UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T X.509

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Corrigendum 3
(10/2001)

SÉRIE X: RÉSEAUX DE DONNÉES ET
COMMUNICATION ENTRE SYSTÈMES OUVERTS

Annuaire

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

Corrigendum Technique 3

Recommandation UIT-T X.509 (1997) – Corrigendum 3

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

RÉSEAUX PUBLICS DE DONNÉES	
Services et fonctionnalités	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalisation et commutation	X.50–X.89
Aspects réseau	X.90–X.149
Maintenance	X.150–X.179
Dispositions administratives	X.180–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	
Modèle et notation	X.200–X.209
Définitions des services	X.210–X.219
Spécifications des protocoles en mode connexion	X.220–X.229
Spécifications des protocoles en mode sans connexion	X.230–X.239
Formulaires PICS	X.240–X.259
Identification des protocoles	X.260–X.269
Protocoles de sécurité	X.270–X.279
Objets gérés des couches	X.280–X.289
Tests de conformité	X.290–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Généralités	X.300–X.349
Systèmes de transmission de données par satellite	X.350–X.369
Réseaux à protocole Internet	X.370–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	**X.500–X.599**
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	
Réseautage	X.600–X.629
Efficacité	X.630–X.639
Qualité de service	X.640–X.649
Dénomination, adressage et enregistrement	X.650–X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680–X.699
GESTION OSI	
Cadre général et architecture de la gestion-systèmes	X.700–X.709
Service et protocole de communication de gestion	X.710–X.719
Structure de l'information de gestion	X.720–X.729
Fonctions de gestion et fonctions ODMA	X.730–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850–X.859
Traitement transactionnel	X.860–X.879
Opérations distantes	X.880–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

NORME INTERNATIONALE ISO/CEI 9594-8

RECOMMANDATION UIT-T X.509

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

CORRIGENDUM TECHNIQUE 3

Résumé

Le présent corrigendum technique couvre la résolution des rapports de défauts 272, 273, 275 et 277.

Source

Le Corrigendum 3 de la Recommandation X.509 (1997) de l'UIT-T, élaboré par la Commission d'études 7 (2001-2004) de l'UIT-T, a été approuvé le 29 octobre 2001. Un texte identique est publié comme Corrigendum technique 3 de la Norme Internationale ISO/CEI 9594-8.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT avait été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

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 rfc 822, 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".

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, circuits téléphoniques, télégraphie, télécopie et circuits loués internationaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données et communication entre systèmes ouverts**
Série Y	Infrastructure mondiale de l'information et protocole Internet
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse

Genève, 2002