UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T X.509

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Corrigendum 3
(04/2004)

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 3

Recommandation UIT-T X.509 (2000) – Corrigendum technique 3

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
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 3

Source

Le Corrigendum 3 de la Recommandation UIT-T X.509 (2000) a été approuvé le 29 avril 2004 par la Commission d'études 17 (2001-2004) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8. 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.

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 responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

© UIT 2005

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

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 3

(Portant sur la correction des erreurs signalées dans les relevés de défaut 281, 282, 289, 291, 296, 298, 299, 300, 301, 304 et 305.)

Une version précédemment approuvée, mais non publiée, du présent Corrigendum technique contenait le texte des rectifications à apporter aux erreurs signalées dans le relevé de défaut 280. Suite à l'approbation par vote du projet de Corrigendum technique rectifiant les erreurs signalées dans le relevé de défaut 280, les réalisateurs ont constaté que la méthode adoptée dans la 4ème édition pour traiter la révocation de certificat de clé publique et d'attribut laissait grandement à désirer. Le texte rectifiant les erreurs signalées dans le relevé de défaut 305 reprend dans la 4ème édition la méthode spécifiée dans la 3ème édition. Etant donné que la publication du texte rectifiant les erreurs signalées dans le relevé de défaut 280 n'est plus nécessaire et qu'elle risquerait d'embrouiller les choses pour les produits d'implémentation conformes à la 4ème édition, le texte des rectifications à apporter aux erreurs signalées dans le relevé de défaut 280 est supprimé de la présente version du Corrigendum technique.

1) Correction des défauts signalés dans le relevé de défaut 281

Dans le § 8.6.2.6, ajouter après la syntaxe ASN.1 l'alinéa suivant:

La valeur du type **CRLDistPointsSyntax** est définie comme dans l'extension de point de répartition de liste CRL au § 8.6.2.1.

Remplacer le § B.5.1.4 existant par le suivant:

Toutes les conditions suivantes doivent être satisfaites pour déterminer si une liste CRL est l'une de celles indiquées par un point de répartition dans l'extension de point de répartition de liste CRL ou l'extension de liste CRL la plus récente figurant dans le certificat:

- soit le champ **distributionPoint** est absent de l'extension de point de répartition émetteur de la liste CRL (uniquement lorsque cette extension n'est pas marquée comme critique), soit l'un des noms du champ **distributionPoint** de l'extension de point de répartition de liste CRL ou de l'extension de liste CRL la plus récente du certificat doit correspondre à l'un des noms figurant dans le champ **distributionPoint** de l'extension de point de répartition émetteur de la liste CRL. En variante, l'un des noms du champ **cRLIssuer** de l'extension de point de répartition de liste CRL ou de l'extension de liste CRL la plus récente du certificat peut correspondre à l'un des noms de point de répartition du point IDP;
- si le certificat est un certificat d'entité finale, la liste CRL ne doit alors pas contenir de champ **onlyContainsAuthorityCerts** positionné sur **VRAI** dans l'extension de point de répartition émetteur de la liste CRL;
- si le champ **onlyContainsAuthorityCerts** est positionné sur **VRAI** dans l'extension de point de répartition émetteur de la liste CRL, le certificat en cours de vérification doit alors contenir l'extension **basicConstraints** avec un composant **cA** positionné sur **VRAI**;
- si le champ **reasons** figure dans l'extension de point de répartition de liste CRL ou de l'extension de liste CRL la plus récente du certificat, le champ **onlySomeReasons** doit alors, soit être absent de l'extension de point de répartition émetteur de la liste CRL, soit contenir l'un au moins des codes motif déclarés dans l'extension de point de répartition de liste CRL ou l'extension de liste CRL la plus récente du certificat;
- si le champ **cRLIssuer** ne figure pas dans l'extension appropriée (extension de point de répartition de liste CRL ou extension de liste CRL la plus récente du certificat), la liste CRL doit alors être signée par la même autorité de certification que celle qui a signé le certificat;

– si le champ **cRLIssuer** figure dans l'extension appropriée (extension de point de répartition de liste CRL ou extension de liste CRL la plus récente du certificat), la liste CRL doit alors être signée par l'émetteur de liste CRL indiqué dans le champ **cRLIssuer** et la liste CRL doit contenir l'extension de point de répartition émetteur avec le champ **indirectCRL** positionné sur **VRAI**.

NOTE – Lorsqu'on procède à un essai visant à vérifier que le champ **reasons** ou **cRLIssuer** est présent, cet essai n'est concluant que si le champ considéré est présent dans le même champ **DistributionPoint** de l'extension de point de répartition de liste CRL ou de l'extension de liste CRL la plus récente pour laquelle il y a une correspondance de nom dans le champ point de répartition correspondant de l'extension de point IDP de la liste CRL.

2) Correction des défauts signalés dans le relevé de défaut 282

Dans le § 7, dans l'alinéa suivant immédiatement la définition du champ version et dans l'alinéa suivant immédiatement la définition du champ extensions, remplacer:

"... conformément aux règles d'extensibilité décrites au 7.5.2.2 de la Rec. UIT-T X.519 | ISO/CEI 9594-5."

par

"... conformément aux règles d'extensibilité décrites au § 12.2.2 de la Rec. UIT-T X.519 | ISO/CEI 9594-5."

Dans le § 7.3, immédiatement après la NOTE 6 et dans le § 12.1 immédiatement après la définition du champ extensions, ajouter le nouvel alinéa suivant:

"Si des éléments inconnus figurent dans les extensions et si l'extension n'est pas marquée comme étant critique, ces éléments inconnus seront alors ignorés conformément aux règles d'extensibilité décrites au § 12.2.2 de la Rec. UIT-T X.519 | ISO/CEI 9594-5."

3) Correction des défauts signalés dans le relevé de défaut 289

Remplacer le texte du point c) du § 10.1 par le suivant:

c) un ensemble *initial-policy-set* constitué d'un ou de plusieurs identificateurs de certificat de politique indiquant qu'une ou plusieurs politiques sont acceptables par l'utilisateur de certificat aux fins de traitement de l'itinéraire de certification; cet ensemble peut également prendre la valeur *any-policy*, mais il ne peut pas être nul;

Remplacer le § 10.5.4, dans son intégralité, par le paragraphe suivant:

10.5.4 Traitement final

Une fois que tous les certificats de l'itinéraire ont été traités, les actions suivantes sont effectuées:

a) Déterminer l'ensemble *authorities-constrained-policy-set* d'après le tableau *authorities-constrained-policy-set*. Si le tableau est vide, l'ensemble *authorities-constrained-policy-set* est l'ensemble vide ou nul. Si *authorities-constrained-policy-set[0, path-depth]* est *any-policy*, alors, *authorities-constrained-policy-set* est *any-policy*. Dans les autres cas, *authorities-constrained-policy-set* est, pour chaque rangée du tableau, égal à la valeur de la cellule la plus à gauche qui ne contient pas l'identificateur *any-policy*.

b) Calculer l'ensemble *user-constrained-policy-set* en formant l'intersection de l'ensemble *authorities-constrained-policy-set* et de l'ensemble *initial-policy-set*.

c) Si l'indicateur *explicit-policy-indicator* est sélectionné, vérifier que ni l'ensemble *authorities-constrained-policy-set* ni l'ensemble *user-constrained-policy-set* n'est vide.

Si l'une quelconque des vérifications précédentes échoue, la procédure se termine alors en renvoyant une indication d'échec avec un code motif adéquat, l'indicateur *explicit-policy-indicator*, l'ensemble *authorities-constrained-policy-set* et l'ensemble *user-constrained-policy-set*. Si l'échec est dû à un ensemble *user-constrained-policy-set* vide, l'itinéraire est valide dans le cadre de la politique ou des politiques contraintes par l'autorité, mais aucune n'est acceptable pour l'utilisateur.

Si aucun des contrôles ci-dessus ne devait échouer pour le certificat final, la procédure se termine alors en renvoyant une indication de succès ainsi que l'indicateur *explicit-policy-indicator*, l'ensemble *authorities-constrained-policy-set* et l'ensemble *user-constrained-policy-set*.

4) Correction des défauts signalés dans le relevé de défaut 291

Dans le § 3.3.44, dans la définition de "certificat de clé publique", remplacer "non falsifiables par chiffrement" *par* "non falsifiables par signature numérique".

Dans le § 3.1, ajouter "signature numérique" *à la liste des termes définis dans la Rec. CCITT X.800 | ISO/CEI 7498-2. Ajouter ce terme dans l'ordre alphabétique et renuméroter en conséquence les points restants de la liste*.

5) Correction des défauts signalés dans le relevé de défaut 296

Dans le § B.5.1.1, dans la première phrase, ajouter immédiatement après "les certificats d'autorité de certification" *le membre de phrase* "émis par l'émetteur de la liste CRL".

Dans le § B.5.1.1, remplacer le troisième alinéa en retrait par le suivant:

– l'extension de point de répartition émetteur ne doit pas contenir de champ **distributionPoint** ou un des noms de ce champ doit correspondre au champ **issuer** de la liste CRL;

Dans le § B.5.1.2, remplacer le troisième alinéa en retrait par le suivant:

– l'extension de point de répartition émetteur ne doit pas contenir de champ **distributionPoint** ou un des noms de ce champ doit correspondre au champ **issuer** de la liste CRL;

Dans le § B.5.1.3, remplacer le troisième alinéa en retrait par le suivant:

– l'extension de point de répartition émetteur ne doit pas contenir de champ **distributionPoint** ou un des noms de ce champ doit correspondre au champ **issuer** de la liste CRL;

Dans le § B.5.1.4, dans le premier alinéa en retrait, remplacer la dernière phrase par la suivante:

– En variante, si le champ **distributionPoint** est absent de l'extension de point de répartition de la liste CRL du certificat, l'un des noms du champ **cRLIssuer** de l'extension de point de répartition de liste CRL du certificat peut correspondre à l'un des noms de point de répartition du point IDP. Si les champs **distributionPoint** et **cRLIssuer** sont tous deux absents de l'extension de point de répartition de la liste CRL du certificat, le champ **issuer** du certificat peut correspondre à l'un des noms de l'extension de point de répartition du point IDP;

6) Correction des défauts signalés dans le relevé de défaut 298

Dans le § 7.3, ajouter à la suite de l'énumération introduite par la phrase "une autorité qui émet des certificats et les révoque par la suite:", le nouveau point d) suivant:

d) si elle n'utilise que des listes CRL subdivisées, émettra un ensemble complet de listes CRL subdivisées englobant l'ensemble complet des certificats dont le statut de révocation sera signalé au moyen du mécanisme de listes CRL. Ainsi, l'ensemble complet de listes CRL subdivisées équivaudra à une liste CRL complète pour le même ensemble de certificats, si l'émetteur des listes CRL n'utilisait pas de listes CRL subdivisées.

Dans le § 8.6.2.2, ajouter immédiatement après la première phrase le nouveau texte suivant:

Si seules des listes CRL subdivisées sont utilisées, l'ensemble complet de listes CRL subdivisées doit englober l'ensemble complet des certificats dont le statut de révocation sera signalé au moyen du mécanisme de listes CRL. Ainsi, l'ensemble complet de listes CRL subdivisées équivaudra à une liste CRL complète pour le même ensemble de certificats, si l'émetteur des listes CRL n'utilisait pas de listes CRL subdivisées.

7) Correction des défauts signalés dans le relevé de défaut 299

Insérer le nouveau § 7.4 suivant:

7.4 Répudiation d'une signature numérique

Tout participant à un événement peut ultérieurement décider de répudier tout document qu'il a signé numériquement au cours de cet événement. Par exemple, un participant peut très bien contester avoir participé à l'élaboration d'une clé ou être l'auteur d'un message électronique signé, tout aussi facilement qu'il peut contester avoir signé un document dans l'intention d'être lié par le contenu de ce document. La répudiation peut ne pas aboutir. La Rec. UIT-T X.813 | ISO/CEI 10181-4 définit la procédure de résolution des litiges suivante:

1) la production des preuves;
2) le transfert, la conservation et la consultation des preuves;
3) la vérification des preuves;
4) la résolution des litiges.

Les preuves produites peuvent inclure, de manière non limitative:

– des enregistrements d'audit ayant trait à l'événement et à la déclaration d'intention;
– des attestations établies par les notaires des parties adverses;
– des déclarations de principe;
– des informations comportant une signature numérique, au nombre desquelles des enregistrements d'audit et des attestations notariales;
– les horodatages des informations comportant une signature numérique;
– les certificats confirmant la validité de la signature numérique;
– les informations de révocation appropriées publiées et disponibles au moment où l'événement contesté s'est produit;
– les éventuelles révocations de certificat ultérieures à l'heure à laquelle l'événement s'est produit, indiquant que la clé a été mise en danger avant que cet événement ne se produise.

L'intégrité des données stockées qui peuvent être présentées comme preuves peut être maintenue par divers moyens: contrôle d'accès, stockage des hachages par un tiers de confiance, signature numérique, par exemple. En outre, il peut être nécessaire de renforcer périodiquement la protection desdites données stockées pour faire échec aux améliorations du traitement informatique ou de l'analyse cryptographique.

NOTE – Ni le type et le nombre de preuves produites ni le niveau d'intégrité ne sont précisés par la présente Spécification d'annuaire. Toutefois, il est à prévoir que le niveau d'effort sera proportionné au risque encouru.

La vérification des preuves peut obliger à revalider les signatures numériques des différentes données – messages, documents, certificats, listes de révocation de certificats (CRL), horodatages, par exemple – qui ont été utilisées au cours du processus de validation initial. Le fait qu'un certificat ne soit plus valable ne doit pas empêcher de l'utiliser pour revalider des signatures créées pendant la période de validité de ce certificat. Un certificat qui a été révoqué peut être utilisé si l'on peut déterminer que ce certificat était valable au moment où l'événement contesté s'est produit.

Même si toutes les preuves numériques décrites ci-dessus sont considérées comme étant techniquement valables, d'autres conditions – telles que l'intention du signataire, son interprétation des faits ou sa qualité légale, par exemple – peuvent autoriser le signataire à les répudier.

Remplacer le § 8.2.2.3 par le suivant:

8.2.2.3 Extension d'utilisation de clé

Ce champ indique l'utilisation prévue pour le certificat émis. Par ailleurs, la politique adoptée peut imposer des contraintes qui limiteront l'utilisation prévue. Cette politique peut être énoncée dans la définition de la politique générale d'un certificat, dans un contrat ou dans toute autre spécification. Toutefois, une politique ne doit pas annuler la contrainte indiquée par un bit du champ **KeyUsage**. Par exemple, une politique de certificat ne saurait autoriser à utiliser un certificat comme signature numérique dans le cas où le champ **KeyUsage** indiquerait que ce certificat ne peut être utilisé que comme accord de clé.

Sélectionner une valeur donnée pour le champ **KeyUsage** dans un certificat ne constitue pas en soi une indication, pour une instance de communication, que les participants de la communication prennent des mesures adaptées à cette valeur, par exemple au moment où ils signent un document. La définition des méthodes que pourront utiliser les participants pour signaler leur intention en ce qui concerne une instance de communication donnée (choix du contenu de cette

instance, par exemple) ne relève pas de la présente spécification d'annuaire. Toutefois, il est à prévoir que plusieurs méthodes coexisteront. Bien que cela ne soit pas recommandé, il est possible d'utiliser le contenu du certificat – la politique de certificat, par exemple – pour signaler l'objet de la signature. Cela étant, comme cette opération a été faite au moment où le certificat a été émis par l'autorité de certification, il se peut qu'une telle utilisation du contenu du certificat soit contraire à la règle qui impose que la déclaration de l'objet de la signature se fasse au moment où le signataire appose sa signature.

Plusieurs bits peuvent être sélectionnés dans une instance de l'extension du champ **keyUsage**. Cela ne doit pas modifier la signification de chacun de ces bits pris isolément mais les valeurs retenues doivent indiquer que le certificat peut être utilisé pour toutes les fins indiquées par les bits sélectionnés. La sélection de plusieurs bits peut comporter des risques. Ces risques feront l'objet d'une annexe informative qui sera établie ultérieurement. Le texte proposé dans l'observation 4 de l'AFNOR extrait de la synthèse des suffrages exprimés sur le Document DTC-6, SC6 N12648, sera incorporé dans cette annexe.

Ce champ est défini comme suit:

```
keyUsage EXTENSION ::= {
    SYNTAX              KeyUsage
    IDENTIFIED BY       id-ce-keyUsage }

KeyUsage ::= BIT STRING {
    digitalSignature        (0),
    contentCommitment       (1),
    keyEncipherment         (2),
    dataEncipherment        (3),
    keyAgreement            (4),
    keyCertSign             (5),
    cRLSign                 (6),
    encipherOnly            (7),
    decipherOnly            (8) }
```

L'utilisation des bits du type **keyUsage** (*utilisation de la clé*) est la suivante:

a) **digitalSignature** (*signature numérique*): vérification des signatures numériques utilisées pour un service d'authentification d'entité, un service d'authentification de l'origine des données ou un service d'intégrité;

b) **contentCommitment** (*acceptation du contenu*): vérification des signatures numériques visant à signaler que le signataire s'engage à accepter les conditions énoncées dans le texte qu'il signe. Le type d'engagement que le certificat permet de prendre peut être soumis à des contraintes supplémentaires par l'autorité de certification, dans le cadre d'une politique de certificat, par exemple. Le type précis d'engagement du signataire – "examiné et approuvé" ou "avec l'intention d'être lié", par exemple – peut être indiqué par le contenu qui est signé – le document signé proprement dit ou des informations signées complémentaires, par exemple.

   Une signature d'acceptation du contenu étant considérée comme une transaction avec signature numérique, le bit **digitalSignature** ne doit pas nécessairement être activé dans le certificat. S'il est activé, cela n'a aucune incidence sur le niveau d'engagement pour lequel le signataire a opté dans le contenu signé.

   Notons qu'il n'est pas fautif de faire référence au bit **keyUsage** en utilisant l'identificateur **nonRepudiation**. Toutefois, l'utilisation de cet identificateur est déconseillée. Quel que soit l'identificateur utilisé, la sémantique de ce bit est définie dans la présente spécification d'annuaire;

c) **keyEncipherment** (*chiffrement de clé*): chiffrement de clés ou d'autres informations de sécurité, par exemple pour le transport de clé;

d) **dataEncipherment** (*chiffrement de données*): chiffrement de données utilisateur, autres que des clés ou des informations de sécurité comme dans l'alinéa c) ci-dessus;

e) **keyAgreement** (*accord de clé*): utilisé comme clé d'agrément d'une clé publique;

f) **keyCertSign** (*signature de certificat de clé*): vérification de la signature d'une autorité de certification pour des certificats.

   La signature d'un certificat étant assimilée à une acceptation du contenu de ce certificat par l'autorité de certification, les bits **digitalSignature** et **contentCommitment** ne doivent ni l'un ni l'autre être activés dans le certificat. Si l'un de ces bits (ou les deux) est (sont) activé(s), cela n'a aucune incidence sur le niveau d'engagement pour lequel le signataire a opté dans le certificat signé;

g) **cRLSign** (*signature de liste CRL*): vérification de la signature d'une autorité pour des listes CRL.

   La signature d'une liste CRL étant assimilée à l'acceptation du contenu de la liste CRL par l'émetteur de la liste CRL, les bits **digitalSignature** et **contentCommitment** ne doivent ni l'un ni l'autre être activés

dans le certificat. Si l'un de ces bits (ou les deux) est (sont) activé(s), cela n'a aucune incidence sur le niveau d'engagement pour lequel le signataire a opté dans la liste CRL signée;

h) **encipherOnly** (*chiffrement seulement*): agrément de clé pour une clé publique utilisée exclusivement pour le chiffrement de données lorsque le bit **keyAgreement** est également positionné (la signification n'est pas définie lorsque l'autre bit d'utilisation de clé est positionné);

i) **decipherOnly** (*déchiffrement seulement*): agrément de clé pour une clé publique utilisée exclusivement pour le déchiffrement de données lorsque le bit **keyAgreement** est également positionné (la signification n'est pas définie lorsque l'autre bit d'utilisation de clé est positionné).

Les spécifications des applications doivent indiquer lequel des deux bits considérés, à savoir le bit **digitalSignature** ou le bit **contentCommitment**, se prête le mieux à l'utilisation de ces applications. Si une application de signature ignore l'intention du signataire en ce qui concerne l'acception du contenu, l'application doit signer et joindre à l'appui de sa signature un certificat dont le bit **digitalSignature** est activé dans l'extension **keyUsage** de ce certificat.

Même si une signature numérique a été vérifiée à l'aide d'un certificat dont seul le bit **digitalSignature** était activé, d'autres facteurs extérieurs à la vérification de la signature numérique peuvent également contribuer à déterminer l'objet de la signature. A l'inverse, même si une signature numérique a été vérifiée à l'aide d'un certificat dont seul le bit **contentCommitment** était activé, des facteurs extérieurs peuvent être utilisés par le signataire pour revenir sur son acceptation du contenu signé.

Le bit **keyCertSign** est utilisable exclusivement dans les certificats d'autorité de certification. Si le champ **KeyUsage** est positionné sur **keyCertSign**, la valeur du composant **cA** (*autorité de certification*) de l'extension **basicConstraints** (*contraintes de base)* doit alors être positionnée sur **VRAI**. Les autorités de certification peuvent également employer d'autres utilisations définies pour les bits dans **KeyUsage**, par exemple **digitalSignature** pour fournir l'authentification et l'intégrité de transactions d'administration en ligne.

Cette extension peut être critique ou non, au choix de l'émetteur du certificat.

Si l'extension est marquée comme critique ou si l'extension est marquée comme non critique mais que le système utilisant des certificats la reconnaît, le certificat sera alors uniquement utilisé dans un but pour lequel le bit d'utilisation de clé est positionné sur un. Si l'extension est marquée comme non critique et que le système utilisant des certificats ne la reconnaît pas, cette extension doit alors être ignorée. Un bit positionné sur zéro indique que la clé n'est pas prévue pour ce but. Si l'extension est présente avec tous ses bits positionnés sur zéro, ceci indique que la clé est prévue pour un autre but que ceux énumérés ci-dessus.

8) Correction des défauts signalés dans le relevé de défaut 300

Remplacer la première phrase du point b) du § 10.5.1 par la suivante:

Dans le cas d'un certificat intermédiaire de version 3, vérifier que l'extension **basicConstraints** est présente et que le composant **cA** figurant dans cette extension est positionné sur VRAI.

9) Correction des défauts signalés dans le relevé de défaut 301

Remplacer le texte du troisième alinéa en retrait de la deuxième phrase du § B.5.2 par le suivant:

– la liste CRL de base est la liste CRL référencée dans la liste dCRL ou dans une liste postérieure;

10) Correction des défauts signalés dans le relevé de défaut 304

Dans l'Annexe F, déplacer la définition:

id-ea-rsa OBJECT IDENTIFIER ::= {id-ea-1}

après le texte suivant:

"-- l'attribution des identificateurs d'objet suivants réserve les valeurs assignées aux fonctions déconseillées"

Supprimer:

-- attribution d'identificateurs d'objet --

11) Correction des défauts signalés dans le relevé de défaut 305

Dans le § 8.6.2, ajouter le nouveau point c) suivant et renuméroter d) à g) les points c) à f) actuels:

c) point de répartition émetteur d'autorité d'attribut;

Dans le § 8.6.2, remplacer la deuxième phrase du dernier alinéa par la suivante:

Le point de répartition émetteur, le point de répartition émetteur d'autorité d'attribut, l'indicateur de liste CRL delta et la mise à jour de base seront utilisés exclusivement comme extensions de liste CRL.

Ajouter à la fin du texte du § 8.6.2, immédiatement avant le § 8.6.2.1, le nouvel alinéa suivant:

Bien qu'elles répondent à des besoins analogues, l'extension de point de répartition émetteur et l'extension de point de répartition émetteur d'autorité d'attribut s'appliquent à des certificats différents. L'extension de point de répartition émetteur s'applique uniquement aux certificats de clé publique délivrés aux utilisateurs ou aux autorités de certification. L'extension de point de répartition émetteur d'autorité d'attribut s'applique uniquement aux certificats d'attribut délivrés aux utilisateurs et aux autorités d'attribut, ainsi qu'aux certificats de clé publique délivrés aux sources d'autorité. Si une liste CRL inclut des types de certificat qui recouvrent ces deux extensions, la liste CRL devra inclure ces deux extensions. Notons que l'extension de domaine d'application de liste CRL définie au § 8.5.2.5 est, elle aussi, analogue à ces deux extensions. Toutefois, l'extension de domaine d'application de liste CRL laissant notoirement à désirer, son utilisation est déconseillée et il convient d'utiliser à la place l'extension de point de répartition émetteur ou l'extension de point de répartition émetteur d'autorité d'attribut.

Dans le § 8.5.2.5 (extension de domaine d'application de liste CRL), remplacer l'alinéa suivant:

Il convient de noter que les extensions **issuingDistributionPoint** et **crlScope** peuvent entrer en conflit et que leur utilisation simultanée n'est pas prévue. Si la liste CRL contient toutefois une extension **issuingDistributionPoint** et une extension **crlScope**, le certificat concerne alors le domaine d'application de la liste CRL si, et seulement s'il est conforme aux critères des deux extensions. Si la liste CRL ne contient aucune des extensions **issuingDistributionPoint** et **crlScope**, le domaine d'application est alors celui de l'autorité dans son ensemble et la liste CRL peut être utilisée pour tout certificat émis par cette autorité.

par le texte suivant:

Il convient de noter que les extensions **issuingDistributionPoint** et **crlScope** peuvent entrer en conflit et que leur utilisation simultanée n'est pas prévue. Si la liste CRL contient toutefois une extension **issuingDistributionPoint** et une extension **crlScope**, le certificat de clé publique concerne alors le domaine d'application de la liste CRL si, et seulement s'il est conforme aux critères des deux extensions. Si la liste CRL contient une extension **AAissuingDistributionPoint**, mais qu'elle ne contient aucune extension **issuingDistributionPoint** ou **crlScope**, le domaine d'application ne contient pas de certificats de clé publique. Si la liste CRL ne contient aucune des extensions **issuingDistributionPoint**, **AAissuingDistributionPoint** ou **crlScope**, le domaine d'application est alors celui de l'autorité dans son ensemble et la liste CRL peut être utilisée pour tout certificat émis par cette autorité. De même, les extensions **AAissuingDistributionPoint** et **crlScope** peuvent entrer en conflit et ne sont pas destinées à être utilisées simultanément. Si la liste CRL contient toutefois une extension **AAissuingDistributionPoint** et une extension **crlScope**, le certificat d'attribut concerne alors le domaine d'application de la liste CRL si, et seulement s'il est conforme aux critères des deux extensions. Si la liste CRL contient une extension **issuingDistributionPoint**, mais qu'elle ne contient aucune extension **AAissuingDistributionPoint** ou **crlScope**, le domaine d'application ne contient pas de certificats d'attribut. Si la liste CRL ne contient aucune extension **issuingDistributionPoint**, **AAissuingDistributionPoint** ou **crlScope**, le domaine d'application est alors celui de l'autorité dans son ensemble et la liste CRL peut être utilisée pour tout certificat émis par cette autorité.

Remplacer le § 8.6.2.2 par le suivant:

8.6.2.2 Extension de point de répartition émetteur

Ce champ d'extension de liste CRL identifie le point de répartition de liste CRL pour les certificats de clé publique de la liste CRL considérée et indique si cette dernière est indirecte ou si son application est limitée à un sous-ensemble des informations de révocation, compte tenu, par exemple, d'un sous-ensemble de l'ensemble des certificats ou d'un sous-ensemble de motifs de révocation. La liste CRL est signée au moyen de la clé privée de l'émetteur de liste CRL, les points de répartition de liste CRL ne possédant pas de paire de clés. Toutefois, une liste CRL répartie par le biais de l'annuaire est stockée dans l'entrée du point de répartition de liste CRL, qui peut ne pas être l'entrée d'annuaire de l'émetteur de la liste CRL. Si les champs point de répartition émetteur, point de répartition émetteur d'autorité d'attribut et domaine d'application de liste CRL sont tous absents, la liste CRL contiendra des éléments pour tous les certificats de clé publique révoqués non caducs en provenance de l'émetteur de la liste CRL. Si les champs point de répartition émetteur et domaine d'application de liste CRL sont tous deux absents, mais que le champ point de répartition émetteur d'autorité d'attribut est présent, le domaine d'application de la liste CRL ne contient pas de certificats de clé publique.

Note de l'éditeur – A noter que lors de l'élaboration de la prochaine édition de la Rec. UIT-T X.509, il conviendra d'ajouter, par suite de la décision du Comité technique 3 et de la correction des défauts signalés dans le relevé de défaut 298, la nouvelle phrase suivante:

Une fois qu'un certificat est paru dans une liste CRL, il ne figurera plus dans toutes les listes CRL suivantes après son expiration. Ce champ est défini comme suit:

```
issuingDistributionPoint EXTENSION : : = {
        SYNTAX IssuingDistPointSyntax
        IDENTIFIED BY id-ce-issuingDistributionPoint }

IssuingDistPointSyntax ::= SEQUENCE {

-- Si les composants onlyContainsUserPublicKeyCerts (contient uniquement des certificats de clé publique
d'utilisateur) et onlyContainsCACerts (contient uniquement des certificats d'autorité de certification) sont tous deux mis
à la valeur FAUX, la liste CRL s'applique aux deux types de certificats --

        distributionPoint                [0] DistributionPointName OPTIONAL,
        onlyContainsUserPublicKeyCerts   [1] BOOLEAN DEFAULT FALSE,
        onlyContainsCACerts              [2] BOOLEAN DEFAULT FALSE,
        onlySomeReasons                  [3] ReasonFlags OPTIONAL,
        indirectCRL                      [4] BOOLEAN DEFAULT FALSE }
```

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 alors 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 alors des révocations pour des certificats d'autorité de certification. Si les valeurs des composants **onlyContainsUserPublicKeyCerts** et **onlyContainCACerts** sont toutes deux égales à "Faux", la liste CRL contient alors des révocations pour des certificats de clé publique d'entité finale et pour des certificats d'autorité de certification. Si le composant **onlySomeReasons** est présent, la liste CRL contient alors uniquement des révocations de certificats de clé publique pour le ou les motifs indiqués; dans le cas contraire, la liste CRL contient des révocations pour tous les motifs. Si la valeur du composant **indirectCRL** (*liste CRL indirecte*) est égale à "Vrai", la liste CRL peut alors contenir des notifications de révocation pour des certificats de clé publique provenant d'autorités autres que l'émetteur de la liste CRL. L'autorité particulière responsable pour chaque entrée est indiquée par l'extension d'entrée d'émetteur de liste CRL du certificat dans cette entrée ou conformément aux règles par défaut décrites au § 8.6.2.3. 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 indiquent cet émetteur de liste CRL dans leurs certificats de clé publique.

Les règles suivantes s'appliquent pour des listes CRL réparties par le biais de l'annuaire. Si la liste CRL est une liste dCRL (*liste delta de révocation de certificat*), elle sera répartie par le biais de l'attribut **deltaRevocationList** du point de répartition associé ou, si aucun point de répartition n'est indiqué, par le biais de l'attribut **deltaRevocationList** de l'entrée de l'émetteur de la liste CRL, quels que soient les paramètres des types de certificats auxquels s'applique la liste CRL. Sauf dans le cas où la liste CRL est une liste dCRL:

- une liste CRL dont le composant **onlyContainsCACerts** est activé et qui ne contient pas d'extension **AAissuingDistributionPoint** sera répartie par le biais de l'attribut **authorityRevocationList** du point de répartition associé ou, si aucun point de répartition n'est indiqué, par le biais de l'attribut **authorityRevocationList** de l'entrée de l'émetteur de la liste CRL.
- Une liste CRL dont le composant **onlyContainsCACerts** est activé et qui contient une extension **AAissuingDistributionPoint** dont le composant **containsUserAttributeCerts** est mis à la valeur "Faux" sera répartie par le biais de l'attribut **authorityRevocationList** du point de répartition associé ou, si aucun point de répartition n'est indiqué, par le biais de l'attribut **authorityRevocationList** de l'entrée de l'émetteur de la liste CRL.
- Une liste CRL dont seul le composant **onlyContainsCACerts** est mis à la valeur "Faux" sera répartie par le biais de l'attribut **certificateRevocationList** du point de répartition associé ou, si aucun point de répartition n'est indiqué, par le biais de l'attribut **certificateRevocationList** de l'entrée de l'émetteur de la liste CRL.
- Une liste CRL qui contient à la fois une extension **issuingDistributionPoint** et une extension **AAissuingDistributionPoint** dont le composant **containsUserAttributeCerts** est activé, sera répartie par le biais de l'attribut **certificateRevocationList** du point de répartition associé ou, si aucun point de répartition n'est indiqué, par le biais de l'attribut **certificateRevocationList** de l'entrée de l'émetteur de la liste CRL.

Cette extension est toujours critique. Un utilisateur de certificat qui ne comprend pas cette extension ne peut pas faire l'hypothèse que la liste CRL contient une liste complète de certificats révoqués de l'autorité indiquée. Les listes CRL qui ne contiennent pas d'extension critique doivent contenir tous les éléments actuels de liste CRL pour l'autorité émettrice, y compris les éléments pour tous les certificats d'utilisateur et certificats d'autorité révoqués.

NOTE 1 – Les moyens utilisés par les autorités pour communiquer les informations de révocation aux émetteurs de liste CRL ne sont pas abordés dans la présente spécification d'annuaire.

NOTE 2 – Si une autorité publie une liste CRL avec un composant **onlyContainsUserPublicKeyCerts** ou **onlyContainsCACerts** mis à la valeur "Vrai", elle doit alors s'assurer que tous les certificats de l'autorité de certification visés par cette liste CRL contiennent l'extension **basicConstraints**.

Ajouter le nouveau paragraphe suivant:

8.6.X.X Extension de point de répartition émetteur d'autorité d'attribut

Ce champ d'extension de liste CRL identifie le point de répartition de liste CRL pour les certificats d'attribut de la liste CRL considérée et indique si cette dernière est indirecte ou si son application est limitée à un sous-ensemble des informations de révocation, compte tenu d'un sous-ensemble de l'ensemble de certificats ou d'un sous-ensemble de motifs de révocation. La liste CRL est signée au moyen de la clé privée de l'émetteur de liste CRL, les points de répartition de liste CRL ne possédant pas de paire de clés. Toutefois, une liste CRL répartie par le biais de l'annuaire est stockée dans l'entrée du point de répartition de liste CRL, qui peut ne pas être l'entrée d'annuaire de l'émetteur de la liste CRL. Si l'extension de point de répartition émetteur, l'extension de point de répartition émetteur d'autorité d'attribut et le champ domaine d'application de liste CRL sont tous les trois absents, la liste CRL contiendra des éléments pour tous les certificats d'attribut révoqués non caducs en provenance de l'émetteur de la liste CRL. Si le champ point de répartition émetteur d'autorité d'attribut et le champ domaine d'application de liste CRL sont tous deux absents, mais que le champ point de répartition émetteur est présent, le domaine d'application de liste CRL ne comportera pas de certificats d'attribut.

Une fois qu'un certificat est paru dans une liste CRL, il ne figurera plus dans toutes les listes CRL suivantes après son expiration.

Ce champ est défini comme suit:

```
AAissuingDistributionPoint EXTENSION : : = {
        SYNTAX AAIssuingDistPointSyntax
        IDENTIFIED BY id-ce-AAissuingDistributionPoint }

AAIssuingDistPointSyntax ::= SEQUENCE {
        distributionPoint               [0] DistributionPointName OPTIONAL,
        onlySomeReasons                 [1] ReasonFlags OPTIONAL,
        indirectCRL                     [2] BOOLEAN DEFAULT FALSE,
        containsUserAttributeCerts      [3] BOOLEAN DEFAULT TRUE,
        containsAACerts                 [4] BOOLEAN DEFAULT TRUE,
        containsSOAPublicKeyCerts       [5] BOOLEAN DEFAULT TRUE }
```

Le composant **distributionPoint** contient le nom du point de répartition sous une ou plusieurs formes de nom. Si le composant **onlySomeReasons** est présent, la liste CRL contient alors uniquement des révocations de certificats d'attribut pour le ou les motifs indiqués; dans le cas contraire, la liste CRL contient des révocations pour tous les motifs.

Si la valeur du composant **indirectCRL** (*liste CRL indirecte*) est égale à "Vrai", la liste CRL peut alors contenir des notifications de révocations pour des certificats d'attribut provenant d'autorités autres que l'émetteur de la liste CRL. L'autorité particulière responsable pour chaque entrée est indiquée par l'extension d'entrée d'émetteur de liste CRL du certificat dans cette entrée ou conformément aux règles par défaut décrites au § 8.6.2.3. 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 **containsUserAttributeCerts**, **containsAACerts**, **containsSOAPublicKeyCerts** et **onlySomeReasons** en provenance de toutes les autorités qui indiquent cet émetteur de liste CRL dans leurs certificats d'attribut.

Si la valeur du composant **containsUserAttributeCerts** (*contient des certificats d'attribut d'utilisateur*) est égale à "Vrai", la liste CRL contient alors des révocations de certificats d'attribut émis à destination d'entités finales qui ne sont pas elles-mêmes des autorités d'attribut. Si la valeur du composant **containsAACerts** (*contient des certificats d'autorité d'attribut*) est égale à "Vrai", la liste CRL contient alors des révocations de certificats d'attribut émis à destination d'entités qui ne sont pas elles-mêmes des autorités d'attribut.

Si la valeur du composant **containsSOAPublicKeyCerts** (*contient des certificats de clé publique de source d'autorité*) est égale à "Vrai", la liste CRL contient des révocations pour des certificats de clé publique émis à destination d'une entité qui est une source d'autorité à des fins de gestion de privilège (c'est-à-dire des certificats qui contiennent l'extension **SOAIdentifier**). Les règles suivantes s'appliquent pour des listes CRL réparties par le biais de l'annuaire. Si la liste CRL est une liste dCRL, elle sera répartie par le biais de l'attribut **deltaRevocationList** du point de répartition

associé ou, si aucun point de répartition n'est indiqué, par le biais de l'attribut **deltaRevocationList** de l'entrée de l'émetteur de la liste CRL, quels que soient les paramètres des types de certificat auxquels s'applique la liste CRL. Sauf dans le cas où la liste CRL est une liste dCRL:

- Une liste CRL qui ne contient aucune extension **issuingDistributionPoint** dont seul le composant **containsAACerts** ou **containsSOAPublicKeyCerts** est activé sera répartie par le biais de l'attribut **attributeAuthorityRevocationList** du point de répartition associé ou, si aucun point de répartition n'est indiqué, par le biais de l'attribut **attributeAuthorityRevocationList** de l'entrée de l'émetteur de la liste CRL.
- Une liste CRL qui ne contient aucune extension **issuingDistributionPoint** dont le composant **containsUserAttributeCerts** est activé (et dont le composant **containsAACerts** ou **containsSOAPublicKeyCerts** est ou non également activé) sera répartie par le biais de l'attribut **attributeCertificateRevocationList** du point de répartition associé ou, si aucun point de répartition n'est indiqué, par le biais de l'attribut **attributeCertificateRevocationList** de l'entrée de l'émetteur de la liste CRL.
- Une liste CRL qui contient une extension **issuingDistributionPoint** sera répartie comme indiqué au § 8.6.2.2.

Cette extension est toujours critique. Un utilisateur de certificat qui ne comprend pas cette extension ne peut pas faire l'hypothèse que la liste CRL contient une liste complète de certificats révoqués de l'autorité indiquée. Les listes CRL qui ne contiennent pas d'extension critique doivent contenir tous les éléments actuels de liste CRL pour l'autorité émettrice, y compris les éléments pour tous les certificats d'utilisateur et certificats d'autorité révoqués.

NOTE 1 – Les moyens utilisés par les autorités pour communiquer les informations de révocation aux émetteurs de liste CRL ne sont pas abordés dans la présente spécification d'annuaire.

NOTE 2 – Si une autorité publie une liste CRL dont le composant **containsAACerts** est mis à la valeur "Vrai" et dont le composant **containsUserAttributeCerts** n'est pas mis à la valeur "Vrai", elle doit alors s'assurer que tous les certificats d'autorité d'attribut visés par cette liste CRL contiennent l'extension **basicAttConstraints**.

NOTE 3 – Si une autorité publie une liste CRL dont le composant **containsSOAPublicKeyCerts** est mis à la valeur "Vrai", elle doit alors s'assurer que tous les certificats de source d'autorité visés par cette liste CRL contiennent l'extension **SOAIdentifier**.

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, protocole Internet et réseaux de nouvelle génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2005