UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T Q.817

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(01/2001)

SÉRIE Q: COMMUTATION ET SIGNALISATION

Interface Q3

Infrastructure des clés publiques du RGT – Profils des certificats numériques et des listes de révocation des certificats

Recommandation UIT-T Q.817

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE Q

COMMUTATION ET SIGNALISATION

SIGNALISATION DANS LE SERVICE MANUEL INTERNATIONAL	Q.1–Q.3
EXPLOITATION INTERNATIONALE AUTOMATIQUE ET SEMI-AUTOMATIQUE	Q.4–Q.59
FONCTIONS ET FLUX D'INFORMATION DES SERVICES DU RNIS	Q.60–Q.99
CLAUSES APPLICABLES AUX SYSTÈMES NORMALISÉS DE L'UIT-T	Q.100–Q.119
SPÉCIFICATIONS DES SYSTÈMES DE SIGNALISATION N° 4 ET N° 5	Q.120–Q.249
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION N° 6	Q.250–Q.309
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION R1	Q.310–Q.399
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION R2	Q.400–Q.499
COMMUTATEURS NUMÉRIQUES	Q.500–Q.599
INTERFONCTIONNEMENT DES SYSTÈMES DE SIGNALISATION	Q.600–Q.699
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION N° 7	Q.700–Q.799
INTERFACE Q3	**Q.800–Q.849**
SYSTÈME DE SIGNALISATION D'ABONNÉ NUMÉRIQUE N° 1	Q.850–Q.999
RÉSEAUX MOBILES TERRESTRES PUBLICS	Q.1000–Q.1099
INTERFONCTIONNEMENT AVEC LES SYSTÈMES MOBILES À SATELLITES	Q.1100–Q.1199
RÉSEAU INTELLIGENT	Q.1200–Q.1699
PRESCRIPTIONS ET PROTOCOLES DE SIGNALISATION POUR LES IMT-2000	Q.1700–Q.1799
RNIS À LARGE BANDE	Q.2000–Q.2999

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

Recommandation UIT-T Q.817

Infrastructure des clés publiques du RGT – Profils des certificats numériques et des listes de révocation des certificats

Résumé

La présente Recommandation expose la manière dont les certificats numériques d'infrastructure et les listes de révocation de ces certificats peuvent être utilisés dans le RGT et définit les conditions d'utilisation de ces extensions des certificats et listes.

Source

La Recommandation Q.817 de l'UIT-T, élaborée par la Commission d'études 4 (2001-2004) de l'UIT-T, a été approuvée le 19 janvier 2001 selon la procédure définie dans la Résolution 1 de l'AMNT.

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

Recommandation UIT-T Q.817

Infrastructure des clés publiques du RGT – Profils des certificats numériques et des listes de révocation des certificats

1 Domaine, objet et application

1.1 Domaine

La présente Recommandation est destinée à faciliter l'interopérabilité entre éléments RGT utilisant l'infrastructure de clé publique (PKI, *public key infrastructure*) dans le cadre des fonctions de sécurité. Elle concerne toutes les interfaces et applications du RGT. Elle est indépendante de la pile de protocoles de communication ou du protocole de gestion de réseau utilisé. Les ressources de l'infrastructure PKI peuvent être utilisées dans une grande étendue de fonctions de sécurité comme l'authentification, l'intégrité, la non-répudiation et l'échange de clés (UIT-T M.3016). La présente Recommandation ne spécifie cependant pas la façon dont il convient d'implémenter de telles fonctions, avec ou sans infrastructure PKI.

L'infrastructure PKI s'est révélée être une méthode efficace et modulable pour l'authentification sûre, pour la non-répudiation et pour la distribution ou la gestion des clés de chiffrement ainsi que d'autres paramètres associés à la sécurité. Une infrastructure PKI est fondée sur des certificats numériques. L'UIT-T X.509 spécifie le format de ces certificats. Les certificats numériques X.509 peuvent contenir un nombre quelconque d'extensions. Pour qu'une infrastructure PKI assure l'interopérabilité entre éléments RGT, tous ces éléments doivent avoir la capacité de traiter le même ensemble d'extensions de certificat. Théoriquement, tous les éléments RGT devraient également manifester le même comportement lors du traitement des extensions de certificat. Afin de faciliter l'interopérabilité sûre entre éléments RGT, la présente Recommandation spécifie les extensions de certificat qui doivent être prises en charge par une infrastructure PKI de RGT. Elle indique également les comportements par défaut pour le traitement de ces extensions.

En vue de faciliter l'harmonisation avec d'autres industries, la présente Recommandation est fondée sur la série des Recommandations UIT-T X.500 et en particulier sur l'UIT-T X.509, et sur la demande de commentaires 2459 concernant l'infrastructure PKI, émise par le Groupe de travail sur l'ingénierie Internet (IETF, *Internet engineering task force*).

1.2 Objet

L'objet de la présente Recommandation est d'offrir un mécanisme interopérable et modulable pour la distribution et la gestion de clés à l'intérieur d'un RGT, de part et d'autre de toutes les interfaces, ainsi que pour la prise en charge d'un service de non-répudiation à travers l'interface X.

1.3 Application

La présente Recommandation s'applique à toutes les interfaces Q et X du RGT, quel que soit le protocole de communication. Elle vise les informations relatives aux clés publiques et à leur révocation, utilisées ou échangées par des éléments du RGT.

Selon les besoins spécifiques de l'application, le RGT peut utiliser, à la place de certificats, des clés publiques prédéfinies qui sont distribuées par des moyens qui ne relèvent pas du domaine de la présente Recommandation.

2 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée.

2.1 Normes UIT-T et ISO/CEI

– UIT-T M.3016 (1998), *Aperçu général de la sécurité du RGT*.

– UIT-T Q.812 (1997), *Profils des protocoles des couches supérieures pour les interfaces Q3 et X.*

– UIT-T X.500 (2001) | ISO/CEI 9594-1:2001, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: aperçu général des concepts, modèles et services.*

– UIT-T X.509 (2000) | ISO/CEI 9594-8:2001, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut.*

– UIT-T X.680 (1997) | ISO/CEI 8824-1:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification de la notation de base.*

– UIT-T X.681 (1997) | ISO/CEI 8824-2:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des objets informationnels.*

– UIT-T X.682 (1997) | ISO/CEI 8824-3:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des contraintes.*

– UIT-T X.683 (1997) | ISO/CEI 8824-4:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: paramétrage des spécifications de la notation de syntaxe abstraite numéro un.*

– UIT-T X.690 (1997) | ISO/CEI 8825-1:1998, *Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage de base, des règles de codage canoniques et des règles de codage distinctives.*

– UIT-T X.736 (1992) | ISO/CEI 10164-7:1992, *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: fonction de signalisation des alarmes de sécurité.*

– UIT-T X.740 (1992) | ISO/CEI 10164-8:1993, *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: fonction de piste de vérification de sécurité.*

2.2 Autres normes

– IETF RFC 2459 (1999), *Internet X.509 Public Key Infrastructure – Certificate and CRL Profile* (certificat Internet d'infrastructure de clé publique X.509 et profil de liste CRL).

– IETF RFC 2251 (1997), *Lightweight Directory Access Protocol (v3)* (protocole allégé d'accès à l'Annuaire).

3 Définitions

La présente Recommandation utilise les définitions des services et mécanismes de sécurité figurant dans l'UIT-T M.3016. Elle utilise également les définitions d'éléments d'infrastructure de clé publique qui sont spécifiées dans la demande RFC 2459.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

ASN.1 notation de syntaxe abstraite numéro un (*abstract syntax notation one*)

BER règles de codage de base (*basic encoding rules*)

CA autorité de certification (*certification authority*)

CRL liste de révocation de certificats (*certificate revocation list*)

DER règles de codage distinctives (*distinguished encoding rules*)

IETF Groupe de travail d'ingénierie Internet (*Internet engineering task force*)

OID identificateur d'objet (*object identifier*)

PKCS norme cryptographique de clé publique (*public key cryptography standard*)

PKI infrastructure de clé publique (*public key infrastructure*)

RA organisme d'enregistrement (*registration authority*)

RFC demande de commentaires (*request for comments*)

RSA Rivest Shamir Adelman

UIT-T Union internationale des télécommunications – Secteur de la normalisation des télécommunications

5 Aperçu général

L'**infrastructure des clés publiques (PKI)** apparaît comme la solution modulable la plus économique pour assurer la sécurité dans un RGT. La présente Recommandation vise à faciliter l'interopérabilité entre composants d'infrastructure PKI issus de différents fournisseurs de produits et de services. Elle vise également à assurer l'interopérabilité entre différentes compagnies ou administrations. Le présent paragraphe donne un aperçu général de haut niveau sur l'infrastructure PKI du RGT.

L'infrastructure PKI du RGT est constituée des **composants** suivants:

Une **autorité de certification (CA)** produit des **certificats de clés publiques** pour toutes les entités du RGT qui ont besoin de sécuriser leurs communications, ainsi que pour d'éventuelles entités externes qui ont besoin de sécuriser leurs communications avec des entités du RGT. Une autorité de certification émet également des certificats à l'intention de ses homologues situés à l'extérieur du RGT, ainsi que des **listes de révocation de certificats (CRL)** si nécessaire. Une liste CRL contient les numéros de série des certificats qui ont été révoqués (par exemple parce que la clé a été compromise ou parce que le sujet ne fait plus partie du personnel) et dont la période de validité n'a pas encore expiré. L'autorité de certification emploie normalement un ordinateur inviolable placé au niveau de sécurité le plus élevé[1]. Le terme autorité de certification est également utilisé pour

[1] Les exigences de sécurité physique et logicielle d'un ordinateur inviolable sont hors du domaine d'application de la présente Recommandation.

désigner une organisation (plutôt qu'un dispositif) qui offre un service, habituellement payant, d'émission de certificats.

Le format le plus courant d'un certificat est défini dans l'UIT-T X.509, qui définit plusieurs champs obligatoires et qui prévoit l'adjonction d'un nombre quelconque d'**extensions**. Chaque extension est marquée comme étant critique ou non critique. Si une entité traitant un certificat rencontre une extension non critique et ne la reconnaît pas, elle peut l'ignorer. Si une entité traitant un certificat rencontre une extension critique et ne la reconnaît pas, elle doit rejeter le certificat. L'UIT-T X.509 permet également d'apporter des extensions à des listes CRL et à des entrées individuelles de ces listes. L'interopérabilité dans un RGT ou entre plusieurs RGT exige au moins un accord complet sur toutes les extensions critiques éventuellement contenues dans des certificats utilisés pour des applications RGT.

Un **organisme d'enregistrement (RA)** vérifie l'authenticité de chaque entité (NE, OS, WS, employé, client, fournisseur, …) devant recevoir un certificat de clé publique issu de l'organisme de certification du RGT. L'organisme d'enregistrement se compose normalement d'un petit nombre d'administrateurs de sécurité ayant accès à l'organisme de certification.

Un organisme d'enregistrement publie généralement une **déclaration de politique de certification (CPS, *certification policy statement*)** qui spécifie les conditions dans lesquelles (par exemple contrôle d'identité) il émettra un certificat.

L'infrastructure PKI comporte un **annuaire** pour la mémorisation et la diffusion des certificats et des listes CRL. L'UIT-T X.500 offre la base de l'annuaire. L'UIT-T Q.812 contient un profil d'utilisation du protocole d'accès à l'annuaire (DAP, *directory access protocol*) X.500. Les annuaires fondés sur le profil PKI de l'IETF pour le protocole DAP allégé, sous-ensemble du protocole DAP (LDAPv3, *lightweight DAP*) peuvent cependant être plus facilement accessibles que les annuaires fondés sur l'UIT-T X.500.

Chaque **entité RGT** aura besoin d'interagir avec l'annuaire d'infrastructure PKI du RGT afin d'extraire et de recevoir les certificats d'autres entités ainsi que les listes CRL correspondantes. Elle aura besoin de pouvoir traiter ces certificats et ces listes CRL. Chaque entité RGT devra aussi pouvoir construire et traiter des itinéraires de certification.

Les composants d'infrastructure PKI du RGT doivent pouvoir interagir au moyen de **protocoles** normalisés. Les interactions entre composants PKI du RGT sont illustrés dans la Figure 1.

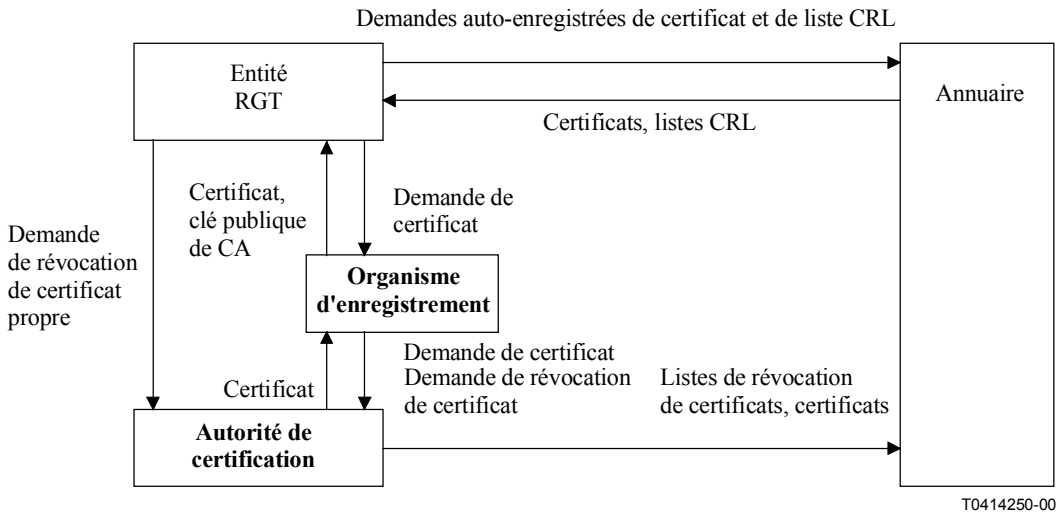

Figure 1/Q.817 – Interactions entre composants d'infrastructure PKI de RGT

6 Extensions de certificat

L'infrastructure PKI du groupe IETF utilise les **certificats** définis dans l'UIT-T X.509. Ce format permet un nombre quelconque d'extensions. L'infrastructure PKI de l'IETF comporte de nombreuses extensions, qui sont énumérées ci-dessous. (Les extensions sont définies dans la demande RFC 2459 de l'IETF, à laquelle la présente Recommandation fait référence pour sa partie normative.)

La présente Recommandation offre un profil RFC 2459 propre au RGT sans répéter le texte de ce commentaire RFC.

Elle donne les directives par défaut suivantes pour le traitement des extensions de certificat. Chaque administration peut choisir des comportements différents, selon sa politique de sécurité:

- si une extension non critique, qui doit être présente, est absente ou a une valeur non valide, le certificat correspondant doit être accepté et traité. En même temps, l'événement doit être enregistré dans un journal d'audit de sécurité et une alarme de sécurité doit être émise. L'enregistrement du journal d'audit ainsi que l'alarme de sécurité doivent contenir une copie du certificat, une copie du message contenant le certificat, l'heure à laquelle le certificat a été reçu et l'indication de l'entité qui a détecté la divergence;
- si une extension non critique est présente alors qu'elle ne devrait pas l'être, le certificat doit être accepté et traité. En même temps, l'événement doit être enregistré dans un journal d'audit de sécurité et une alarme de sécurité de bas niveau doit être émise. L'enregistrement du journal d'audit ainsi que l'alarme de sécurité doivent contenir une copie du certificat, une copie du message contenant le certificat, l'heure à laquelle le certificat a été reçu et l'indication de l'entité qui a détecté la divergence;
- si une entité finale ne reconnaît pas une extension critique, elle ne doit pas donner suite au traitement du certificat. En même temps, l'événement doit être enregistré dans un journal d'audit de sécurité et une alarme de sécurité doit être émise. L'enregistrement du journal d'audit ainsi que l'alarme de sécurité doivent contenir une copie du certificat, une copie du message contenant le certificat, l'heure à laquelle le certificat a été reçu et l'indication de l'entité qui a détecté la divergence. Cette entité doit répondre à l'entité émettrice du certificat (explicitement ou implicitement par référence) au moyen d'un message indiquant que le certificat contient une extension critique non reconnue;
- si une entité finale rencontre une valeur non valide dans une extension critique, elle ne doit pas donner suite au traitement du certificat. En même temps, l'événement doit être enregistré dans un journal d'audit de sécurité et une alarme de sécurité doit être émise. L'enregistrement du journal d'audit ainsi que l'alarme de sécurité doivent contenir une copie du certificat, une copie du message contenant le certificat, l'heure à laquelle le certificat a été reçu et l'indication de l'entité qui a détecté la divergence. Cette entité ne doit pas répondre à l'entité émettrice du certificat (explicitement ou implicitement par référence).

Sauf indication contraire, ces extensions peuvent être utilisées dans les certificats de l'organisme de certification comme dans les certificats de l'entité finale.

6.1 Identificateur de clé d'organisme

Cette extension est définie et prescrite par l'UIT-T X.509.

Elle est prescrite par la demande RFC 2459 et par la présente Recommandation dans tous les certificats conformes, mais elle peut être omise dans un certificat signé par l'organisme de certification.

Cette extension n'est jamais critique.

L'identificateur de clé doit être la représentation, en chaîne binaire (BIT STRING) de 160 bits hachée par SHA-1, de la clé publique (à l'exclusion de l'étiquette, de la longueur et du nombre de bits inutilisés). La demande RFC 2459 indique la construction de cette chaîne binaire pour divers types de clé publique.

6.2 Identificateur de clé du sujet

Cette extension est définie et prescrite par l'UIT-T X.509.

Cette extension est prescrite par la demande RFC 2459 et par la présente Recommandation dans tous les certificats conformes.

Elle est facultative pour les certificats d'entité finale dont l'interaction s'effectue par l'interface X.

Elle ne doit pas être utilisée pour les certificats d'entité finale dont l'interaction ne s'effectue que par des interfaces Q.

Cette extension n'est jamais critique.

L'identificateur de clé doit être la représentation, en chaîne binaire (BIT STRING) de 160 bits hachée par SHA-1, de la clé publique (à l'exclusion de l'étiquette, de la longueur et du nombre de bits inutilisés). La demande RFC 2459 indique la construction de cette chaîne binaire pour divers types de clé publique.

6.3 Usage de clé

Cette extension est définie et prescrite par l'UIT-T X.509.

Elle est facultative pour les certificats d'entité finale dont l'interaction s'effectue par l'interface X.

Elle ne doit pas être utilisée pour les certificats d'entité finale dont l'interaction ne s'effectue que par des interfaces Q.

Si elle est présente, cette extension est critique.

6.4 Période d'usage de clé privée

Cette extension est définie et prescrite par l'UIT-T X.509.

Elle n'est pas recommandée dans la demande RFC 2459.

Elle est facultative dans la présente Recommandation et doit être marquée comme étant non critique si elle est présente.

6.5 Politiques de certificat

Dans les certificats à utiliser de part et d'autre de l'interface Q, cette extension est facultative et son usage n'est pas recommandé: elle doit être alors être marquée comme étant non critique.

Dans les certificats à utiliser de part et d'autre de l'interface X, cette extension est facultative et son usage est recommandé: elle doit alors être marquée comme étant critique.

Cette extension n'est pas nécessaire pour les entités qui n'interagissent que par l'interface Q. L'organisme d'enregistrement peut décider de différentes politiques de certification pour différents éléments RGT, en imposant des politiques plus strictes aux éléments possédant des privilèges d'accès plus étendus. La fonction de contrôle d'accès aux ressources du RGT ne sera alors fondée que sur l'identité authentifiée de l'initiateur et sur les privilèges d'accès de cet initiateur, et non pas sur la politique de certification relative au certificat de l'initiateur.

Cette extension est utile pour les entités qui interagissent par l'interface X. Toutes ces entités devraient donc être en mesure de traiter cette extension, dont l'inclusion est recommandée pour les certificats émis vers des entités censées interagir par l'interface X.

Si cette extension est présente, elle doit se composer d'un seul identificateur OID.

6.6 Mappage de politique

La demande RFC 2459 spécifie que cette extension n'est jamais critique et qu'elle ne peut être présente que dans des certificats d'autorité de certification.

Cette extension n'est pas requise pour les certificats d'autorité de certification du RGT si ces certificats ne sont émis qu'à l'intérieur de ce RGT (c'est-à-dire pour des interactions par interface Q). Les entités finales qui n'interagissent que par interfaces Q ne sont pas tenues de traiter cette extension.

Celle-ci peut être présente dans des certificats CA utilisés pour des interactions par interface X.

6.7 Autre nom du sujet

Cette extension n'est pas requise pour les interactions RGT par l'interface Q. Si elle est présente, elle doit être marquée comme étant non critique (c'est-à-dire que le nom distinctif du sujet doit être présent). Les entités finales qui n'interagissent que par interfaces Q ne sont pas tenues de traiter cette extension.

Cette extension peut être utile pour certaines interactions par l'interface X, auxquels cas son usage doit être comme spécifié dans la demande RFC 2459.

6.8 Autre nom de l'émetteur

Les entités du RGT ne sont pas tenues de traiter cette extension. Si celle-ci est présente, elle doit être marquée comme étant non critique.

6.9 Attributs d'annuaire du sujet

Cette extension n'est pas recommandée pour les applications du RGT. Son usage est facultatif.

Si elle est présente, cette extension doit être marquée comme étant non critique.

6.10 Contraintes de base

Cette extension doit être présente dans tous les certificats d'organisme de certification et doit être marquée comme étant critique.

Elle ne doit être présente dans aucun certificat d'entité finale.

6.11 Contraintes de nom

Cette extension peut être présente dans un certificat d'organisme de certification et doit être marquée comme étant critique.

Elle ne doit être présente dans aucun certificat d'entité finale.

6.12 Contraintes de politique

Cette extension est facultative. Elle peut être marquée comme étant critique ou non critique.

Si le certificat est émis par un organisme de certification à l'intention d'une autre autorité de certification située dans le même domaine de sécurité, on recommande d'indiquer que cette extension n'est pas critique. Dans ce cas, on n'exige pas des éléments de réseaux qu'ils traitent cette extension.

Si le certificat est émis par une seule autorité de certification à l'intention d'une autre autorité de certification située dans un autre domaine de sécurité ou dans une autre administration, cette extension doit alors être marquée comme étant critique. Différentes administrations sont toujours

situées dans différents domaines de sécurité: les passerelles prenant en charge des interfaces X sont donc tenues de traiter cette extension.

6.13 Usage étendu de clé

Cette extension ne doit pas être utilisée pour les applications du RGT. Une entité RGT prenant en charge l'interaction par interface X peut cependant rencontrer ce champ dans des certificats émis par un organisme de certification externe.

Cette extension ne doit pas être utilisée dans les certificats à utiliser pour des applications par interface Q.

Elle est facultative dans les certificats à utiliser pour les applications par interface X.

Si cette extension est présente, elle doit être marquée comme étant critique.

6.14 Points de distribution de liste CRL

Cette extension est recommandée pour les certificats utilisés de part et d'autre de l'interface X. Elle est facultative pour les certificats utilisés dans les transactions par interface Q.

NOTE – Des contributions sont sollicitées au sujet de la criticité de cette extension.

6.15 Accès aux informations d'organisme

Cette extension ne doit pas être utilisée dans les certificats destinés à être utilisés de part et d'autre d'une interface Q. Elle peut être utilisée dans les certificats destinés à être utilisés de part et d'autre d'une interface X. Si elle est présente, cette extension doit être marquée comme étant non critique.

7 Extensions de liste de révocation de certificats (CRL)

L'infrastructure PKI du groupe IETF utilise les listes **CRL** qui sont définies dans la version de 1993 de l'UIT-T X.509. Elle spécifie également plusieurs extensions de la liste CRL de base (qui sont définies dans la demande RFC 2459).

7.1 Identificateur de clé d'organisme

Cette extension doit être présente et être marquée comme étant non critique.

7.2 Autre nom de l'émetteur

Cette extension ne doit pas être utilisée pour les transactions RGT par interface Q. Elle peut être présente dans les certificats utilisés de part et d'autre d'une interface X. Si elle est présente, elle doit être marquée comme étant non critique.

7.3 Numéro de liste CRL

Cette extension doit être présente et être marquée comme étant non critique.

7.4 Indicateur de liste CRL delta

Cette extension est facultative pour les listes CRL qui prennent en charge les transactions par interface Q. Elle n'est pas requise si l'administrateur du RGT décide de ne pas émettre de listes CRL delta. L'usage de cette extension offre à l'administrateur du RGT plus de flexibilité pour distribuer les informations relatives aux listes CRL. Cette extension peut être présente dans les listes CRL externes. Si elle est présente, cette extension doit être marquée comme étant critique.

7.5 Point de distribution à l'émission

Cette extension est facultative. Le champ facultatif (OPTIONAL) "onlySomeReasons" ne doit pas être utilisé dans les applications du RGT.

Cette extension peut être présente dans des listes CRL externes. Si elle est présente, cette extension doit être marquée comme étant critique.

8 Extensions pour entrées individuelles de liste CRL

L'infrastructure PKI du groupe IETF énumère plusieurs extensions pour **entrées individuelles de liste CRL**. (Ces extensions sont définies dans la demande RFC 2459.)

8.1 Code de cause

Cette extension est facultative. Si elle est présente, elle doit être marquée comme étant non critique.

8.2 Code d'instruction de mise en attente

Cette extension est facultative. Elle n'est pas requise dans les listes CRL qui prennent en charge les transactions par interface Q. Elle peut être présente dans des listes CRL externes. Si elle est présente, elle doit être marquée comme étant non critique.

8.3 Date de non validité

Cette extension est facultative. Elle n'est pas requise dans les listes CRL qui prennent en charge les transactions par interface Q. Elle peut être présente dans des listes CRL externes. Si elle est présente, elle doit être marquée comme étant non critique.

8.4 Emetteur de certificat

Cette extension ne doit pas être utilisée dans les listes CRL qui prennent en charge les transactions par interface Q. Elle peut être présente dans des listes CRL externes. Si elle est présente, elle doit être marquée comme étant critique.

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	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, de télégraphie, de télécopie, circuits téléphoniques 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 informatiques généraux des systèmes de télécommunication

Genève, 2001