INTERNATIONAL STANDARD ISO/IEC 9594-8:1998
TECHNICAL CORRIGENDUM 1

Published 2000-12-15

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: Authentication framework

TECHNICAL CORRIGENDUM 1

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'Annuaire: Cadre d'authentification

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to International Standard ISO/IEC 9594-8:1998 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 9594-8:1998/Cor.1:2000(E)**

Printed in Switzerland

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – THE DIRECTORY: AUTHENTICATION FRAMEWORK

TECHNICAL CORRIGENDUM 1

1) Resolution to defect report 9594/200

Subclause 12.6.2

Add the following at the end of the paragraph beginning with "If this extension is flagged critical ...":

"Where the distribution points are used to distribute CRL information for all revocation reason codes and all certificates issued by the CA include the **crlDistributionPoint** as a critical extension, the CA is not required to also publish a full CRL at the CA entry."

2) Resolution to defect report 9594/201

Subclause 12.6.3.1

Move the second sentence of the second paragraph "If this field is absent …CRL issuer." *to the first paragraph immediately before the sentence* "This field is defined as follows:":

Add a paragraph break following the relocated sentence, making "This field is defined as follows:" *as an independent paragraph immediately before the ASN.1.*

3) Resolution to defect report 9594/212

Subclause 12.7.6

Add the following to subclause 12.7.6:

"g) **authorityKeyIdentifier** matches if the value of this component in the stored attribute value equals that in the presented value; there is no match if the stored attribute value contains no authority key identifier extension or if not all components in the presented value are present in the stored attribute value."

4) Resolution to defect report 9594/213

Subclause 12.7.6 d)

Replace the text of 12.7.6 d) with the following:

"d) **reasonFlags** matches if any of the bits that are set in the presented value are also set in the **onlySomeReasons** components of the issuing distribution point extension of the stored attribute value; there is also a match if the stored attribute value contains no **reasonFlags** in the issuing distribution point extension, or if the stored attribute value contains no issuing distribution point extension;

NOTE – Even though a CRL matches on a particular value of **reasonFlags**, the CRL may not contain any revocation notices with that reason code."

5) Resolution to defect report 9594/218

Subclause 12.7.2 j)

Replace the text of 12.7.2 j) with the following:

"j) **policy** matches if at least one member of the **CertPolicySet** presented appears in the certificate policies extension in the stored attribute value; there is no match if there is no certificate policies extension in the stored attribute value;"

6) Resolution to defect report 9594/220

Subclause 11.2, Note 3

In Note 3, in the second sentence, replace "shall be absent" *with* "may be absent".

In Note 3, at the beginning of the 3rd sentence, replace "This may permit" *with* "If **version** is absent, this may permit".

In Note 3, at the beginning of the 4th sentence, replace "An implementation that supports version 2 (or greater) CRLs may" *with* "An implementation that supports version 2 (or greater) CRLs, in the absence of **version**, may also ...".

7) Resolution to defect report 9594/185

Clause 8

Add the following text immediately following the ASN.1 for **certificatePair**:

"The **cACertificate** attribute of a CA's directory entry shall be used to store self-issued certificates (if any) and certificates issued to this CA by CAs in the same realm as this CA.

The **forward** elements of the **crossCertificatePair** attribute of a CA's directory entry shall be used to store all, except self-issued certificates issued to this CA. Optionally, the **reverse** elements of the **crossCertificatePair** attribute, of a CA's directory entry may contain a subset of certificates issued by this CA to other CAs. When both the **forward** and the **reverse** elements are present in a single attribute value, issuer name in one certificate shall match the subject name in the other and vice versa, and the subject public key in one certificate shall be capable of verifying the digital signature on the other certificate and vice versa.

When a **reverse** element is present, the forward element value and the reverse element value need not be stored in the same attribute value; in other words, they can be stored in either a single attribute value or two attribute values.

In the case of v3 certificates, none of the above CA certificates shall include a **basicConstraints** extension with the **cA** value set to **FALSE**.

The definition of realm is purely a matter of local policy."

Also, replace Figure 4 with the following:

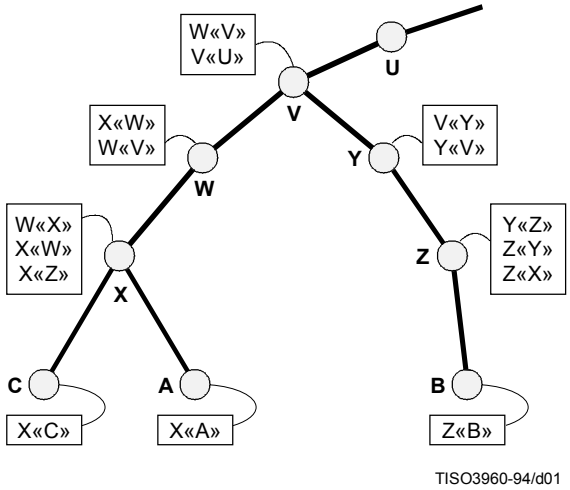

Figure 4 – Certification path – hypothetical example

8) Resolution to defect report 9594/204

Subclause 12.6.3.1

In the first sentence following the ASN.1, delete "unexpired".

Add the following as a new second sentence in the first paragraph following the ASN.1:

"After a certificate appears on a CRL, it may be deleted from a subsequent CRL after the certificate's expiry."

9) Resolution to defect report 9594/222

Add the following to subclause 12.1:

"Certificate policy

The authentication framework contains three types of entity: the certificate user, the certification authority and the certificate subject (or end-entity). Each entity operates under obligations to the other two entities and, in return, enjoys limited warranties offered by them. These obligations and warranties are defined in a certificate policy. A certificate policy is a document (usually in plain-language). It can be referenced by a unique identifier, which may be included in the certificate policies extension of the certificate issued by the certification authority, to the end-entity and upon which the certificate user relies. A certificate may be issued in accordance with one or more than one policy. Definition of the policy, and assignment of the identifier, are performed by a policy authority. And the set of policies administered by a policy authority is called a policy domain. All certificates are issued in accordance with a policy, even if the policy is neither recorded anywhere nor referenced in the certificate. The Recommendation | International Standard does not prescribe the style or contents of the certificate policy.

The certificate user may be bound to its obligations under the certificate policy by the act of importing an authority public key and using it as a trust anchor, or by relying on a certificate that includes the associated policy identifier. The certification authority may be bound to ***its*** obligations under the policy by the act of issuing a certificate that includes the associated policy identifier. And, the end-entity may be bound to ***its*** obligations under the policy by the act of requesting and accepting a certificate that includes the associated policy identifier and by using the corresponding private key. Implementations that do not use the certificate policies extension should achieve the required binding by some other means.

For an entity to simply declare conformance to a policy does not generally satisfy the assurance requirements of the other entities in the framework. They require some reason to believe that the other parties operate a reliable implementation of the policy. However, if explicitly so stated in the policy, certificate users may accept the certification authority's assurances that its end-entities agree to be bound by their obligations under the policy, without having to confirm this directly with them. This aspect of certificate policy is outside the scope of the Recommendation | International Standard.

A certification authority may place limitations on the use of its certificates, in order to control the risk that it assumes as a result of issuing certificates. For instance, it may restrict the community of certificate users, the purposes for which they may use its certificates and/or the type and extent of damages that it is prepared to make good in the event of a failure on its part, or that of its end-entities. These matters should be defined in the certificate policy.

Additional information, to help affected entities understand the provisions of the policy, may be included in the certificate policies extension in the form of policy qualifiers.

Cross-certification

A certification authority may be the subject of a certificate issued by another certification authority. In this case, the certificate is called a cross-certificate, the certification authority that is the subject of the certificate is called the subject certification authority and the certification authority that issues the cross-certificate is called an intermediate certification authority (see Figure 1). Both the cross-certificate and the end-entity's certificate may contain a certificate policies extension.

The warranties and obligations shared by the subject certification authority, the intermediate certification authority and the certificate user are defined by the certificate policy identified in the cross-certificate, in accordance with which the subject certification authority may act as, or on behalf of, an end-entity. And the warranties and obligations shared by the certificate subject, the subject certification authority and the intermediate certification authority are defined by the certificate policy identified in the end-entity's certificate, in accordance with which the intermediate certification authority may act as, or on behalf of, a certificate user.

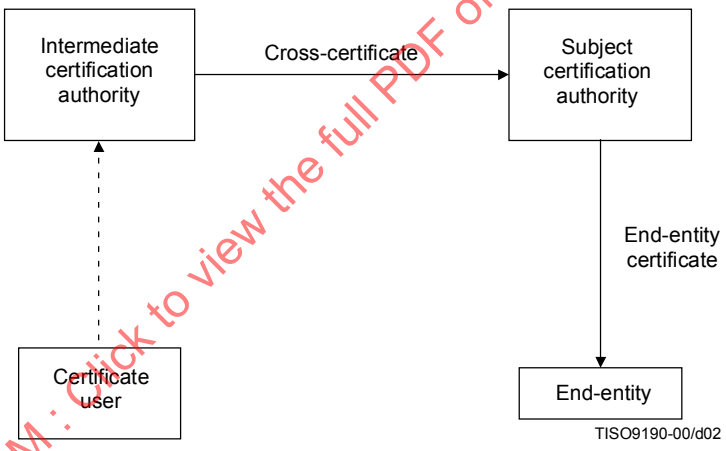

Figure 1 – Cross-certification

A certification path is said to be valid under the set of policies that are common to all certificates in the path.

An intermediate certification authority may, in turn, be the subject of a certificate issued by another certification authority, thereby creating certification paths of length greater than two certificates. And, since trust suffers dilution as certificate paths grow in length, controls are required to ensure that end-entity certificates with an unacceptably low associated trust level will be rejected by the certificate user. This is part of the function of the certification path processing procedure.

In addition to the situation described above, there are two special cases to be considered:

1) the certification authority does not use the certificate policies extension to convey its policy requirements to certificate users; and

2) the certificate user or intermediate certification authority delegates the job of controlling policy to the next authority in the path.

In the first case, the certificate should not contain a certificate policies extension at all. As a result, the set of policies under which the path is valid will be null. But, the path may be valid nonetheless. Certificate users must still ensure that they are using the certificate in conformance with the policies of the authorities in the path.

In the second case, the certificate user or intermediate certification authority should include the special value *any-policy* in the *initial-policy-set* or cross-certificate. Where a certificate includes the special value *any-policy*, it should not include any other certificate policy identifiers. The identifier *any-policy* should not have any associated policy qualifiers.

The certificate user can ensure that all its obligations are conveyed in accordance with the Recommendation | International Standard by setting the *initial-explicit-policy* indicator. In this way, only authorities that use the standard certificate policies extension as their way of achieving binding are accepted in the path, and certificate users have no additional obligations. Because authorities also attract obligations when they act as, or on behalf of, a certificate user, they can ensure that all their obligations are conveyed in accordance with the Recommendation | International Standard by setting **requireExplicitPolicy** in the cross-certificate.

Policy mapping

Some certification paths may cross boundaries between policy domains. The warranties and obligations according to which the cross-certificate is issued may be materially equivalent to some or all of the warranties and obligations according to which the subject certification authority issues certificates to end-entities, even though the policy authorities under which the two certification authorities operate may have selected different unique identifiers for these materially equivalent policies. In this case, the intermediate certification authority may include a policy mappings extension in the cross-certificate. In the policy mappings extension, the intermediate certification authority assures the certificate user that it will continue to enjoy the familiar warranties, and that it should continue to fulfill its familiar obligations, even though subsequent entities in the certification path operate in a different policy domain. The intermediate certification authority should include one or more mappings for each of a subset of the policies under which it issued the cross-certificate, and it should not include mappings for any other policies. If one or more of the certificate policies according to which the subject certification authority operates is identical to those according to which the intermediate certification authority operates (i.e. it has the same unique identifier), then these identifiers should be excluded from the policy mapping extension, but included in the certificate policies extension.

Policy mapping has the effect of converting all policy identifiers in certificates further down the certification path to the identifier of the equivalent policy, as recognized by the certificate user.

Policies should not be mapped either to or from the special value *any-policy*.

Certificate users may determine that certificates issued in a policy domain other than its own should not be relied upon, even though a trusted intermediate certification authority may determine its policy to be materially equivalent to its own. It can do this by setting the *initial-policy-mapping-inhibit* input to the path validation procedure. Additionally, an intermediate certification authority may make a similar determination on behalf of its certificate users. In order to ensure that certificate users correctly enforce this requirement, it can set **inhibitPolicyMapping** in a policy constraints extension.

Certification path processing

The certificate user faces a choice between two strategies:

1) it can require that the certification path be valid under at least one of a set of policies pre-determined by the user; or

2) it can ask the path validation module to report the set of policies for which the certification path is valid.

The first strategy may be most appropriate when the certificate user knows, a priori, the set of policies that are acceptable for its intended use.

The second strategy may be most appropriate when the certificate user does not know, a priori, the set of policies that are acceptable for its intended use.

In the first instance, the certification path validation procedure will indicate the path to be valid only if it is valid under one or more of the policies specified in the *initial-policy-set*, and it will return the sub-set of the *initial-policy-set* under which the path is valid. In the second instance, the certification path validation procedure may indicate that the path is invalid under the *initial-policy-set*, but valid under a disjoint set: the *authorities-constrained-policy-set*. Then the certificate user must determine whether its intended use of the certificate is consistent with one or more of the certificate policies under which the path ***is*** valid. By setting the *initial-policy-set* to *any-policy*, the certificate user can cause the procedure to return a valid result if the path is valid under any (unspecified) policy.

Self-issued certificates

There are three circumstances under which a certification authority may issue a certificate to itself:

1) as a convenient way of encoding its public key for communication to, and storage by, its certificate users;

2) for certifying key usages other than certificate and CRL signing (such as time-stamping); and

3) for replacing its own expired certificates.

These types of certificate are called self-issued certificates, and they can be recognized by the fact that the issuer and subject names present in them are identical. For purposes of path validation, self-issued certificates of type one are verified with the public key contained in them, and if they are encountered in the path, they shall be ignored.

Self-issued certificates of type two may only appear as end certificates in a path, and shall be processed as end certificates.

Self-issued certificates of type three (also known as self-issued intermediate certificates) may appear as intermediate certificates in a path. As a matter of good practice, when replacing a key that is on the point of expiration, a certification authority should request the issuance of any in-bound cross-certificates that it requires for its replacement public key before using the key. Nevertheless, if self-issued certificates are encountered in the path, they shall be processed as intermediate certificates, with the following exception: they do not contribute to the path length for purposes of processing the **pathLenConstraint** component of the **basicConstraints** extension and the *skip-certificates* values associated with the *policy-mapping-inhibit-pending* and *explicit-policy-pending* indicators."

In subclause 12.2.2.6, after the 2nd sentence of the 1st paragraph, add the following:

"The presence of this extension in an end-entity certificate indicates the certificate policies for which this certificate is valid. The presence of this extension in a certificate issued by one CA to another CA indicates the certificate policies for which this certificate can be used to validate certification paths."

Add the following text in subclause 12.2.2.6, after the 1st sentence of the 1st paragraph:

"The list of certificate policies is used in determining the validity of a certification path, as described in 12.4.3. The optional qualifiers are not used in the certification path processing procedure, but relevant qualifiers are provided as an output of that process to the certificate using application to assist in determining whether a valid path is appropriate for the particular transaction."

In subclause 12.2.2.7, replace the sentence "This extension is always non-critical." *with the following:*

"This extension may, at the option of the certificate issuer, be either critical or non-critical. It is recommended that it be critical, otherwise a certificate user may not correctly interpret the stipulation of the issuing CA."

Add the following new subclause 12.4.2.4:

"12.4.2.4 Inhibit any policy field

This field specifies a constraint that indicates any-policy is not considered an explicit match for other certificate policies for the remainder of the certification path.

```
inhibitAnyPolicy ::= EXTENSION {
        SYNTAX SkipCerts
IDENTIFIED BY {id-ce-inhibitAnyPolicy }}
```

This extension may, at the option of the certificate issuer, be either critical or non-critical. It is recommended that it be critical, otherwise a certificate user may not correctly interpret the stipulation of the issuing CA."

Add the following to the list of OIDs in the certificateExtensions module in Annex A:

"id-ce-inhibitAnyPolicy OBJECT IDENTIFIER ::= {id-ce 54}"

Replace subclause 12.4.3 with the following:

"**12.4.3 Certification path processing procedure**

Certification path processing is carried out in a system which needs to use the public key of a remote end entity, e.g. a system which is verifying a digital signature generated by a remote entity. The certificate policies, basic constraints, name constraints, and policy constraints extensions have been designed to facilitate automated, self-contained implementation of certification path processing logic.

The following is an outline of a procedure for validating certification paths. A conformant implementation shall be functionally equivalent to the external behaviour resulting from this procedure. But, the algorithm used by a particular implementation to derive the correct output(s) from the given inputs is not standardized.

The inputs to the certification path processing procedure are:

a) a set of certificates comprising a certification path;

b) a trusted public key value or key identifier (if the key is stored internally to the certification path processing module), for use in verifying the first certificate in the certification path;

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*;

d) an *initial-explicit-policy* indicator value, which indicates whether an acceptable policy identifier must appear in the certificate policies extension field of all certificates in the path;

e) an *initial-policy-mapping-inhibit* indicator value, which indicates whether policy mapping is forbidden in the certification path;

f) an *initial-inhibit-policy* indicator value, which indicates if the special value **anyPolicy**, if present in a certificate policies extension, is considered a match for any specific certificate policy value in a constrained set; and

g) the current date/time (if not available internally to the certification path processing module).

The values of c), d), e) and f) will depend upon the policy requirements of the user-application combination that needs to use the certified end-entity public key.

Note that because these are individual inputs to the path validation process, a certificate user may limit the trust it places in any given trusted public key to a given set of certificate policies. This can be achieved by ensuring that a given public key is the input to the process only when *initial-policy-set* input includes policies for which the certificate user trusts that public key. Since another input to the process is the certification path itself, this control could be exercised on a transaction by transaction basic.

The outputs of the procedure are:

a) an indication of success or failure of certification path validation;

b) if validation failed, a diagnostic code indicating the reason for failure;

c) the set of authorities-constrained policies and their associated qualifiers in accordance with which the certification path is valid, or the special value *any-policy*;

d) the set of user-constrained policies, formed from the intersection of the *authorities-constrained-policy-set* and the *initial-policy-set*;

e) *explicit-policy-indicator*, indicating whether the certificate user or an authority in the path requires that an acceptable policy be identified in every certificate in the path; and

f) details of any policy mapping that occurred in processing the certification path.

NOTE – If validation is successful, the certificate-using system may still choose not to use the certificate as a result of values of policy qualifiers or other information in the certificate.

The procedure makes use of the following set of state variables:

a) *authorities-constrained-policy-set*: A table of policy identifiers and qualifiers from the certificates of the certification path (rows represent policies, their qualifiers and mapping history, and columns represent certificates in the certification path);

b) *permitted-subtrees*: A set of subtree specifications defining subtrees within which all subject names in subsequent certificates in the certification path must fall, or may take the special value *unbounded*;