UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T X.509

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Corrigendum 1
(10/2001)

SÉRIE X: RÉSEAUX DE DONNÉES ET
COMMUNICATION ENTRE SYSTÈMES OUVERTS

Annuaire

Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut

Corrigendum Technique 1

Recommandation UIT-T X.509 (2000) – Corrigendum 1

(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 général des certificats de clé publique et d'attribut

CORRIGENDUM TECHNIQUE 1

Résumé

Le présent corrigendum technique corrige les défauts signalés dans les rapports de défauts 272, 273, 274, 275, 276, 277, 278 et 279.

Source

Le Corrigendum 1 de la Recommandation X.509 (2000) de l'UIT-T, élaboré par la Commission d'études 7 (2001-2004) de l'UIT-T, a été approuvé le 2 octobre 2001. Un texte identique est publié comme Corrigendum technique 1 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 général des certificats de clé publique et d'attribut

CORRIGENDUM TECHNIQUE 1

(Couvrant les résolutions des rapports de défauts 272, 273, 274, 275, 276, 277, 278 et 279)

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

Au § 8.4.2.1, ajouter le texte suivant à la fin de l'alinéa qui commence par "le composant **pathLenConstraint** sera présent uniquement si ..."

Cette contrainte prend effet à partir du certificat suivant sur le chemin. La 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 aucun 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 segment limité par cette extension. La contrainte contrôle 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 du certificat 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 qui sont limités par la valeur de cette extension.)

Au § 15.5.2.1, dans l'alinéa qui commence par "le composant **pathLenConstraint** est significatif uniquement si ..."*, remplacer les deux dernières phrases de cet alinéa par le texte suivant*:

Cette contrainte limite la longueur du segment du chemin de délégation entre le certificat contenant cette extension et le certificat d'entité finale. Elle n'a aucune incidence sur le nombre de certificats AA sur le chemin de délégation entre l'ancre de confiance et le certificat contenant cette extension. Par conséquent, la longueur d'un chemin de délégation complet peut être supérieure à la longueur maximale du segment limité par cette extension. La contrainte limite le nombre de certificats AA entre le certificat AA contenant la contrainte et le certificat d'entité finale. Par conséquent la longueur de ce segment du chemin 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 AA entre les deux points d'extrémité limités par la valeur de cette extension.)

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

Remplacer le § 8.4.2.2 par le suivant:

8.4.2.2 Extension de contraintes de noms

Ce champ, qui sera utilisé uniquement dans un certificat CA, indique un espace de noms dans lequel doivent se trouver tous les noms de sujets dans les certificats subséquents sur un chemin de certification. 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: 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 facultativement, à l'intérieur du sous-arbre considéré, un domaine qui est limité par des niveaux supérieurs et/ou inférieurs. Si le composant **permittedSubtrees** est présent, les noms de sujets dans ces sous-arbres sont acceptables. Si le composant **excludedSubtrees** est présent, tout certificat émis par l'autorité CA sujette ou les autorités CA subséquentes sur le chemin de certification qui a un nom de sujet à l'intérieur de ces sous-arbres est inacceptable. Si les deux composants **permittedSubtrees** et **excludedSubtrees** sont présents et si les espaces noms se chevauchent, la déclaration d'exclusion a la priorité pour les noms qui se trouvent dans la partie commune (qui se chevauche). Si à la fois les composants **permittedSubtrees** et **excludedSubtrees** sont spécifiés dans une forme de nom, tout nom dans cette forme de nom est acceptable. Si le composant **requiredNameForms** est présent, tous les certificats subséquents sur le chemin de certification doivent inclure un nom d'au moins l'une des formes de noms requises.

Si le composant **permittedSubtrees** est présent, ce qui suit s'applique à tous les certificats subséquents du chemin. Si un certificat contient un nom de sujet (dans le champ **subject** ou dans l'extension **subjectAltNames**) d'une forme de nom pour laquelle des sous-arbres autorisés sont spécifiés, le nom doit se trouver dans au moins l'un des sous-arbres spécifiés. Si un certificat contient uniquement les noms de sujets des formes de noms autres que ceux pour lesquels les sous-arbres autorisés sont spécifiés, les noms de sujets ne doivent pas obligatoirement se trouver dans l'un des sous-arbres spécifiés. Par exemple, si l'on suppose que deux sous-arbres autorisés sont 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 le composant **requiredNameForms** est spécifié avec les bits **directoryName** et **rfc822Name** présents. Un certificat qui aurait contenu seulement des noms autres qu'un nom d'annuaire ou un nom rfc822 aurait été inacceptable. Si le composant **requiredNameForms** n'était pas spécifié, toutefois, un tel certificat serait acceptable. Par exemple, supposons que deux sous-arbres autorisés sont 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 et le composant **requiredNameForms** n'est pas présent. Un certificat qui aurait contenu seulement un nom de domaine DN qui se trouve dans le sous-arbre autorisé spécifié, aurait été acceptable. Un certificat qui aurait contenu à la fois un nom DN et un nom rfc822 et dans lequel seul l'un de ces noms se trouve dans le sous-arbre autorisé spécifié, aurait été inacceptable. Un certificat qui n'aurait contenu que des noms autres qu'un nom DN ou un nom rfc822 aurait été également acceptable.

Si le composant **excludedSubtrees** est présent, tout certificat émis par l'autorité CA sujette ou les autorités CA subséquentes sur le chemin de certification qui ont un nom de sujet (dans le champ **subject** ou dans l'extension **subjectAltNames**) dans ces sous-arbres est inacceptable. Par exemple, supposons que deux sous-arbres exclus sont spécifiés, l'un pour la forme de nom DN, l'autre pour la forme de nom rfc822. Un certificat qui n'aurait contenu qu'une forme de nom DN située dans le sous-arbre exclu spécifié, aurait été inacceptable. Un certificat qui aurait contenu à la fois un nom DN et un nom rfc822 dans lequel au moins l'un des deux noms se trouvait dans le sous-arbre exclu spécifié, aurait été inacceptable.

Lorsqu'un certificat sujet a plusieurs noms de la même forme de nom (incluant, dans le cas de la forme de nom **directoryName**, le nom dans le champ sujet du certificat s'il n'est pas vide) il convient alors de tester l'homogénéité de tous ces noms avec la contrainte de nom de cette forme de nom.

Si le composant **requiredNameForms** est présent, tous les certificats subséquents du 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 cette exigence; 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 nœud supérieur du sous-arbre. Par exemple, si **minimum** à la valeur un, le sous-arbre de nommage exclut le nœud de la base mais inclut les nœuds subordonnés.

Le champ **maximun** spécifie la limite inférieure de la zone dans le sous-arbre. Tous les noms dont le dernier composant se trouvent 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 du composant **maximum** signifie qu'on ne doit pas imposer de limite inférieure dans la zone à l'intérieur du sous-arbre. Par exemple, si la valeur de **maximum** est égale à un, le sous-arbre de nommage exclut tous les nœuds à l'exception du nœud de la base de sous-arbre et de ses nœuds subordonnés immédiats.

Cette extension peut, si l'émetteur du certificat choisit cette option, être critique ou non critique. On recommande de le marquer comme critique, sinon un utilisateur de certificat peut ne pas vérifier que les certificats subséquents du chemin de certification sont situés dans l'espace nom voulu par l'autorité CA émettrice.

Les implémentations conformes ne doivent pas nécessairement reconnaître toutes les formes de nom possibles.

Si l'extension est présente et est marquée comme critique, une implémentation utilisatrice de certificat doit reconnaître et traiter toutes les formes de nom pour lesquelles il y a à la fois une spécification de sous-arbre (autorisée ou exclue) dans l'extension et une valeur correspondante dans le champ **subject** ou l'extension **subjectAltNames** de tout certificat subséquent sur le chemin de certification. Si une forme de nom non reconnue apparaît à la fois dans une spécification de sous-arbre et un certificat subséquent, le certificat doit être traité comme s'il y avait une extension critique non reconnue. Si un nom de sujet du certificat se trouve dans un sous-arbre exclu, le certificat n'est pas acceptable. 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 le composant **requiredNameForms** spécifie seulement des formes de nom non reconnues, ce certificat doit être traité comme si on avait rencontré 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 est marquée comme non critique et qu'une implémentation utilisant le certificat 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 l'une des formes de nom spécifiées dans le composant **requiredNameForms** qui n'est pas reconnue par la implémentation utilisant le certificat, le certificat doit être traité comme si la composante **requiredNameForms** était absente.

Dans le § 10.3, ajouter une nouvelle variable de traitement d'itinéraire comme suit et renuméroter en conséquence les sous-alinéas subséquents:

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 un nom d'une des formes de nom de l'ensemble;

Au § 10.4, ajouter la nouvelle étape d'initialisation suivante et renuméroter en conséquence les sous-alinéas subséquents:

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

Au § 10.5.1, ajouter la nouvelle étape suivante aux vérifications appliquées à tous les certificats:

h) si le certificat n'est pas un certificat auto-émis intermédiaire, 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.

Au § 10.5.2, ajouter la nouvelle étape suivante aux actions d'enregistrement de contrainte appliquées aux certificats intermédiaires:

c) si l'extension **nameConstraints** avec un composant **requiredNameForms** est présente dans le certificat, donner à la variable *required-name-forms* une valeur égale à l'union de ces valeurs précédentes et l'ensemble composé de l'ensemble des formes de nom spécifiées dans l'extension de certificat. Si le composant **requiredNameForms** contient plusieurs formes de nom, la variable *required-name-forms* doit signaler qu'un nom d'au moins l'une des formes de nom indiquées dans cette extension doit être présent dans tous les certificats subséquents. L'union d'une valeur précédente de la variable *required-name-forms* avec la valeur provenant de l'extension de certificats courante est un ensemble d'ensembles signalant les conditions à respecter pour tous les certificats subséquents. Par exemple, si la variable *required-name-forms* courante est mise à une valeur exigeant qu'un nom DN ou un nom rfc822 doit être présent dans les certificats et l'extension courante dans le certificat en cours de traitement indique que 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 un nom rfc822 ou à la fois un nom DN et un nom DNS.

Dans l'Annexe A, module **certificateExtensions** *mettre à jour l'ASN.1 pour l'extension* **nameConstraints** *comme ci-dessus*.

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

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

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

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

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

```
id-ce 30
```

3) Ce qui suit corrige les défauts signalés dans le rapport de défaut 274

Dans l'Annexe A, remplacer la production ASN.1 **AttCertVersion** *par*:

```
AttCertVersion      ::=     INTEGER  {v2(1) }
```

Au § 12.1, remplacer le premier alinéa qui suit l'ASN.1 par ce qui suit:

La **version** permet de différencier les différentes versions du certificat d'attribut. Pour les certificats d'attribut émis conformément à la syntaxe de la présente Spécification, **version** doit être **v2**.

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

Au § 8.2.2.4, ajouter le texte ci-dessous en tant que deuxième alinéa suivant l'ASN.1 pour l'extension **extKeyUsage**:

Une autorité CA peut déclarer une extension d'utilisation de clé étendue (any-extended-key-usage) en utilisant l'identificateur **anyExtendedKeyUsage**. Cela permet à une autorité CA d'émettre un certificat qui contient des identificateurs OID pour les utilisations de clé étendues qui peuvent être requises dans certaines applications utilisant des certificats, sans limiter le certificat à ces utilisations de clé. Si l'utilisation de clé étendue restreint l'utilisation de clé, l'inclusion de cet identificateur OID lève cette restriction.

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

5) Ce qui suit corrige les défauts signalés dans le rapport de défaut 276

Au § 8.1.5:

Dans la dernière phrase, remplacer "et *explicit-policy-pending* (attente de politique explicite)" *par* "*explicit-policy-pending* (*attente de politique explicite*) et *inhibit-any-policy* (*interdiction de politique*)".

Au § 8.4.2.4, dans la première phrase:

Remplacer "pour tous les certificats sur l'itinéraire de certification" *par* "pour tous les certificats non auto-émis sur l'itinéraire de certification".

Au § 10.5.1, point e):

Remplacer "ou si l'indicateur *inhibit-any-policy-indicator* est fixé, supprimer" *par* "ou si l'indicateur *inhibit-any-policy-indicator* est positionné et le certificat n'est pas un certificat intermédiaire auto-émis, supprimer alors".

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

Au § 8.4.2.3, dans la dernière phrase du second alinéa:

Remplacer "qui est le sujet d'un certificat suivant" *par* "qui est l'émetteur d'un certificat subséquent".

7) Ce qui suit corrige les défauts signalés dans le rapport de défaut 278

Au § 8.6.2.6, dans la première phrase:

Remplacer "sera utilisée exclusivement comme extension de certificat elle peut être …" *par* "peut être utilisée comme certificat ou extension de liste CRL. Dans les certificats, cette extension peut être …"

8) Ce qui suit corrige les défauts signalés dans le rapport de défaut 279

A l'article 7, ajouter ce qui suit immédiatement après la production ASN.1 **CrossCertificates**:

PkiPath ::= SEQUENCE OF Certificate

PkiPath est utilisé pour représenter un chemin de certification. Dans la séquence, l'ordre des certificats est tel que le sujet du premier certificat est l'émetteur de deuxième certificat, etc.

Au § 11.1.6:

Remplacer "la classe d'objets **pkiCA**" *par* "**pkiCA** ou **pkiUser**".

Dans la dernière phrase du dernier alinéa, article 7:

Remplacer "de l'itinéraire **CertificationPath** " *par* "composant de l'itinéraire **CertPath** ou une valeur de **Certificate** dans **PkiPath**."

Au § 11.2.10:

Supprimer la production ASN.1 **PkiPath**.

Dans la première phrase du § 11.2.10:

Remplacer "certificats croisés" *par* "certificats".

Au § 11.2.10, remplacer le texte suivant l'ASN.1 par ce qui suit:

Cet attribut peut être stocké dans une entrée d'annuaire de la classe d'objets **pkiCA** ou **pkiUser**.

Lorsqu'elles sont stockées dans les entrées **pkiCA**, les valeurs de cet attribut contiennent les chemins de certification excluant les certificats d'entité finale. De ce fait, l'attribut est utilisé pour stocker les chemins de certification qui sont fréquemment utilisés par les participants faisant confiance associés à cette autorité CA. Une valeur de cet attribut peut être utilisée en association avec un certificat d'entité finale émis par le sujet du dernier certificat dans la valeur d'attribut.

Lorsqu'elles sont stockées dans les entrées **pkiUser**, les valeurs de cet attribut contiennent les chemins de certification qui incluent le certificat d'entité finale. De ce fait, l'entité finale est l'utilisateur dont l'entrée détient cet attribut. Ces valeurs de l'attribut représentent les chemins de certification complets pour les certificats émis vers cet utilisateur.

Au § 11.3.9, dans la dernière phrase du premier alinéa:

Remplacer "émis à destination de l'autorité de certification qui a émis le certificat d'entité finale en cours de validation" *par* "émis vers le sujet spécifié."

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

Genève, 2002