corrigendum 3 to ISO/IEC 9594-8:2014 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems.* The identical text is published as Rec. ITU-T X.509 (2012)/ Cor.3 (04/2016).

ICS 35.100.70 **Ref. No. ISO/IEC 9594-8:2014/Cor.3:2016(E)**

Published in Switzerland

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

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 the 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.~~