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.*

ICS 35.100.70 **Ref. No. ISO/IEC 9594-8:2001/Cor.3:2005(E)**

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information 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A previously approved, but unpublished version of this TC contained text to resolve DR280.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.*

5) This corrects the defects reported in defect report 296

*In clause B.5.1.1, in the first sentence, add "*issued by the CRL issuer" *immediately after "*and CA-certificates*".*

In clause B.5.1.1, replace the 3rd bullet with the following:

– Either the issuing distribution point extension shall not contain distribution point field or one of the names in the distribution point field shall match the **issuer** field in the CRL; and

In clause B.5.1.2, replace the 3rd bullet with the following:

– Either the issuing distribution point extension shall not contain distribution point field or one of the names in the distribution point field shall match the **issuer** field in the CRL; and

In clause B.5.1.3, replace the 3rd bullet with the following:

– Either the issuing distribution point shall not contain distribution point field or one of the names in the distribution point field shall match the **issuer** field in the CRL; and

In clause B.5.1.4, in the first bullet, replace the last sentence with the following:

– Alternatively, if the distribution point field is absent from the certificate's CRL DP, one of the names in the **cRLIssuer** field of the certificate's CRL DP can match one of the names in DP of the IDP. If both the distribution point and the **cRLIssuer** fields are absent from the certificate's CRL DP, the certificate's **issuer** field can match one of the names in the DP of the IDP; and

6) This corrects the defects reported in defect report 298

In clause 7.3, add a new list item "d" to the list that is introduced by the sentence "An authority that issues and subsequently revokes certificates:" as follows:

d) if using only partitioned CRLs, shall issue a full set of partitioned CRLs covering the complete set of certificates whose revocation status will be reported using the CRL mechanism. Thus the complete set of partitioned CRLs shall be equivalent to a full CRL for the same set of certificates, if the CRL issuer was not using partitioned CRLs.

In clause 8.6.2.2, add the following as new text immediately after the first sentence:

If using only partitioned CRLs, the full set of partitioned CRLs shall cover the complete set of certificates whose revocation status will be reported using the CRL mechanism. Thus the complete set of partitioned CRLs shall be equivalent to a full CRL for the same set of certificates, if the CRL issuer was not using partitioned CRLs.

7) This corrects the defects reported in defect report 299

Insert the following paragraphs as a new subclause 7.4:

7.4 Repudiation of a digital signing

Any participant in an event may subsequently decide to repudiate anything that participant digitally signed in that event. For example, one can dispute one's participation in a key establishment or being the originator of a signed email message as easily as one can dispute one's signing a document with the intent to be bound to the content of that document. The repudiation may not be successful. The Non-repudiation Framework, ITU-T Rec. X.813 | ISO/IEC 10181-4, describes a dispute resolution process as follows:

1) evidence generation;
2) evidence transfer, storage and retrieval;
3) evidence verification; and
4) dispute resolution.

The generated evidence may include, but is not limited to:

– audit records pertinent to the event and assertion of intent;
– statements made by third party notaries;
– policy statements;
– digitally signed information, including audit records and notary statements;

- timestamps of the digitally signed information;
- the certificates supporting the digital signature;
- the appropriate revocation information published and available at the time of the disputed event; and
- any certificate revocations subsequent to the time of the event which indicate key compromise occurred before the time of the event.

The integrity of stored data that might be presented as evidence may be maintained in a variety of ways, e.g. access control, storage of hashes by trusted third party, digital signature. It may also be necessary to periodically strengthen the protection of that stored data to counteract improvements in computer processing and/or crypto-analysis.

NOTE – Neither the type and amount of evidence generated nor the level of integrity is specified by this Directory Specification. However it is expected that the level of effort will be commensurate with the risk involved.

Evidence verification may require the revalidation of the digital signatures of data, e.g. messages, documents, certificates, CRLs, and timestamps that were used in the initial validation process. The fact that a certificate has expired shall not preclude its use for revalidating signatures created during the validity period of that certificate. A certificate that has been revoked may be used if it can be determined that the certificate was valid at the time of the disputed event.

Even if all the digital evidence described above is considered technically valid, other conditions, e.g. the intent, understanding, or competence of the signer, may allow the signer to successfully repudiate it.

Replace clause 8.2.2.3 with the following:

8.2.2.3 Key usage extension

This field identifies the intended usage for which the certificate has been issued. The intended usage may be further constrained by policy. This policy may be stated in a certificate policy definition, a contract, or other specification. However, a policy shall not override the constraint indicated by a **KeyUsage** bit, e.g. a certificate policy could not allow a certificate to be used for digital signature if **KeyUsage** indicated that it could only be used for key agreement.

Setting a specific value of **KeyUsage** in a certificate does not in itself signal for an instance of communication that the communicating parties are acting in accordance with this setting, e.g. when signing a document. Definition of methods by which parties may signal their intent for a specific instance of communication (e.g. commitment to content for that specific instance) is outside the scope of this Directory Specification, but it is anticipated that multiple methods will exist. Although not recommended, it is possible to use the content of the certificate, e.g. certificate policy, to signal the intent of the signing. However, since that signal was made when the certificate was issued by the CA, such use may not meet the requirement that declaring the intent is made at the time of signing by the signer.

More than one bit may be set in an instance of the **keyUsage** extension. The setting of multiple bits shall not change the meaning of each individual bit but shall indicate that the certificate may be used for all of the purposes indicated by the set bits. There may be risks incurred when setting multiple bits. A review of those risks is documented in the informative annex tbd. The text proposed in AFNOR comment 4 from the Summary of Voting on DTC-6, SC6 N12648, will be included in that annex.

This field is defined as follows:

```
keyUsage EXTENSION ::= {
        SYNTAX                  KeyUsage
        IDENTIFIED BY           id-ce-keyUsage }

KeyUsage ::= BIT STRING {
        digitalSignature        (0),
        contentCommitment       (1),
        keyEncipherment         (2),
        dataEncipherment        (3),
        keyAgreement            (4),
        keyCertSign             (5),
        cRLSign                 (6),
        encipherOnly            (7),
        decipherOnly            (8) }
```

Bits in the **KeyUsage** type are as follows:

a) **digitalSignature**: for verifying digital signatures that are used with an entity authentication service, a data origin authentication service and/or an integrity service;

b) **contentCommitment**: for verifying digital signatures which are intended to signal that the signer is committing to the content being signed. The type of commitment the certificate can be used to support may be further constrained by the CA, e.g. through a certificate policy. The precise type of commitment of the signer e.g. "reviewed and approved" or "with the intent to be bound", may be signalled by the content being signed, e.g. the signed document itself or some additional signed information.

Since a content commitment signing is considered to be a digitally signed transaction, the **digitalSignature** bit need not be set in the certificate. If it is set, it does not affect the level of commitment the signer has endowed in the signed content.

Note that it is not incorrect to refer to this **keyUsage** bit using the identifier **nonRepudiation**. However, the use of this identifier has been deprecated. Regardless of the identifier used, the semantics of this bit are as specified in this Directory Specification;

c) **keyEncipherment**: for enciphering keys or other security information, e.g. for key transport;

d) **dataEncipherment**: for enciphering user data, but not keys or other security information as in c) above;

e) **keyAgreement**: for use as a public key agreement key;

f) **keyCertSign**: for verifying a CA's signature on certificates.

Since certificate signing is considered to be a commitment to the content of the certificate by the CA, neither the **digitalSignature** bit nor the **contentCommitment** bit need be set in the certificate. If either (or both) is set, it does not affect the level of commitment the signer has endowed in the signed certificate;

g) **cRLSign**: for verifying an authority's signature on CRLs.

Since CRL signing is considered to be a commitment to the content of the CRL by the CRL issuer, neither the **digitalSignature** bit nor the **contentCommitment** bit need be set in the certificate. If either (or both) is set, it does not affect the level of commitment the signer has endowed in the signed CRL;

h) **encipherOnly**: public key agreement key for use only in enciphering data when used with **keyAgreement** bit also set (meaning with other key usage bit set is undefined);

i) **decipherOnly**: public key agreement key for use only in deciphering data when used with **keyAgreement** bit also set (meaning with other key usage bit set is undefined).

Application specifications should indicate which of the **digitalSignature** or **contentCommitment** bits are appropriate for their use. If a signing application has no knowledge of the signer's intent regarding commitment to content, the application shall sign and support that signing with a certificate that has the **digitalSignature** bit set in that certificate's **keyUsage** extension.

Even though a digital signature was verified using a certificate that has only the **digitalSignature** bit set, other factors external to the verification of the digital signature may also play a role in determining the intent of the signing. Conversely, even though a digital signature was verified using a certificate that has only the **contentCommitment** bit set, external factors may be used by the signer to disclaim commitment to the signed content.

The bit **keyCertSign** is for use in CA-certificates only. If **KeyUsage** is set to **keyCertSign**, the value of the **cA** component of the **basicConstraints** extension shall be set to **TRUE**. CAs may also use other defined key usage bits in **KeyUsage**, e.g. **digitalSignature** for providing authentication and integrity of online administration transactions.

This extension may, at the option of the certificate issuer, be either critical or non-critical.

If the extension is flagged critical or if the extension is flagged non-critical but the certificate-using system recognizes it, then the certificate shall be used only for a purpose for which the corresponding key usage bit is set to one. If the extension is flagged non-critical and the certificate-using system does not recognize it, then this extension shall be ignored. A bit set to zero indicates that the key is not intended for that purpose. If the extension is present with all bits set to zero, the key is intended for some purpose other than those listed above.

8) This corrects the defects reported in defect report 300

In clause 10.5.1, item b, replace the first sentence with the following:

For an intermediate version 3 certificate, check that **basicConstraints** is present and that the **cA** component in the **basicConstraints** extension is TRUE.

9) This corrects the defects reported in defect report 301

In clause B.5.2, second sentence, third bullet, replace the sentence with the following:

The base CRL is the CRL referenced in the dCRL or a later one.

10) This corrects the defects reported in defect report 304

In Annex F, move the statement:

id-ea-rsa OBJECT IDENTIFIER ::= {id-ea 1}

to right after the following text:

"-- the following object identifier assignments reserve values assigned to deprecated functions"

Delete:

-- object identifier assignments --

11) This corrects the defects reported in defect report 305

In clause 8.6.2 add a new list item c) as follows and renumber the existing list items c) through f) to d) through g) accordingly:

c) AAissuingDistributionPoint;

In clause 8.6.2, replace the second sentence of the last paragraph with the following:

Issuing distribution point, AA issuing distribution point, delta CRL indicator and base update shall be used only as CRL extensions.

In clause 8.6.2, add the following paragraph to the end of the clause, immediately before clause 8.6.2.1:

While the issuing distribution point extension and the AA issuing distribution point extension serve similar purposes, they apply to different certificates. The issuing distribution point extension applies only to public key certificates issued to users and/or CAs. The AA issuing distribution point extension applies only to attribute certificates issued to users and AAs as well as public-key certificates issued to SOAs. If a single CRL covers certificate types that span these, then that CRL would need to include both extensions. Note that the CRL scope extension defined in 8.5.2.5 is also similar to these two extensions. However, that extension is known to be flawed and its usage is deprecated. The issuing distribution point extension and/or AA issuing distribution point extension should be used instead of the CRL scope extension.

In clause 8.5.2.5 (CRL scope extension), replace the following paragraph:

Note that the **issuingDistributionPoint** extension and **crlScope** extension can conflict with each other and are not intended to be used together. However, if the CRL contains both an **issuingDistributionPoint** extension and a **crlScope** extension, then a certificate falls within the scope of the CRL if and only if it meets the criteria of both extensions. If the CRL contains neither an **issuingDistributionPoint** nor **crlScope** extension, then the scope is the entire scope of the authority, and the CRL may be used for any certificate from that authority.

with:

Note that the **issuingDistributionPoint** extension and **crlScope** extension can conflict with each other and are not intended to be used together. However, if the CRL contains both an **issuingDistributionPoint** extension and a **crlScope** extension, then a public-key certificate falls within the scope of the CRL if and only if it meets the criteria of both extensions. If the CRL contains an **AAissuingDistributionPoint** extension, but does not contain an **issuingDistributionPoint** or **crlScope** extension, then the scope does not include public-key certificates. If the CRL does not contain an **issuingDistributionPoint**, **AAissuingDistributionPoint**, or **crlScope** extension, then the scope is the entire scope of the authority, and the CRL may be used for any certificate from that authority. Similarly, the **AAissuingDistributionPoint** extension and **crlScope** extension can conflict with each other and are not intended to be used together. However, if the CRL contains both an **AAissuingDistributionPoint** extension and a **crlScope** extension, then an attribute certificate falls within the scope of the CRL if and only if it meets the criteria of both extensions. If the CRL contains an **issuingDistributionPoint** extension, but does not contain an **AAissuingDistributionPoint** or **crlScope** extension, then the scope does not include attribute certificates. If the CRL does not contain an