



NORME INTERNATIONALE ISO/CEI 9594-8:1998
RECTIFICATIF TECHNIQUE 2

Publié 2002-06-15

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

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

RECTIFICATIF TECHNIQUE 2

Information technology — Open Systems Interconnection — The Directory: Authentication framework

TECHNICAL CORRIGENDUM 2

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Le Rectificatif technique 2 à la Norme internationale ISO/CEI 9594-8:1998 a été élaboré par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 6, *Téléinformatique*.

<https://standards.iteh.ai/catalog/standards/sist/5dcb5566-4e80-4c26-b755-9159ed4c43c5/iso-iec-9594-8-1998-cor-2-2002>

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 9594-8:1998/Cor 2:2002

<https://standards.iteh.ai/catalog/standards/sist/5dcb356b-4e80-4c2b-b733-9159ed4c43c5/iso-iec-9594-8-1998-cor-2-2002>

**NORME INTERNATIONALE
RECOMMANDATION UIT-T**

**Technologies de l'information – Interconnexion des systèmes ouverts –
L'annuaire: cadre d'authentification**

CORRIGENDUM TECHNIQUE 2

NOTE – Ce corrigendum technique couvre les projets de Corrigenda techniques 8 et 9.

1) Relevés de défauts couverts par le projet de Corrigendum technique 8

(couvrant les résolutions relatives aux relevés de défauts 226, 227 et 240)

1.1) Ce qui suit rectifie les défauts figurant dans le relevé de défauts 226

Au § 11.2, supprimer le deuxième alinéa:

La production d'un certificat ... compromission improbable.

ITeH STANDARD PREVIEW
(standards.iteh.ai)

1.2) Ce qui suit rectifie les défauts figurant dans le relevé de défauts 227

Au § 12.2.2.1, ajouter les 2 phrases suivantes à la fin de l'alinéa qui commence par "Les autorités de certification doivent attribuer ..."

ISO/IEC 9594-8:1998/Cor 2:2002
<https://standards.iteh.ai/catalog/standards/sist/5dcb556b-4e80-4c26-b755-9159ed4c43c5/iso-iec-9594-8-1998-cor-2-2002>

On peut utiliser la forme **keyIdentifieur** pour sélectionner des certificats d'une autorité de certification pendant la construction de chemin. On ne peut utiliser la paire **authorityCertIssuer**, **authoritySerialNumber** que pour donner la préférence à un certificat par rapport aux autres pendant la construction de chemin.

1.3) Ce qui suit rectifie les défauts figurant dans le relevé de défauts 240

*Il convient d'apporter les corrections suivantes à l'édition de 1997 du module **authenticationFramework** donné à l'Annexe A:*

- 1) *Ajouter "id-mr" à la liste d'objets importés depuis le module **UsefulDefinitions** dans le module **authenticationFramework**.*
- 2) *Ajouter "AttributeType", "Attribute" et "MATCHING-RULE" à l'ensemble d'objets importés dans le module **authenticationFramework** depuis le module **InformationFramework**.*
- 3) *Ajouter "GeneralNames" à l'ensemble d'objets importés dans le module **authenticationFramework** depuis le module **CertificateExtensions**.*
- 4) *Ajouter la définition suivante au module **authenticationFramework** car elle est importée dans d'autres modules des Recommandations de la série X.500, mais ne figure pas dans l'édition de 1997 de la Recommandation X.509:*

```

HASH {ToBeHashed} ::= SEQUENCE {
    algorithmIdentifier AlgorithmIdentifier,
    hashValue           BIT STRING ( CONSTRAINED BY {
        -- doit être le résultat de l'application d'une procédure de dispersion aux octets à codage DER --
        -- de valeur --ToBeHashed } ) }

```

- 5) Ajouter les assignations d'identificateur d'objet suivantes dans le module **authenticationFramework**:
- id-at-attributeCertificateRevocationList OBJECT IDENTIFIER ::= {id-at 59}**
- id-mr-attributeCertificateMatch OBJECT IDENTIFIER ::= {id-mr 42}**
- 6) Ajouter "Time" à l'ensemble d'objets importés dans le module **CertificateExtensions** depuis le module **authenticationFramework**.
- 7) Dans le module **CertificateExtensions** et au § 12.7.2 du corps de la Recommandation X.509, remplacer:
- CertPolicySet ::= SEQUENCE (1..MAX) OF CertPolicyId**
- par:
- CertPolicySet ::= SEQUENCE SIZE (1..MAX) OF CertPolicyId**

2) Relevés de défauts couverts par le projet de Corrigendum technique 9

(couvrant les résolutions relatives aux relevés de défauts 244, 256, 257 et 258)

2.1) Ce qui suit rectifie les défauts figurant dans le relevé de défauts 244

Dans l'article 8:

ajouter à la fin de l'alinéa qui commence par "Le champ d'**extension** permet d'ajouter de nouveaux ..." les deux phrases suivantes:

Lorsqu'une application qui utilise la certification reconnaît une extension et est en mesure de la traiter, elle effectue ce traitement quelle que soit la valeur du fanion de criticité. Il convient de noter que les extensions marquées comme étant non critiques seront traitées différemment selon les systèmes. Les systèmes qui utilisent la certification traiteront l'extension, tandis que ceux qui utilisent la certification mais ne la reconnaissent pas n'en tiendront pas compte.

Ajouter le texte suivant juste après l'alinéa qui commence par "Si des éléments inconnus apparaissent dans l'extension ...":

Une autorité de certification a trois possibilités en ce qui concerne une extension:

- i) elle peut exclure l'extension du certificat;
- ii) elle peut inclure l'extension et la marquer comme étant non critique;
- iii) elle peut inclure l'extension et la marquer comme étant critique.

Un moteur de validation a deux possibilités en ce qui concerne une extension:

- i) il peut ne pas tenir compte de l'extension et accepter le certificat (les autres éléments étant les mêmes);
- ii) il peut effectuer le traitement de l'extension et accepter ou rejeter le certificat en fonction du contenu de l'extension et des conditions de traitement (par exemple, les valeurs en cours des variables de traitement de l'itinéraire).

Certaines extensions ne peuvent être marquées que comme étant critiques. Dans ces cas, un moteur de validation qui comprend l'extension la traite et accepte ou rejette le certificat en fonction (au moins en partie) du contenu de l'extension. Un moteur de validation qui ne comprend pas l'extension rejette le certificat.

Certaines extensions ne peuvent être marquées que comme étant non critiques. Dans ces cas, un moteur de validation qui comprend l'extension la traite et accepte ou rejette le certificat en fonction (au moins en partie) du contenu de l'extension. Un moteur de validation qui ne comprend pas l'extension accepte le certificat (à moins que des facteurs autres que cette extension ne provoquent son rejet).

Certaines extensions peuvent être marquées comme étant critiques ou non critiques. Dans ces cas, un moteur de validation qui comprend l'extension la traite et accepte ou rejette le certificat en fonction (au moins en partie) du contenu de l'extension, quel que soit le fanion de criticité. Un moteur de validation qui ne comprend pas l'extension accepte le certificat si l'extension est marquée comme étant non critique (à moins que des facteurs autres que cette extension ne provoquent son rejet) et rejette le certificat si l'extension est marquée comme étant critique.

Lorsqu'une autorité de certification envisage d'inclure une extension dans un certificat, elle le fait en espérant qu'il sera tenu compte, lorsque cela est possible, de sa signification. S'il faut tenir compte du contenu de l'extension avant d'avoir recours au certificat, l'autorité de certification marquera l'extension comme étant critique. Elle doit le faire en tenant compte que tout moteur de validation qui n'effectue pas le traitement de l'extension rejettera le certificat (en limitant probablement l'ensemble des applications qui peuvent vérifier le certificat). L'autorité de certification peut marquer certaines extensions comme étant non critiques afin d'assurer la compatibilité avec des applications de validation antérieures qui n'effectuent pas le traitement des extensions. Lorsqu'il est plus important d'assurer la compatibilité et l'interfonctionnement avec des applications antérieures qui ne sont pas en mesure de traiter les extensions que de faire en sorte que l'autorité de certification puisse mettre en pratique les extensions, alors les extensions qui, facultativement, sont marquées comme étant critiques devraient être marquées comme ne l'étant pas. Il est très probable que les autorités de certification effectueraient le marquage de cette manière pendant une période de transition, au cours de laquelle les applications de traitement des certificats utilisées par les vérificateurs sont mises à niveau afin qu'elles puissent effectuer le traitement des extensions.

Au § 12.1:

dans l'alinéa qui commence par "Dans un certificat ou dans une liste CRL, une extension est étiquetée ...", ajouter le texte suivant juste après la troisième phrase qui se termine par "... sans tenir compte de l'extension.":

Si une extension est marquée comme étant non critique, un système qui utilise la certification mais ne reconnaît pas l'extension effectuera quand même le traitement de celle-ci.

Au § 12.2.2.3:

dans l'alinéa qui commence par "Si l'extension est étiquetée comme étant non critique ...", remplacer la deuxième phrase par le texte suivant:

Si cette extension est présente et que le système qui utilise la certification reconnaisse le type d'extension **keyUsage** et effectue le traitement de celui-ci, ce système assurera que le certificat ne sera utilisé qu'à des fins pour lesquelles la valeur du bit correspondant d'emploi de la clé est égale à un.

<https://standards.iteh.ai/catalog/standards/sist/5dcb356b-4e80-4c2b-b733-9159ed4c43c5/iso-iec-9594-8-1998-cor-2-2002>

Au § 12.2.2.4:

dans l'alinéa qui commence par "Si l'extension est étiquetée comme étant non critique ...", remplacer les deuxième et troisième phrases par le texte suivant:

Si cette extension est présente et que le système qui utilise la certification reconnaisse le type d'extension **extendedKeyUsage** et effectue le traitement de celui-ci, ce système assurera que le certificat ne sera utilisé qu'à l'une des fins indiquées.

Au § 12.4.2.1:

dans le quatrième alinéa qui suit la structure en ASN.1, remplacer la partie de phrase "Si cette extension est présente et est étiquetée comme critique:" par le texte suivant:

Si cette extension est présente et est étiquetée comme critique, ou comme non critique mais en étant reconnue par le système utilisant la certification, alors:

Au § 12.4.2.2:

remplacer la dernière phrase "Si cette extension est présente et est étiquetée comme critique ..." par le texte suivant:

Si cette extension est présente et est marquée comme étant critique, ou comme non critique mais en étant reconnue par le système qui utilise une certification, ce système vérifiera que l'itinéraire de certification est traité conformément à la valeur de cette extension.

2.2) Ce qui suit rectifie les défauts figurant dans le relevé de défauts 256

A l'article 8:

dans le premier alinéa de la description de l'attribut "paire de certificats croisés" (qui commence par "Les éléments **forward** ..."), ajouter la nouvelle troisième phrase suivante:

Si l'autorité de certification délivre un certificat à une autre autorité et que, dans une hiérarchie, celle-ci n'est pas subordonnée à la première, alors l'autorité émettrice doit placer ce certificat dans l'élément **reverse** de l'attribut **crossCertificatePair** de sa propre entrée d'annuaire.

2.3) Ce qui suit rectifie les défauts figurant dans le relevé de défauts 257

A l'article 8, dans la structure en ASN.1 **CertificatePair**:

remplacer "**forward**" par "**issuedByThisCA**" et

"**reverse**" par "**issuedToThisCA**", en apportant les modifications au texte correspondant comme il est décrit ci-dessous.

Modifier le texte descriptif de l'ensemble de la Rec. UIT-T X.509 en conséquence de manière à tenir compte de ces nouveaux termes. Cela concerne notamment les paragraphes particuliers suivants:

- le texte descriptif général de l'article 8;
- la structure en ASN.1 et le texte descriptif de l'attribut "paire de certificats croisés" de l'article 8;
- la structure en ASN.1 et le texte descriptif des règles de correspondance associées des § 12.7.3 et 12.7.4;
- les structures en ASN.1 reproduites à l'Annexe A.

Ajouter également ce qui suit à la fin du paragraphe commençant par "Dans les éditions précédentes; le terme **forward** ...":

<https://standards.iteh.ai/catalog/standards/sist/5dcb356b-4e80-4c2b-b733-9159ed4c43c5/iso-iec-9594-8-1998-cor-2-2002>

Le terme **Forward** était utilisé dans les éditions précédentes pour **issuedByThisCA** et le terme **reverse** était utilisé dans les éditions précédentes pour **issuedToThisCA**.

2.4) Ce qui suit rectifie les défauts figurant dans le relevé de défauts 258

A l'article 8, ajouter le nouvel alinéa suivant à la fin de ce §, juste avant le § 8.1:

Chaque certificat d'un itinéraire de certification doit être unique. Aucun certificat ne doit figurer plus d'une fois dans une valeur de la composante **theCACertificates** de l'itinéraire **CertificationPath** ou dans une valeur de **certificate** de la composante **CrossCertificates** de l'itinéraire **ForwardCertificationPath**.

Au § 12.4.3, ajouter la Note suivante juste après l'alinéa "a) ensemble des certificats ...":

NOTE – Tout certificat contenu dans un itinéraire de certification est unique. Un itinéraire qui contient deux fois ou plus le même certificat n'est pas un itinéraire de certification valable.