NORME INTERNATIONALE ISO/CEI 9594-8:1998
RECTIFICATIF TECHNIQUE 3

Publié 2002-09-01
Version française parue en 2003

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 3

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

TECHNICAL CORRIGENDUM 3

Le Rectificatif technique 3 à l'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*.

ICS 35.100.70 **Réf. nº ISO/CEI 9594-8:1998/Cor.3:2002(F)**

Publié en Suisse

NORME INTERNATIONALE

RECOMMANDATION UIT-T

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

CORRIGENDUM TECHNIQUE 3

(couvrant les résolutions des rapports de défauts 272, 273, 275 et 277)

1) Ce qui suit corrige les défauts signalés dans le rapport de défaut 272

Au § 12.4.2.1, ajouter le texte suivant à la fin de l'alinéa qui commence par "la composante **pathLenConstraint** sera présente ..."

Cette contrainte prend effet à partir du certificat suivant sur le chemin. Cette contrainte limite la longueur du segment du chemin de certification entre le certificat contenant cette extension et le certificat d'entité finale. Elle n'a pas d'effet sur le nombre de certificats CA sur le chemin de certification entre l'ancre de confiance et le certificat contenant cette extension. Par conséquent, la longueur d'un chemin de certification complet peut être supérieure à la longueur maximale du chemin limitée par cette extension. La contrainte limite le nombre de certificats CA non auto-émis entre le certificat CA contenant la contrainte et le certificat d'entité finale. Par conséquent, la longueur totale de ce segment de chemin, à l'exclusion des certificats auto-émis, peut être supérieure à la valeur de la contrainte de deux certificats au maximum. (Ceci inclut les certificats aux deux points d'extrémité du segment plus les certificats CA entre les deux points d'extrémité soumis à des contraintes imposées par la valeur de cette extension.)

2) Ce qui suit corrige les défauts signalés dans le rapport de défaut 273

Remplacer le § 12.4.2.2 par le texte suivant:

12.4.2.2 Extension des contraintes de nom

Ce champ, qui doit uniquement être utilisé dans un certificat CA, indique un espace nom dans lequel tous les noms de sujet dans les certificats subséquents d'un chemin de certification doivent se trouver. Ce champ est défini comme suit:

```
nameConstraints EXTENSION ::= {
        SYNTAX              NameConstraintsSyntax
        IDENTIFIED BY       id-ce-nameConstraint }

NameConstraintsSyntax ::= SEQUENCE {
        permittedSubtrees           [0]     GeneralSubtrees OPTIONAL,
        excludedSubtrees            [1]     GeneralSubtrees OPTIONAL,
        requiredNameForms           [2]     NameForms OPTIONAL  }

GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree

GeneralSubtree ::= SEQUENCE {
        base                        GeneralName,
        minimum     [0]             BaseDistance DEFAULT 0,
        maximum     [1]             BaseDistance OPTIONAL }

BaseDistance ::= INTEGER (0..MAX)

NameForms  ::= SEQUENCE {
    basicNameForms      [0]     BasicNameForms OPTIONAL,
    otherNameForms      [1]     SEQUENCE SIZE (1..MAX) OF OBJECT IDENTIFIER OPTIONAL }
(ALL EXCEPT ({ -- néant; c'est-à-dire qu'au moins un composant doit être présent -- }))
```

```
BasicNameForms  ::= BIT STRING {
        rfc822Name          (0),
        dNSName                     (1),
        x400Address                 (2),
        directoryName               (3),
        ediPartyName                (4),
        uniformResourceIdentifier   (5),
        iPAddress                   (6),
        registeredID                (7) }  (SIZE (1..MAX))
```

S'ils sont présents, les composants **permittedSubtrees** et **excludedSubtrees** spécifient chacun un ou plusieurs sous-arbres de nommage, chacun étant défini par le nom de la racine du sous-arbre et, optionnellement, à l'intérieur du sous-arbre, une zone qui est limitée par des niveaux supérieurs et/ou inférieurs. Si la composante **permittedSubtrees** est présente, les noms de sujet dans ces sous-arbres sont acceptables. Si le composant **excludedSubtrees** est présent, tout certificat émis par l'autorité CA considérée, ou les CA subséquents dans le chemin de certification qui ont un nom de sujet à l'intérieur de ces sous-arbres, est inacceptable. Si les deux composants **permittedSubtrees** et **excludedSubtrees** sont simultanément présents et que les espaces de noms se chevauchent, la déclaration d'exclusion a la priorité pour les noms situés dans la partie qui se chevauchent. Si les sous-arbres autorisés ou exclus ne sont pas présents pour une fore de nom, tout nom dans la forme de nom est acceptable. Si le composant **requiredNameForms** est présent, tous les certificats subséquents dans le chemin de certification doivent inclure un nom d'au moins une des formes de nom requises.

Si le composant **permittedSubtrees** est présent, ce qui suit s'applique à tous les certificats subséquents situés sur le chemin. Si un certificat contient un nom de sujet (dans le champ **subject** ou une extension **subjectAltNames**) d'une forme de nom pour lequel des sous-arbres autorisés sont spécifiés, le nom doit se trouver dans au moins un des sous-arbres spécifiés. Si un certificat contient seulement les noms de sujet des formes de nom autres que celles pour lesquelles les sous-arbres autorisés sont spécifiés, il n'est pas exigé que les noms de sujet se trouvent dans l'un des sous-arbres spécifiés. Par exemple, supposons que deux sous-arbres soient spécifiés, l'un pour la forme de nom DN et l'autre pour la forme de nom rfc822, aucun sous-arbre exclu n'est spécifié, mais **requiredNameForms** est spécifié avec le bit du **directoryName** et le bit **rfc822Name** présents. Un certificat qui contient seulement des noms autres que le nom d'annuaire ou le nom rfc822 serait inacceptable. Si toutefois les **requiredNameForms** n'étaient pas spécifiés, un tel certificat serait acceptable. Par exemple, supposons que deux sous-arbres autorisés soient spécifiés, un pour la forme de nom DN et l'autre la forme de nom rfc822, on ne spécifie pas de sous-arbres exclus, et le composant **requiredNameForms** n'est pas présent. Un certificat qui n'aurait contenu qu'un DN et où le DN se trouve dans le sous-arbre autorisé spécifié aurait été acceptable. Un certificat qui aurait contenu à la fois un nom de DN et un nom rfc822 et dans lequel un seul de ces noms aurait été à l'intérieur de son sous-arbre autorisé spécifié aurait été inacceptable. Un certificat qui contient seulement des noms autres qu'un nom de DN ou un nom rfc822 serait également acceptable.

Si le composant **excludedSubtrees** est présent, tout certificat émis par l'autorité CA considérée ou les autorités CA subséquentes sur le chemin de certification qui a un nom de sujet (dans le champ **subject** ou l'extension **subjectAltNames**) dans ces sous-arbres est inacceptable. Par exemple, si l'on suppose que deux sous-arbres exclus sont spécifiés, l'un pour la forme de nom DN et l'autre pour la forme de nom rfc822, un certificat qui n'aurait contenu qu'un nom DN se trouvant dans le sous-arbre exclu spécifié aurait été inacceptable. Un certificat qui contiendrait un nom DN et un nom rfc822 dans lequel un de ces noms se trouverait dans le sous-arbre exclu spécifié aurait été inacceptable.

Lorsqu'un sujet d'un certificat a plusieurs noms de la même forme de nom (y compris dans le cas d'une forme de nom **directoryName**, le nom dans le champ sujet du certificat s'il n'est pas vide), l'homogénéité de tous ces noms doit être vérifiée avec une contrainte de nom de cette forme de nom.

Si le composant **requiredNameForms** est présent, tous les certificats subséquents sur le chemin de certification doivent inclure un nom de sujet d'au moins l'une des formes de nom requises.

Parmi les formes de nom disponibles via le type **GeneralName**, seules les formes de nom qui ont une structure hiérarchique bien définie peuvent être utilisées dans les champs **permittedSubtrees** et **excludedSubtrees**. La forme de nom **directoryName** satisfait à cette condition; lorsqu'on utilise cette forme de nom, un sous-arbre de nommage correspond à un sous-arbre DIT.

Le champ **minimum** spécifie la limite supérieure de la zone à l'intérieur du sous-arbre. Tous les noms dont le composant final de nom se trouve au-dessus du niveau spécifié ne sont pas contenus dans cette zone. Une valeur de **minimum** égale à zéro (valeur par défaut) correspond à la base, c'est-à-dire au noeud le plus haut du sous-arbre. Par exemple, si la valeur de **minimum** est un, le sous-arbre de nommage exclut le nœud de base mais inclut les nœuds subordonnés.

Le champ **maximum** spécifie la limite inférieure de la zone dans le sous-arbre. Tous les noms dont le dernier composant se trouve en dessous du niveau spécifié ne sont pas contenus dans la zone. Une valeur de **maximum** égale à zéro correspond à la base, c'est-à-dire au sommet du sous-arbre. L'absence d'un composant **maximum** indique qu'aucune limite ne doit être imposée dans la zone à l'intérieur du sous-arbre. Par exemple, si la valeur de **maximum** est un, le sous-arbre de nommage exclut tous les nœuds à l'exception de la base du sous-arbre et de ses subordonnés immédiats.

Cette extension peut, à la discrétion de l'émetteur du certificat, être critique ou non critique. Il est recommandé de marquer cette extension comme critique avec indicateur, dans les autres cas, un utilisateur de certificat peut ne pas vérifier que les certificats subséquents dans un chemin de certification sont situés dans l'espace nom voulu par l'autorité CA émettrice.

Il n'est pas exigé des implémentations conformes de reconnaître toutes les formes de nom possibles.

Si l'extension est présente et que l'indicateur indique critique, une implémentation utilisant les certificats doit reconnaître et traiter toutes les formes de nom pour lesquelles il y a à la fois une spécification de sous-arbre (autorisé ou exclu) dans l'extension et une valeur correspondante dans le champ **subject** ou dans l'extension **subjectAltNames** de tous certificats subséquents sur le chemin de certification. Si une forme de nom non reconnue apparaît à la fois dans une spécification de sous-arbre et dans un certificat subséquent, ce certificat doit être traité comme s'il y avait une extension critique non reconnue. Si un nom de sujet dans le certificat se trouve dans un sous-arbre exclu, le certificat est inacceptable. Si un sous-arbre est spécifié pour une forme de nom qui n'est pas contenue dans un certificat subséquent, ce sous-arbre peut être ignoré. Si la composante **requiredNameForms** spécifie seulement des formes de nom non reconnues, ce certificat doit être traité comme s'il n'y avait pas une extension critique non reconnue. Dans les autres cas, au moins une des formes de nom reconnues doit apparaître dans tous les certificats subséquents du chemin.

Si l'extension est présente et marquée comme non critique et qu'une implémentation utilisant des certificats ne reconnaît pas une forme de nom utilisée dans une composante **base**, cette spécification de sous-arbre peut être ignorée. Si l'extension est marquée comme non critique et si une des formes de nom spécifiées dans la composante **requiredNameForms** n'est pas reconnue par l'implémentation utilisant le certificat, le certificat doit être traité comme si la composante **requiredNameForms** était absente.

Ajouter au § 12.4.3, une nouvelle variable de traitement de chemin comme suit et renuméroter les sous-paragraphes en conséquence:

d) *required-name-forms (formes de nom requises)*: ensemble (éventuellement vide) d'ensembles de formes de nom. Pour chaque ensemble de formes de nom, chaque certificat subséquent doit contenir le nom d'une des formes de nom de l'ensemble.

Ajouter au § 12.4.3, une nouvelle étape d'initialisation suivante et renuméroter les sous-paragraphes en conséquence:

d) initialisation de l'ensemble *required-name-forms* comme étant un ensemble vide;

Ajouter au § 12.4.3, la nouvelle étape suivante aux vérifications appliquées à tous les certificats:

h) Si le certificat n'est pas un certificat intermédiaire auto-émis, et si l'ensemble *required-name-forms* n'est pas un ensemble vide, pour chaque ensemble de formes de nom de l'ensemble *required-name-forms*, vérifier qu'il y a un nom de sujet dans le certificat de l'une des formes de nom de l'ensemble.

Ajouter au § 12.4.3, l'étape suivante aux actions d'enregistrement de contrainte appliquées aux certificats intermédiaires:

c) Si l'extension **nameConstraints** avec une composante **requiredNameForms** est présente dans le certificat, donner à la variable *required-name-forms* la valeur de l'union de sa précédente valeur et de l'ensemble constitué de l'ensemble des formes de nom spécifiées dans l'extension de certificat. Si la composante **requiredNameForms** contient plusieurs formes de nom, la variable *required-name-forms* doit signaler qu'un nom d'au moins une des formes de nom indiquées dans son extension doit être présent dans tous les certificats subséquents. L'union d'une valeur précédente de la variable *required-name-forms* et de la valeur provenant de l'extension du certificat courant est un ensemble d'ensembles signalant les conditions imposées pour tous les certificats subséquents. Par exemple, si la variable courante *required-name-forms* est mise à exigeant qu'un nom DN ou qu'un nom rfc822 doit être présent dans les certificats et l'extension courante dans le certificat en cours de traitement indique soit des noms rfc822 ou DNS sont requis, l'union résultante, c'est-à-dire la nouvelle variable *required-name-forms*, indique que chaque certificat subséquent doit avoir soit un nom rfc822 ou à la fois un nom DN et un nom DNS.

Dans l'Annexe A, module **certificateExtensions,** *actualiser la représentation ASN.1 de l'extension* **nameConstraints** *comme ci-dessus*:

Dans l'Annexe A, module **certificateExtensions**, *ajouter ce qui suit:*

```
id-ce-nameConstraint                OBJECT IDENTIFIER ::=     {id-ce 30 1}
```

Dans l'Annexe A, module **certificateExtensions**, *supprimer ce qui suit:*

```
id-ce-nameConstraints               OBJECT IDENTIFIER ::=     {id-ce 30}
```

Dans l'Annexe A, module **certificateExtensions**, *ajouter ce qui suit à l'ensemble d'identificateurs OID non utilisés dans cette Spécification:*

```
id-ce 30
```

3) Ce qui suit corrige les défauts signalés dans le rapport de défaut 275

Au § 12.2.2.4, ajouter le texte suivant comme deuxième nouvel alinéa suivant l'ASN.1 pour l'extension **extKeyUsage**.

Une autorité CA peut affirmer any-extended-key-usage en utilisant l'identificateur **anyExtendedKeyUsage**. Ceci permet à une autorité de certification CA d'émettre un certificat qui contient des identificateurs OID pour des utilisations de clés élargies qui peuvent être requises par les applications utilisant les certificats, sans limiter l'utilisation du certificat aux utilisations clés. Si l'utilisation de clé étendue limitait l'utilisation des clés, l'inclusion de cet identificateur OID lève cette restriction.


```
anyExtendedKeyUsage  OBJECT IDENTIFIER  ::= { 2 5 29 37 0 }
```


4) Ce qui suit corrige les défauts signalés dans le rapport de défaut 277

Au § 12.4.2.3, dans la dernière phrase du deuxième alinéa:

Remplacer "qui est titulaire d'un certificat subséquent" *par* "qui est l'émetteur d'un certificat subséquent".