



INTERNATIONAL STANDARD ISO/IEC 9594-8:2014
TECHNICAL CORRIGENDUM 1

Published 2015-10-01

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 1

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 1

Technical Corrigendum 1 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*.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION**Information technology – Open Systems Interconnection –
The Directory: Public-key and attribute certificate frameworks****Technical Corrigendum 1***(Covering resolution to defect reports 389, 390, 393, 394, 395, 397, 398, 399, 400, 401, 402, 403, 404 and 405)***1) Correction of the defects reported in defect report 389***Replace clause 3.5.61 with the following:*

3.5.61 self-issued attribute certificate: An attribute certificate where the issuer and the holder are the same attribute authority. An attribute authority might use a self-issued attribute certificate, for example, to publish policy information.

2) Correction of the defects reported in defect report 390*Delete the last paragraph of clause 8.6.2.***3) Correction of the defects reported in defect report 393***Replace the last paragraph of clause 8.5.2.9 with:*

The scope of a CRL containing this extension is extended to include the revocation status of revoked certificates that expired after the date specified in **ExpiredCertsOnCRL** or at that date. The revocation status of a certificate shall not be updated once the certificate has expired.

4) Correction of the defects reported in defect report 394*Add the following references to clause 2.4*

- IETF RFC 5914 (2010), *Trust Anchor Format*.

Add a new definition to clause 3.5:

3.5.68 trust anchor store: A trust anchor information collection at a relying party for one or more trust anchors.

*Replace clause 7.5 with:***7.5 Trust anchor**

An entity is a trust anchor for a particular relying party for one or more purposes, typically including certificate validation. A trust anchor is identified by trust anchor information. Trust anchor information includes a public key and some associated data. This trust anchor information is configured into the relying party in a trust anchor store. A relying party may have configured information about multiple trust anchors into one or more trust anchor stores.

A trust anchor may be a CA that issues public-key certificates and certificate revocation lists (CRLs) (see clause 7.10). The relying party may then use the trust anchor information for public-key certificate and CRL validation.

A trust anchor may also function as an end entity by signing other types of information such as software packages, time stamps, responses to online certificate status protocol (OCSP) requests (see IETF RFC 6960), etc.

A CA may be a trust anchor for some entities with respect to particular public-key certificates, but may otherwise be an ordinary CA.

NOTE 1 – As an example, entities within a company may trust all the public-key certificates issued by the company CA. This CA is then the trust anchor for these local relying parties with respect to locally issued public-key certificates. However, by use of name constraints, it might not be a trust anchor with respect to public-key certificates issued outside the company. Likewise, relying parties outside the company may not consider the company CA as the trust anchor for any public-key certificates.

NOTE 2 – The term trust anchor is seen as synonymous with the term root-CA. In a strict hierarchy, the CA at the top of the hierarchy may be the root CA and it may also be a trust anchor. However, in more complex environments, it may not be possible