Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.509

Corrigendum 1

(01/2007)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

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 (2005) – Corrigendum technique 1

Union internationale des télécommunications

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

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.379
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.889
Applications génériques de l'ASN.1	X.890–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DES TÉLÉCOMMUNICATIONS	X.1000–

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

Source

Le Corrigendum 1 de la Recommandation UIT-T X.509 (2005) a été approuvé le 13 janvier 2007 par la Commission d'études 17 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8. 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.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

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 développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Page

1) Correction des erreurs signalées dans le relevé d'erreurs 310 1
2) Correction des erreurs signalées dans le relevé d'erreurs 311 1
3) Correction des erreurs signalées dans le relevé d'erreurs 314 2

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

(portant sur la correction des erreurs sigalées dans les relevés d'erreurs 310, 311 et 314)

1) Correction des erreurs signalées dans le relevé d'erreurs 310

Remplacer la Note 4 du § 7.3 par le texte suivant:

Lorsqu'une implémentation traitant une liste CRL trouve le numéro de série du certificat concerné dans un élément de liste CRL, mais qu'elle ne reconnaît pas une extension critique dans le champ **crlEntryExtensions** provenant de cet élément de liste CRL, il n'est pas possible d'utiliser cette liste CRL pour déterminer le statut du certificat. Lorsqu'une implémentation ne reconnaît pas une extension critique dans le champ **crlExtensions,** il n'est pas possible d'utiliser cette liste CRL pour déterminer le statut du certificat, que le numéro de série du certificat concerné y figure ou non.

NOTE 4 – Dans ces cas, il se peut que la politique locale prévoie des mesures complémentaires ou des mesures plus strictes que celles énoncées dans la présente Spécification, telle que la recherche d'informations de statut de révocation auprès d'autres sources.

Les certificats pour lesquels le statut de révocation ne peut pas être déterminé ne devraient pas être considérés comme valables.

2) Correction des erreurs signalées dans le relevé d'erreurs 311

a) Remplacer la Note 5 du § 7.3 par le texte suivant:

Si une extension affecte le traitement de la liste (plusieurs listes CRL devant, par exemple, être examinées en totalité pour déterminer les certificats révoqués, ou un élément peut représenter un domaine de certificats), cette extension ou une extension connexe sera marquée comme critique dans le champ **crlExtensions.** Par conséquent, une extension critique dans le champ **crlEntryExtensions** d'un élément affectera uniquement le certificat spécifié dans cet élément, à moins qu'il n'existe une extension critique connexe dans le champ **crlExtensions** qui publie un traitement particulier pour ce cas. Le seul exemple de cette situation définie dans la présente Spécification est l'extension **certificateIssuer** de l'élément de liste CRL et l'extension connexe **issuingDistributionPoint** d'une liste CRL, lorsque l'opérateur booléen **indirectCRL** a la valeur **VRAI**.

b) Au § 8.6.2.2 remplacer le premier alinéa figurant après les définitions ASN.1 par le texte suivant:

Le composant **distributionPoint** contient le nom du point de répartition sous une ou plusieurs formes de nom. Si la valeur du composant **onlyContainsUserPublicKeyCerts** (*contient uniquement des certificats de clé publique d'utilisateur*) est égale à **VRAI**, la liste CRL contient uniquement des révocations pour des certificats de clé publique d'entité finale. Si la valeur du composant **onlyContainsCACerts** (*contient uniquement des certificats d'autorité de certification*) est égale à **VRAI**, la liste CRL contient uniquement des révocations pour des certificats d'autorité de certification. Si les valeurs des composants **onlyContainsUserPublicKeyCerts** et **onlyContainsCACerts** sont toutes deux égales à **FAUX**, la liste CRL contient des révocations pour des certificats de clé publique d'entité finale et pour des certificats d'autorité de certification. Une liste CRL ne contient pas cette extension lorsque les composants **onlyContainsUserPublicKeyCerts** et **onlyContainsCACerts** ont tous deux la valeur **VRAI**. Si le composant **onlySomeReasons** est présent, la liste CRL contient uniquement les révocations de certificats de clé publique correspondant au ou aux motifs indiqués; dans le cas contraire, elle contient des révocations pour tous les motifs. Si la valeur du composant **indirectCRL** (*liste CRL indirecte*) est égale à **VRAI**, la liste CRL peut contenir des notifications de révocation pour des certificats de clé publique émis par des autorités dont le nom est différent de celui de l'émetteur de la liste CRL. L'autorité particulière responsable de chaque entrée est celle indiquée par l'extension **certificateIssuer** de l'élément de liste CRL dans cette entrée ou encore celle indiquée conformément aux règles par défaut décrites au § 8.6.2.3. Par conséquent, un système utilisant des certificats qui peut traiter une liste CRL dans laquelle la valeur du composant **indirectCRL** est égale à **VRAI** doit également pouvoir traiter l'extension **certificateIssuer** de l'élément de liste CRL. Il est de la responsabilité de l'émetteur d'une telle liste CRL de s'assurer qu'elle est complète, c'est-à-dire

qu'elle contient toutes les entrées de révocation, d'une manière cohérente avec les indicateurs **onlyContainsUserPublicKeyCerts**, **onlyContainsCACerts** et **onlySomeReasons** en provenance de toutes les autorités qui identifient cet émetteur de liste CRL dans leurs certificats de clé publique.

3) Correction des erreurs signalées dans le relevé d'erreurs 314

a) Remplacer le § 8.4.2.2 par le texte suivant:

8.4.2.2 Champ de contraintes de nom

Ce champ, qui sera utilisé uniquement dans un certificat d'autorité CA, indique une ou plusieurs formes de nom dont les espaces de nom sont soumis à des contraintes et dans lesquelles doivent se trouver tous les noms de sujet de la même forme de nom figurant dans des certificats suivants sur un itinéraire de certification. En l'absence de cette extension, aucune contrainte n'est imposée à aucune forme de nom. Si cette extension est présente, mais qu'une forme de nom en est exclue, aucune contrainte n'est imposée à cette forme de nom.

NOTE 1 – Etant donné qu'il peut y avoir un ensemble non-lié de formes de nom **registeredID**, il n'est généralement pas possible d'imposer des contraintes à toutes les formes de nom possibles des noms de sujet au moyen de cette extension.

Ce champ est défini comme suit:

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

NameConstraintsSyntax ::= SEQUENCE {
    permittedSubtrees       [0]   GeneralSubtrees OPTIONAL,
    excludedSubtrees        [1]   GeneralSubtrees OPTIONAL }
(ALL EXCEPT ({ -- aucun, c'est-à-dire: au moins un composant est présent --}))

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

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

BaseDistance ::= INTEGER (0..MAX)
```

Au moins un des composants **permittedSubtrees** et **excludedSubtrees** doit être présent.

La présence du composant **permittedSubtrees** spécifie un ou plusieurs sous-arbres, pour une ou plusieurs formes de nom, dans lesquels devront être contenus les noms de sujet de certificats acceptables. La présence du composant **excludedSubtrees** spécifie un ou plusieurs sous-arbres, pour une ou plusieurs formes de nom, dans lesquels ne devront pas être contenus les noms de sujet de certificats acceptables. Les noms de sujet qui sont comparés par rapport aux sous-arbres spécifiés comprennent les noms qui sont à la fois présents dans le champ **subject** et dans l'extension **subjectAltNames** d'un certificat. Chaque sous-arbre est défini par le nom de sa racine, le composant **base** et, facultativement, à l'intérieur du sous-arbre considéré, un domaine qui est limité par des niveaux supérieurs et/ou inférieurs.

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 exclut le nœud de la base, mais inclut les nœuds subordonnés.

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

L'ensemble de tous les composants **permittedSubtrees** et **excludedSubtrees** pour une forme de nom comprend l'espace de nom soumis à des contraintes pour cette forme de nom. Tous les noms de sujet, figurant dans des certificats émis par l'autorité de certification sujette et par les autorités de certification suivantes sur un itinéraire de certification, qui appartiennent à une forme de nom soumise à des contraintes doivent se trouver dans l'espace de nom soumis à des contraintes, pour que le certificat puisse être acceptable.

S'il est présent, le composant **permittedSubtrees** spécifie les sous-arbres à l'intérieur desquels doivent se trouver tous les noms de sujet appartenant à une forme de nom soumise à des contraintes, pour que le certificat puisse être acceptable. Si le composant **excludedSubtrees** est présent, aucun certificat émis par l'autorité de certification sujette où les autorités de certification suivantes sur l'itinéraire de certification ayant un nom de sujet dans ces sous-arbres n'est acceptable. Si les composants **permittedSubtrees** et **excludedSubtrees** sont tous deux présents pour une forme de nom et si les espaces de nom se chevauchent, la déclaration d'exclusion prévaut.

Si aucune des formes de nom du nom de sujet figurant dans le certificat n'est limitée par cette extension, le certificat est acceptable.

Dans certains cas, il peut être nécessaire d'émettre plusieurs certificats pour respecter les exigences liées aux contraintes de nom. Deux de ces situations sont illustrées dans l'Annexe G. Par exemple, si les contraintes de nom sont définies pour plusieurs formes de nom, alors qu'un certificat est tenu de respecter ces contraintes uniquement pour une seule de ces formes de nom (opérateur logique "OU" positionné sur contraintes), il est nécessaire d'émettre plusieurs certificats limitant chacun une seule forme de nom.

Sur l'ensemble des formes de nom disponibles par le biais du type **GeneralName**, seules celles ayant une structure hiérarchique bien définie peuvent être utilisées dans ces champs.

La forme de nom **directoryName** remplit cette condition; lorsqu'on l'utilise, un sous-arbre de nommage correspond à un sous-arbre DIT. Un **certificate** est considéré comme étant subordonné à la **base** (et donc candidat à l'intérieur du sous-arbre), si la **SEQUENCE** des noms distinctifs relatifs (**RDN**) qui forme le nom d'annuaire complet (DN) dans la **base** est identique à la **SEQUENCE** initiale du même nombre de **RDN** qui constituent la première partie du nom d'annuaire du sujet (dans le champ **subject** ou le composant **directoryName** de l'extension **subjectAltNames**) du **certificate**. Le nom d'annuaire dans le champ **subject** du **certificat** peut comporter dans sa séquence des RDN de queue supplémentaires absents du nom d'annuaire dans la **base**. La règle de concordance **distinguishedNameMatch** permet de comparer la valeur de la **base** à la séquence initiale de noms d'annuaire relatifs **RDN** dans le nom d'annuaire du sujet du certificat.

Les implémentations conformes ne doivent pas nécessairement reconnaître toutes les formes de nom possibles. Si l'extension est marquée comme critique et qu'une implémentation utilisant le certificat ne reconnaît pas une forme de nom utilisée dans une composante **base,** le certificat doit être traité comme s'il y avait une extension critique non reconnue. Si l'extension est marquée comme non critique et qu'une implémentation utilisant le certificat ne reconnaît pas une forme de nom utilisée dans une composante **base** quelconque, ce sous-arbre peut être ignoré.

NOTE 2 – Lorsque l'on vérifie que les noms de sujet des certificats respectent une contrainte d'utilisation de nom, les noms figurant dans des extensions d'autres noms de sujet non critiques ne doivent pas être ignorés, mais doivent être au contraire pris en compte.

Cette extension peut être critique ou non critique, selon le choix de l'émetteur du certificat. On recommande de le marquer comme critique, sinon un utilisateur de certificat peut ne pas vérifier que les certificats suivants sur l'itinéraire de certification sont situés dans les espaces de nom soumis à des contraintes et voulus par l'autorité CA émettrice.

Si cette extension est présente et est marquée comme critique, un système utilisant des certificats doit vérifier que l'itinéraire de certification en cours de traitement est conforme à la valeur de cette extension.

On trouvera des exemples d'utilisation de l'extension contraintes de nom dans l'Annexe G.

b) *Au § 10.5.2, supprimer le point c) et renuméroter les points suivants en conséquence: les points d), e), f), g), h) deviennent c), d), e), f), g).*

c) *A l'Annexe A.2, remplacer les définitions ASN.1 ci-après associées à* **nameConstraints EXTENSION***:*

```
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 ({-- aucun; c'est-à-dire: au moins un composant est présent -- }))

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

par les suivants:

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

NameConstraintsSyntax ::= SEQUENCE {
    permittedSubtrees         [0]   GeneralSubtrees OPTIONAL,
    excludedSubtrees          [1]   GeneralSubtrees OPTIONAL }
(ALL EXCEPT ({ -- aucun; c'est-à-dire: au moins un composant est présent -- }))

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

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

BaseDistance ::= INTEGER (0..MAX)
```

d) A l'Annexe A.2, remplacer l'attribution d'identificateur d'objet suivante:

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

par:

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

e) A l'Annexe A.2, remplacer la série ci-après d'identificateurs d'objets qui ne sont pas utilisés dans la présente Spécification:

```
-- Les IDENTIFICATEURS D'OBJETS suivants ne sont pas utilisés dans la présente Spécification:
-- {id-ce 2}, {id-ce 3}, {id-ce 4}, {id-ce 5}, {id-ce 6}, {id-ce 7},
-- {id-ce 8}, {id-ce 10}, {id-ce 11}, {id-ce 12}, {id-ce 13},
-- {id-ce 22}, {id-ce 25}, {id-ce 26}, {id-ce 30}
```

par:

```
-- Les IDENTIFICATEURS D'OBJETS suivants ne sont pas utilisés dans la présente Spécification:
-- {id-ce 2}, {id-ce 3}, {id-ce 4}, {id-ce 5}, {id-ce 6}, {id-ce 7},
-- {id-ce 8}, {id-ce 10}, {id-ce 11}, {id-ce 12}, {id-ce 13},
-- {id-ce 22}, {id-ce 25}, {id-ce 26}
```

f) Remplacer le texte figurant dans l'Annexe G.3 par le suivant:

G.3 Utilisation de l'extension contraintes de nom

G.3.1 Exemples de format de certificat comportant une extension contraintes de nom

Les autorités de certification peuvent fixer différentes restrictions concernant les noms de sujet (dans le champ **subject** ou dans l'extension **subjectAltName**) des certificats suivants sur l'itinéraire de certification, en incluant l'extension de contraintes de nom dans leurs certificats CA. Le présent paragraphe décrit des exemples de certificats CA comportant l'extension de contraintes de nom et indique les conditions à remplir pour que les certificats suivants soient acceptables sur un itinéraire de certification connexe.

Afin de simplifier les exemples, seule la forme de nom DN (nom d'annuaire) est utilisée dans l'extension de contraintes de nom.

G.3.1.1 Exemples de ***permittedSubtrees*** (*sous-arbres autorisés*)

(1-1) Si le certificat de l'autorité CA contient l'extension de contraintes de nom ci-après, dans tous les certificats suivants sur l'itinéraire de certification, chaque nom de sujet (dans le champ **subject** ou dans l'extension **subjectAltName**) figurant sous la forme de nom DN, s'il existe, est identique ou subordonné à Acme Inc. aux Etats-Unis (c'est-à-dire {C=US, O=Acme Inc}), pour que ce certificat soit acceptable.

extension **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
{{**base(directoryName**) {C=US, O=Acme Inc}}}	(vide)

(1-2) Si le certificat de l'autorité CA contient l'extension de contraintes de nom ci-après, dans tous les certificats suivants sur l'itinéraire de certification, chaque nom de sujet (dans le champ **subject** ou dans l'extension **subjectAltName**) figurant sous la forme de nom DN, s'il existe, est identique ou directement subordonné à Acme Inc. aux Etats-Unis (c'est-à-dire {C=US, O=Acme Inc}), pour que ce certificat soit acceptable.

extension **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
{{**base**(**directoryName**) {C=US, O=Acme Inc}, **maximum 1**}}	(vide)

(1-3) Si le certificat de l'autorité CA contient l'extension de contraintes de nom ci-après, dans tous les certificats suivants sur l'itinéraire de certification, chaque nom de sujet (dans le champ **subject** ou dans l'extension **subjectAltName**) figurant sous la forme de nom DN, s'il existe, est subordonné à Acme Inc. aux Etats-Unis (c'est-à-dire {C=US, O=Acme Inc}), pour que ce certificat soit acceptable.

extension **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
{{**base**(**directoryName**) {C=US, O=Acme Inc}, **minimum 1**}}	(vide)

(1-4) Si le certificat de l'autorité CA contient l'extension de contraintes de nom ci-après, dans tous les certificats suivants sur l'itinéraire de certification, chaque nom de sujet (dans le champ **subject** ou dans l'extension **subjectAltName**) figurant sous la forme de nom DN, s'il existe, est identique ou directement subordonné à Acme Inc. aux Etats-Unis (c'est-à-dire {C=US, O=Acme Inc}), ou identique ou subordonné à Acme Ltd au Royaume-Uni (c'est-à-dire {C=UK, O=Acme Ltd}), pour que ce certificat soit acceptable.

extension **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**directoryName**) {C=UK, O=Acme Ltd}}}	(vide)

G.3.1.2 Exemples de ***excludedSubtrees*** *(sous-arbres exclus)*

(2-1) Si le certificat de l'autorité CA contient l'extension de contraintes de nom ci-après, dans tous les certificats suivants sur l'itinéraire de certification, aucun nom de sujet (dans le champ **subject** ou dans l'extension **subjectAltName**) figurant sous la forme de nom DN, s'il existe, n'est identique ou subordonné à Acme Corp. au Canada (c'est-à-dire {C=CA, O=Acme Corp}), pour que ce certificat soit acceptable.

extension **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
(vide)	{{**base**(**directoryName**) {C=CA, O=Acme Corp}}}

(2-2) Si le certificat de l'autorité CA contient l'extension de contraintes de nom ci-après, dans tous les certificats suivants sur l'itinéraire de certification, aucun nom de sujet (dans le champ **subject** ou dans l'extension **subjectAltName**) figurant sous la forme DN, s'il existe, n'est subordonné à aucune des filiales directes de Acme Corp. au Canada (c'est-à-dire {C=CA, O=Acme Corp}), pour que ce certificat soit acceptable.

extension **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
(vide)	{{**base**(**directoryName**) {C=CA, O=Acme Corp}, **minimum 2**}}

(2-3) Si le certificat de l'autorité CA contient l'extension de contraintes de nom ci-après, dans tous les certificats suivants sur l'itinéraire de certification, aucun nom de sujet (dans le champ **subject** ou dans l'extension **subjectAltName**) figurant sous la forme DN, s'il existe, n'est identique à Acme Corp. au Canada (c'est-à-dire {C=CA, O=Acme Corp}), pour que ce certificat soit acceptable.

extension **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
(vide)	{{**base**(**directoryName**) {C=CA, O=Acme Corp}, **maximum 0**}}

(2-4) Si le certificat de l'autorité CA contient l'extension de contraintes de nom ci-après, dans tous les certificats suivants sur l'itinéraire de certification, aucun nom de sujet (dans le champ **subject** ou dans l'extension **subjectAltName**) figurant sous la forme de nom DN, s'il existe, n'est identique ni subordonné à Acme Corp. au Canada (c'est-à-dire {C=CA, O=Acme Corp}), ni identique ou subordonné à Asia Acme au Japon (c'est-à-dire {C=JP, O=Asia Corp}), pour que ce certificat soit acceptable.

extension **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
(vide)	{{**base**(**directoryName**) {C=CA, O=Acme Corp}}, {**base**(**directoryName**) {C=JP, O=Asia Acme}}}

G.3.1.3 Exemples de **permittedSubtrees** (*sous-arbres autorisés*) et de **excludedSubtrees** (*sous-arbres exclus*)

(3-1) Si le certificat de l'autorité CA contient l'extension de contraintes de nom ci-après, dans tous les certificats suivants sur l'itinéraire de certification, chaque nom de sujet (dans le champ **subject** ou dans l'extension **subjectAltName**) figurant sous la forme de nom DN, s'il existe, est identique ou subordonné à Acme Inc. aux Etats-Unis (c'est-à-dire {C=US, O=Acme Inc}), à l'exception de l'unité de R&D de la société Acme Inc. et des entités qui en dépendent, pour que ce certificat soit acceptable.

extension **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
{{**base**(**directoryName**) {C=US, O=Acme Inc}}}	{{**base**(**directoryName**) {C=US, O=Acme Inc, OU=R&D}}}

(3-2) Si le certificat de l'autorité CA contient l'extension de contraintes de nom ci-après, dans tous les certificats suivants sur l'itinéraire de certification, chaque nom de sujet (dans le champ **subject** ou dans l'extension **subjectAltName**) figurant sous la forme de nom DN, s'il existe, est identique à l'une des filiales directes de la société Acme Inc. aux Etats-Unis (c'est-à-dire {C=US, O=Acme Inc}), à l'exception de l'unité des achats (c'est-à-dire {C=US, O=Acme Inc, OU=Purchasing}), pour que ce certificat soit acceptable.

extension **nameConstraints**	
permittedSubtrees	**excludedSubtrees**
{{**base**(**directoryName**) {C=US, O=Acme Inc}, **minimum 1**, **maximum 1**}}	{{**base**(**directoryName**) {C=US, O=Acme Inc, OU=Purchasing}}}

G.3.2 Exemples de traitement des certificats comportant une extension de contraintes de nom

Les exemples du présent paragraphe décrivent le mode de validation des noms du sujet (dans le champ **subject** ou dans l'extension **subjectAltName**) lors du traitement du certificat par rapport aux variables d'état de traitement d'itinéraire, à savoir *permitted-subtrees* et *excluded-subtrees.*

Pour simplifier ces exemples, seules les formes de nom DN (**directoryName**) et rfc822 name (**rfc822Name**) sont utilisées dans l'extension de contraintes de nom.

G.3.2.1 Contraintes imposées aux espaces de nom par la variable *permitted-subtrees* dans la forme de nom DN

Dans ce cas, pour que le certificat soit acceptable, chaque nom de sujet (dans le champ **subject** ou dans l'extension **subjectAltName**) figurant sous la forme de nom DN dans le certificat en question se conforme à la contrainte imposée par la variable d'état de traitement d'itinéraire *permitted-subtrees*.

(1-1) Une variable "permitted subtree" est présente pour une forme de nom DN.

Variables d'état de traitement d'itinéraire	
permitted-subtrees	*excluded-subtrees*
{{**base**(**directoryName**) {C=US, O=Acme Inc}}}	AUCUNE

Exemples de certificats acceptables

1	**subject** = {C=US, O=Acme Inc, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName** (**rfc822Name**) = manager@purchasing.acme.com
4	**subject** = {} **subjectAltName** (**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName** (**rfc822Name**) = manager@purchasing.acme.com
5	**subject** = {} **subjectAltName** (**rfc822Name**) = manager@purchasing.acme.com
6	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName** (**directoryName**) = {C=US, O=Acme Inc, OU=Accounting}

Exemples de certificats inacceptables

1	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing}
2	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName** (**directoryName**) = {C=US, O=*Acme Ltd*, OU=Purchasing}
3	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName** (**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
4	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName** (**directoryName**) = {C=US, O=*Acme Ltd*, OU=Accounting}

(1-2) Deux variables "permitted subtree" sont présentes pour une forme DN.

Variables d'état de traitement d'itinéraire	
permitted-subtrees	*excluded-subtrees*
{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**directoryName**) {C=US, O=Acme Ltd}}}	AUCUNE

Exemples de certificats acceptables

1	**subject** = {C=US, O=Acme Ltd, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU=Purchasing}
3	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
5	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU= Accounting}
6	**subject** = {} **subjectAltName(rfc822Name)** = manager@purchasing.acme.com

Exemples de certificats inacceptables

1	**subject** = {C=US, O=*Acme International*, OU=Accounting}
2	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme International*, OU=Accounting}
3	**subject** = {C=US, O=*Acme International*, OU=Accounting} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
4	**subject** = {C=US, O=*Acme International*, OU=Accounting} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Corp*, OU=Accounting}
5	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme International*, OU=Accounting} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com

G.3.2.2 Contraintes imposées aux espaces de nom par la variable *excluded-subtrees* dans une forme de nom DN

Dans ce cas, pour que ce certificat soit acceptable, chaque nom de sujet (dans le champ **subject** ou dans l'extension **subjectAltName**) figurant sous la forme de nom DN dans le certificat en question se conforme à la contrainte imposée par la variable d'état de traitement d'itinéraire *excluded-subtrees*.

(2-1) Un composant "excluded subtree" est présent pour la forme de nom DN.

Variables d'état de traitement d'itinéraire	
permitted-subtrees	*excluded-subtrees*
AUCUNE	{{**base**(**directoryName**) {C=US, O=Acme Ltd}}}

Exemples de certificats acceptables

1	**subject** = {C=US, O=Acme Inc, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
5	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Accounting}
6	**subject** = {} **subjectAltName(rfc822Name)** = manager@purchasing.acme.com

Exemples de certificats inacceptables

1	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing}
2	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Ltd*, OU=Accounting}

(2-2) Deux composants "excluded subtree" sont présents pour la forme de nom DN.

Variables d'état de traitement d'itinéraire	
permitted-subtrees	*excluded-subtrees*
AUCUNE	{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**directoryName**) {C=US, O=Acme Ltd}}}

Exemples de certificats acceptables

1	**subject** = {C=US, O=Acme International, OU=Purchasing}
2	**subjaect** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme International, OU=Purchasing}
3	**subject** = {C=US, O=Acme International, OU=Purchasing} **subjectAltName**(**rfc822Name**) = purchasing@acme-international.com
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme International, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme N.Y, OU=Purchasing} **subjectAltName**(**rfc822Name**) = purchasing@acme-international.com
5	**subject** = {} **subjectAltName(rfc822Name)** = purchasing@acme-international.com

Exemples de certificats inacceptables

1	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing}
2	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing}
3	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme International, OU=Accounting}
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme International, OU=Purchasing} **subjectAltName**(**rfc822Name**) = purchasing@acme-international.com

G.3.2.3 Contraintes imposées aux espaces de nom par la variable *permitted subtrees* dans plusieurs formes de nom

Dans ce cas, pour que le certificat soit acceptable, chaque nom de sujet (dans le champ **subject** ou dans l'extension **subjectAltName**) figurant sous la forme de nom DN ou rfc822 Name dans le certificat en question se conforme à la contrainte imposée par la variable d'état de traitement de l'itinéraire *permitted-subtrees*.

Un sous-arbre autorisé pour la forme de nom DN et un autre sous-arbre autorisé pour la forme de nom **rfc822Name** sont présents.

Variables d'état de traitement d'itinéraire	
permitted-subtrees	*excluded-subtrees*
{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**rfc822Name**) {.acme.com}}}	AUCUNE

Exemples de certificats acceptables

1	**subject** = {C=US, O=Acme Inc, OU=Purchasing}
2	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Accounting}
4	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
5	**subject** = {} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-inc.com
6	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-inc.com

Exemples de certificats inacceptables

1	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing}
2	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
3	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme-inc.com*
4	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme-ltd.com*

G.3.2.4 Contraintes imposées aux espaces de nom par la variable *excluded-subtrees* dans plusieurs formes de nom

Dans ce cas, pour que le certificat soit acceptable, chaque nom de sujet (dans le champ **subject** ou dans l'extension **subjectAltName**) figurant sous la forme de nom DN ou rfc822 Name dans le certificat en question se conforme à la contrainte imposée par la variable d'état de traitement d'itinéraire *excluded-subtrees*.

Variables d'état de traitement d'itinéraire	
permitted-subtrees	*excluded-subtrees*
AUCUNE	{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**rfc822Name**) {.acme.com}}}

Exemples de certificats acceptables

1	**subject** = {C=US, O=Acme Ltd, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
3	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
4	**subject** = {} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-inc.com
5	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-ltd.com

Exemples de certificats inacceptables

1	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
3	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
4	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-inc.com
5	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
6	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Inc*, OU=Accounting}

G.3.3 Exemples de cas où plusieurs certificats croisés comportant une extension de contraintes de nom sont nécessaires

Dans certains cas, l'obtention des résultats escomptés peut exiger l'émission par une autorité CA de plusieurs certificats à destination d'une autre autorité CA. Cela peut être le cas si certaines des exigences liées aux contraintes de nom sont contradictoires ou si l'évaluation disjonctive des différentes formes de nom est requise.

G.3.3.1 Exigences contradictoires liées aux contraintes d'espace de nom

Supposons par exemple que la société Acme ait 20 succursales aux Etats-Unis.

La société Widget veut certifier en retour l'autorité de certification centrale de la société Acme, mais souhaite que la communauté Widget n'utilise que les certificats Acme pour les entités qui répondent aux critères suivants:

- succursales 1 à 19 de la société Acme, toutes les entités étant acceptables;
- succursale 20 de la société Acme, toutes les entités étant inacceptables, sauf celles du département des achats.

Ce résultat pourrait être obtenu par l'émission de deux certificats, en procédant comme suit: le premier certificat devrait comporter un champ **permittedSubtrees** de {base: C=US, O=Acme} et un champ **excludedSubtrees** de {base: C=US, O=Acme, OU=branch20}. Le second certificat comporterait un champ **permittedSubtrees** de{base: C=US, O=Acme, OU=branch20, OU=purchasing}.

G.3.3.2 Evaluation disjonctive des contraintes d'espace de nom

Supposons que l'autorité CA d'une organisation X émette des certificats comportant des noms de domaine Internet sous le sous-arbre x.com, tandis qu'une autre autorité CA d'une organisation Y émet des certificats comportant des noms distinctifs X.500 sous le sous-arbre o=y, c=US. Supposons en outre que l'autorité CA de l'organisation A ait certifié en retour les autorités CA des organisations X et Y et qu'une troisième autorité CA d'une organisation B souhaite certifier en retour l'autorité CA de l'organisation A et, de plus, se fier aux certificats émis par les autorités CA des organisations X et Y. Si l'autorité CA de l'organisation B émet un certificat croisé à l'intention de l'autorité CA de l'organisation A contenant une extension de contraintes de nom avec des sous-arbres autorisés x.com et o=y, c=US (en plus de l'espace de nom de l'autorité CA de l'organisation A), dans ce cas, si l'autorité CA de l'organisation X ou Y ajoute des formes de nom supplémentaires à ses certificats qui contiennent respectivement des noms distinctifs ou des noms de domaine, les certificats de cette autorité ne seront plus valables pour les parties faisant confiance qui utilisent l'autorité CA de l'organisation B comme ancre de confiance. Une solution à ce problème serait que l'autorité CA de l'organisation B émette deux certificats croisés à l'intention de l'autorité CA de l'organisation A, l'un contenant une extension de contraintes de nom avec le sous-arbre autorisé x.com, et l'autre contenant le sous-arbre autorisé o=y, c=US.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
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	Gestion des télécommunications y compris le RGT et maintenance des réseaux
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, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2007