



INTERNATIONAL STANDARD ISO/IEC 9594-8:2001
TECHNICAL CORRIGENDUM 3

Published 2005-03-01

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: Public-key and attribute certificate frameworks

TECHNICAL CORRIGENDUM 3

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'annuaire: Cadre général des certificats de clé publique et d'attribut

RECTIFICATIF TECHNIQUE 3

Technical Corrigendum 3 to ISO/IEC 9594-8:2001 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 RECOMMENDATIONInformation technology – Open Systems Interconnection –
The Directory: Public-key and attribute certificate frameworks

Technical Corrigendum 3

(Covering resolutions to defect reports 281, 282, 289, 291, 296, 298, 299, 300, 301, 304 and 305)

A previously approved, but unpublished version of this TC contained text to resolve DR280. Subsequent to the ballot approval of the DTC resolving DR280, implementers discovered that the method introduced into the 4th edition to handle both Public-key and Attribute revocation was seriously flawed. The text resolving DR305 brings the method specified in the 3rd edition forward into the 4th edition. Since publishing the text resolving DR280 is no longer appropriate and may confuse those implementing products conforming to the 4th edition, the text to resolve DR280 is removed from this version of the TC.

1) This corrects the defects reported in defect report 281

In clause 8.6.2.6, add the following paragraph after the ASN.1:

The value of type **CRLDistPointsSyntax** is as defined in the CRL distribution points extension in 8.6.2.1.

Replace the existing subclause B.5.1.4 with the following:

In order to determine that a CRL is one of the CRLs indicated by a distribution point in the CRL distribution point extension or freshest CRL extension, all of the following conditions shall be true:

- Either the distribution point field in the CRL's issuing distribution point extension shall be absent (only when not looking for a critical CRL DP), or one of the names in the distribution point field of the CRL DP or freshest CRL extension shall match one of the names in the distribution point field in the issuing distribution point extension of the CRL. Alternatively, one of the names in the **cRLIssuer** field of the CRL DP or freshest CRL extension can match one of the names in DP of the IDP; and
- If the certificate is an end entity certificate, the CRL shall not contain **onlyContainsAuthorityCerts** field set to **TRUE** in the issuing distribution point extension of the CRL; and
- If **onlyContainsAuthorityCerts** is set to **TRUE** in the issuing distribution point extension of the CRL, then the certificate being checked shall contain the **basicConstraints** extension with the **ca** component set to **TRUE**; and
- If the **reasons** field is present in the CRL DP or freshest CRL extension, the **onlySomeReasons** field shall be either absent from the issuing distribution point extension of the CRL or contain at least one of the reason codes asserted in the CRL DP or freshest CRL extension; and
- If the **cRLIssuer** field is absent from the relevant extension (either CRL DP or freshest CRL), the CRL shall be signed by the same CA that signed the certificate; and
- If the **cRLIssuer** field is present in the relevant extension (CRL DP or freshest CRL), the CRL shall be signed by the CRL issuer identified in the **cRLIssuer** field and the CRL shall contain the issuing distribution point extension with the **indirectCRL** field set to **TRUE**.

NOTE – When testing the **reasons** and **cRLIssuer** field for presence, the test succeeds only if the field is present in the same **DistributionPoint** of the CRL DP or freshest CRL extension for which there is a name match in the corresponding distribution point field of the IDP extension in the CRL.

2) This corrects the defects reported in defect report 282

In clause 7, in the paragraph immediately following the definition of the version field and in the paragraph immediately following the definition of the extensions field, replace:

"documented in 7.5.2.2 in ITU-T Rec. X.519 | ISO/IEC 9594-5"

with:

"documented in 12.2.2 in ITU-T Rec. X.519 | ISO/IEC 9594-5".

In clause 7.3, immediately following Note 6 and in clause 12.1 immediately following the definition of the extensions field, add the following new paragraph:

"If unknown elements appear within the extension, and the extension is not marked critical, those unknown elements shall be ignored according to the rules of extensibility documented in 12.2.2 in ITU-T Rec. X.519 | ISO/IEC 9594-5."

3) This corrects the defects reported in defect report 289

Replace the text of clause 10.1, item c, with the following:

- c) an *initial-policy-set* comprising one or more certificate policy identifiers, indicating that any one of these policies would be acceptable to the certificate user for the purposes of certification path processing; this input can also take the special value *any-policy*, but it cannot be null;

Replace clause 10.5.4, in its entirety, with the following:

10.5.4 Final processing

Once all certificates in the path have been processed, the following actions are then performed:

- a) Determine the *authorities-constrained-policy-set* from the *authorities-constrained-policy-set* table. If the table is empty, then the *authorities-constrained-policy-set* is the empty or null set. If the *authorities-constrained-policy-set*[0, *path-depth*] is *any-policy*, then the *authorities-constrained-policy-set* is *any-policy*. Otherwise, the *authorities-constrained-policy-set* is, for each row in the table, the value in the left-most cell which does not contain the identifier *any-policy*.
- b) Calculate the *user-constrained-policy-set* by forming the intersection of the *authorities-constrained-policy-set* and the *initial-policy-set*.
- c) If the *explicit-policy-indicator* is set, check that neither the *authorities-constrained-policy-set* nor the *user-constrained-policy-set* is empty.

If any of the above checks were to fail, then the procedure shall terminate, returning a failure indication, an appropriate reason code, the *explicit-policy-indicator*, the *authorities-constrained-policy-set* and the *user-constrained-policy-set*. If the failure is due to an empty *user-constrained-policy-set*, then the path is valid under the authority-constrained policy(s), but none is acceptable to the user.

If none of the above checks were to fail on the end certificate, then the procedure shall terminate, returning a success indication together with the *explicit-policy-indicator*, the *authorities-constrained-policy-set* and the *user-constrained-policy-set*.

4) This corrects the defects reported in defect report 291

In clause 3.3.44, in the definition of "public-key certificate", replace "unforgeable by encipherment" with "unforgeable by digital signature".

In clause 3.1, add "digital signature" to the list of terms defined in CCITT Rec. X.800 | ISO 7498-2. Add it in alphabetical order and renumber the remaining items in the list.