UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.509

Corrigendum 2

(02/2001)

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 2

Recommandation UIT-T X.509 (1997) – Corrigendum 2

(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 2

Source

Le Corrigendum 2 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 2 février 2001. Un texte identique est publié comme Corrigendum technique 2 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 n'avait pas 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 2

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

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

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

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

Au § 11.2, supprimer le deuxième alinéa:

La production d'un certificat … compromission improbable.

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

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

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

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

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

1) *Ajouter* "**id-mr**" *à la liste d'objets importés depuis le module* **UsefulDefinitions** *dans le module* **authenticationFramework**.

2) *Ajouter* "**AttributeType**"*,* "**Attribute**" *et* "**MATCHING-RULE**" *à l'ensemble d'objets importés dans le module* **authenticationFramework** *depuis le module* **InformationFramework**.

3) *Ajouter* "**GeneralNames**" *à l'ensemble d'objets importés dans le module* **authenticationFramework** *depuis le module* **CertificateExtensions**.

4) *Ajouter la définition suivante au module* **authenticationFramework** *car elle est importée dans d'autres modules des Recommandations de la série X.500, mais ne figure pas dans l'édition de 1997 de la Recommandation X.509:*

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

5) *Ajouter les assignations d'identificateur d'objet suivantes dans le module* **authenticationFramework***:*

id-at-attributeCertificateRevocationList OBJECT IDENTIFIER ::= {id-at 59}

id-mr-attributeCertificateMatch OBJECT IDENTIFIER ::= {id-mr 42}

6) *Ajouter* "**Time**" *à l'ensemble d'objets importés dans le module* **CertificateExtensions** *depuis le module* **authenticationFramework**.

7) *Dans le module* **CertificateExtensions** *et au § 12.7.2 du corps de la Recommandation X.509, remplacer:*

CertPolicySet ::= SEQUENCE (1..MAX) OF CertPolicyId

par:

CertPolicySet ::= SEQUENCE SIZE (1..MAX) OF CertPolicyId

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

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

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

Dans l'article 8:

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

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

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

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

i) elle peut exclure l'extension du certificat;

ii) elle peut inclure l'extension et la marquer comme étant non critique;

iii) elle peut inclure l'extension et la marquer comme étant critique.

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

i) il peut ne pas tenir compte de l'extension et accepter le certificat (les autres éléments étant les mêmes);

ii) il peut effectuer le traitement de l'extension et accepter ou rejeter le certificat en fonction du contenu de l'extension et des conditions de traitement (par exemple, les valeurs en cours des variables de traitement de l'itinéraire).

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

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

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

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

Au § 12.1:

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

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

Au § 12.2.2.3:

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

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

Au § 12.2.2.4:

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

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

Au § 12.4.2.1:

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

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

Au § 12.4.2.2:

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

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

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

A l'article 8:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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