



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.509

Corrigendum 1

(03/2000)

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 1

Recommandation UIT-T X.509 – Corrigendum 1

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

RÉSEAUX PUBLICS DE DONNÉES	
Services et fonctionnalités	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalisation et commutation	X.50–X.89
Aspects réseau	X.90–X.149
Maintenance	X.150–X.179
Dispositions administratives	X.180–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	
Modèle et notation	X.200–X.209
Définitions des services	X.210–X.219
Spécifications des protocoles en mode connexion	X.220–X.229
Spécifications des protocoles en mode sans connexion	X.230–X.239
Formulaires PICS	X.240–X.259
Identification des protocoles	X.260–X.269
Protocoles de sécurité	X.270–X.279
Objets gérés des couches	X.280–X.289
Tests de conformité	X.290–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Généralités	X.300–X.349
Systèmes de transmission de données par satellite	X.350–X.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 9594-8

RECOMMANDATION UIT-T X.509

**TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES
OUVERTS – L'ANNUAIRE: CADRE D'AUTHENTIFICATION**

CORRIGENDUM TECHNIQUE 1

Source

Le Corrigendum 1 de la Recommandation X.509 de l'UIT-T a été approuvé le 31 mars 2000. Un texte identique est publié comme Corrigendum technique 1 de la Norme 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.

La Conférence mondiale de normalisation des télécommunications (CMNT), qui se réunit tous les quatre ans, détermine les thèmes d'études 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 n° 1 de la CMNT.

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.

© UIT 2000

Droits de reproduction réservés. Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'UIT.

TABLE DES MATIÈRES

		<i>Page</i>
1)	Résolution du compte rendu de faute 9594/200.....	1
	Paragraphe 12.6.2	1
2)	Résolution du compte rendu de faute 9594/201.....	1
	Paragraphe 12.6.3.1	1
3)	Résolution du compte rendu de faute 9594/212.....	1
	Paragraphe 12.7.6	1
4)	Résolution du compte rendu de faute 9594/213.....	1
	Paragraphe 12.7.6 d).....	1
5)	Résolution du compte rendu de faute 9594/218.....	2
	Paragraphe 12.7.2 j).....	2
6)	Résolution du compte rendu de faute 9594/220.....	2
	Paragraphe 11.2, Note 3.....	2
7)	Résolution du compte rendu de faute 9594/185.....	2
	Paragraphe 8	2
8)	Résolution du compte rendu de faute 9594/204.....	3
	Paragraphe 12.6.3.1	3
9)	Résolution du compte rendu de faute 9594/222.....	3

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES
OUVERTS – L'ANNUAIRE: CADRE D'AUTHENTIFICATION

CORRIGENDUM TECHNIQUE 1

1) Résolution du compte rendu de faute 9594/200

Paragraphe 12.6.2

Ajouter le texte suivant à la fin du paragraphe débutant par "Si cette extension est étiquetée critique...":

"Lorsque les points de répartition sont utilisés pour distribuer des informations de liste CRL pour tous les codes motif de révocation et si tous les certificats émis par l'autorité de certification contiennent le champ **crlDistributionPoint** (point de répartition de liste CRL) comme extension critique, l'autorité de certification n'a pas l'obligation de publier également une liste CRL complète dans l'entrée de l'autorité de certification."

2) Résolution du compte rendu de faute 9594/201

Paragraphe 12.6.3.1

Déplacer la deuxième phrase du deuxième paragraphe "Si ce champ est absent ... la liste CRL" dans le premier paragraphe immédiatement après la phrase "Ce champ est défini comme suit:"

Ajouter une marque de paragraphe à la fin de la phrase déplacée, de manière à créer un paragraphe indépendant contenant "Ce champ est défini comme suit:" immédiatement avant la définition ASN.1.

3) Résolution du compte rendu de faute 9594/212

Paragraphe 12.7.6

Ajouter le texte suivant à la fin du paragraphe 12.7.6:

- "g) la composante **authorityKeyIdentifier** (identificateur de clé d'autorité) est en concordance si la valeur de cette composante dans la valeur de l'attribut stocké est égale à celle figurant dans la valeur présentée; il n'y a pas de concordance si la valeur de l'attribut stocké ne contient pas d'extension d'identificateur de clé d'autorité ou si les composantes dans la valeur présentée ne figurent pas toutes dans la valeur de l'attribut stocké."

4) Résolution du compte rendu de faute 9594/213

Paragraphe 12.7.6 d)

Remplacer l'alinéa 12.7.6 d) par le texte suivant:

- "d) la composante **reasonFlags** (fanions de motif) est en concordance si chacun des bits positionnés dans la valeur présentée est également positionné dans les composantes **onlySomeReasons** (uniquement certains motifs) de l'extension de point de répartition émetteur de la valeur de l'attribut stocké; il y a

également concordance si la valeur de l'attribut stocké contient les fanions **reasonFlags** dans l'extension de point de répartition émetteur ou si la valeur de l'attribut stocké ne contient pas d'extension de point de répartition émetteur;

NOTE – Même si une liste CRL correspond à une valeur particulière de fanion **reasonFlags**, il se peut que la liste CRL ne contienne pas de notification de révocation avec ce code motif."

5) Résolution du compte rendu de faute 9594/218

Paragraphe 12.7.2 j)

Remplacer l'alinéa 12.7.2 j) par le texte suivant:

"j) la composante **policy** (politique) est en concordance si au moins l'un des membres de l'ensemble **CertPolicySet** (ensemble de politiques de certificat) présenté figure dans l'extension de politiques de certificat dans la valeur de l'attribut stocké; il n'y a pas concordance s'il n'existe pas d'extension de politiques de certificat normalisée dans la valeur de l'attribut stocké;"

6) Résolution du compte rendu de faute 9594/220

Paragraphe 11.2, Note 3

Dans la deuxième phrase de la Note 3, remplacer "sera absent" par "peut être absent".

*Dans le début de la troisième phrase de la Note 3, remplacer le texte "Ceci permettra" par "Si la composante **version** est absente, ceci peut permettre".*

*Dans le début de la quatrième phrase de la Note 3, remplacer le texte "Une implémentation prenant en charge les listes CRL de version 2 (ou plus) peut" par "En l'absence de la composante **version**, une implémentation prenant en charge les listes CRL de version 2 (ou plus) peut également..."*

7) Résolution du compte rendu de faute 9594/185

Paragraphe 8

*Ajouter le texte suivant immédiatement après la définition ASN.1 de **certificatePair**:*

"L'attribut **cACertificate** (certificat d'autorité de certification) de l'entrée d'annuaire d'une autorité d'attribut sera utilisé pour stocker des certificats auto-émis (s'il en existe) et des certificats émis pour cette autorité de certification par d'autres autorités de certification appartenant au même domaine que la première.

Les éléments **forward** (aller) de l'attribut **crossCertificatePair** (paire de certificats croisés) d'une entrée d'annuaire d'autorité de certification seront utilisés pour stocker tous les certificats émis par cette autorité, à l'exception des certificats auto-émis pour cette dernière. Les éléments **reverse** de l'attribut **crossCertificatePair** d'une entrée d'annuaire d'autorité de certification peuvent contenir de manière optionnelle un sous-ensemble des certificats émis par cette dernière pour d'autres autorités de certification. Lorsque les éléments **forward** et **reverse** sont présents simultanément dans une même valeur d'attribut, le nom de l'émetteur de l'un des certificats doit alors correspondre au nom du sujet de l'autre et réciproquement; la clé publique du sujet de l'un des certificats permettra de vérifier la signature numérique de l'autre et réciproquement.

Lorsqu'un élément **reverse** est présent, les valeurs des éléments **forward** et **reverse** ne sont pas nécessairement stockées dans la même valeur d'attribut; elles peuvent être stockées, soit dans une seule valeur d'attribut, soit dans deux valeurs d'attribut.

Dans le cas de certificats de version 3, aucun de ces derniers ne contiendra une extension **basicConstraints** avec une valeur de composante **ca** positionnée sur **FALSE**.

La définition du domaine est uniquement un problème de politique locale."

Remplacer la Figure 4 par la figure suivante:

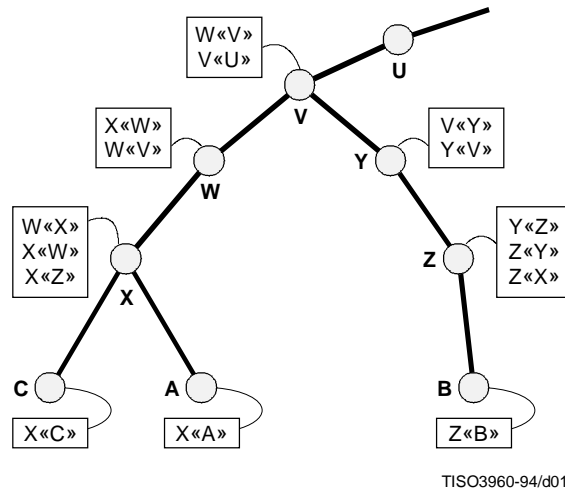


Figure 4 – Exemple fictif de chemin de certification

8) Résolution du compte rendu de faute 9594/204

Paragraphe 12.6.3.1

Supprimer "annulés mais" dans la deuxième phrase suivant la définition ASN.1.

Ajouter la deuxième phrase suivante dans le deuxième paragraphe suivant la définition ASN.1:

"Une fois qu'un certificat figure dans une liste CRL, il peut être supprimé dans toute liste CRL suivante après l'expiration du certificat."

9) Résolution du compte rendu de faute 9594/222

Ajouter le texte suivant au paragraphe 12.1:

"Politique de certificat

Ce cadre contient trois types d'entités: l'utilisateur de certificat, l'autorité de certification et le sujet du certificat (ou entité finale). Chacune d'elles intervient dans le cadre d'obligations imposées par les deux autres et bénéficie en retour des garanties limitées qu'elles offrent. Ces obligations et garanties sont définies dans une politique de certificat. Une politique de certificat est un document (rédigé généralement dans un langage naturel). Elle peut faire l'objet d'une référence au moyen d'un identificateur non ambigu, qui peut figurer dans l'extension de politiques de certificat du certificat émis vers l'entité finale par l'autorité de certification, et auquel l'utilisateur de certificat fait confiance. Un certificat peut être émis dans le cadre d'une ou plusieurs politiques. La définition de la politique et l'attribution de l'identificateur sont faites par une autorité de politique. L'ensemble des politiques administrées par une autorité de politique est appelé "domaine de politique". Tous les certificats sont émis conformément à une politique, même si cette dernière ne figure pas dans le certificat ou n'est pas référencée par ce dernier. La Recommandation | Norme internationale ne prescrit ni le style ni le contenu de la politique de certificat.

L'utilisateur de certificat peut être lié à ses obligations résultant de la politique de certificat par le fait d'importer une clé publique d'autorité et de l'utiliser comme ancre de confiance, ou en faisant confiance à un certificat qui contient l'identificateur de politique associé. L'autorité de certification peut être liée à *ses propres* obligations résultant de la

politique par le fait d'émettre un certificat qui contient l'identificateur de politique associé. L'entité finale peut être liée à *ses propres* obligations résultant de la politique par le fait de demander et d'accepter un certificat qui contient l'identificateur de politique associé et par l'utilisation de la clé privée correspondante. Les implémentations qui n'utilisent pas l'extension de politiques de certificat doivent établir les liaisons correspondantes par d'autres moyens.

Le fait qu'une entité déclare simplement la conformité à une politique ne satisfait pas en général les besoins de garanties des autres entités appartenant au cadre. Ces dernières ont besoin d'une raison pour admettre que les autres participants utilisent une implémentation fiable de la politique. Toutefois, si cela est énoncé explicitement dans la politique, les utilisateurs de certificat peuvent accepter les garanties de l'autorité de certification indiquant que ses entités finales sont d'accord pour être liées par leurs obligations résultant de la politique, ce qui évite d'effectuer une confirmation directe avec ces entités finales. Cette caractéristique de la politique de certificat est en dehors du domaine d'application de la Recommandation | Norme internationale.

Une autorité de certification peut imposer des limitations à l'utilisation de ses certificats afin de rester maîtresse des risques qu'elle assume par l'émission de certificats. Elle peut, par exemple, restreindre la communauté des utilisateurs de certificat, les buts pour lesquels ces derniers utilisent les certificats ou le type de dommages qu'elle est prête à assumer en cas d'une défaillance de sa part ou de ses entités finales. Ces points doivent être définis dans la politique de certificat.

D'autres informations peuvent figurer dans l'extension de politiques de certificat sous la forme de qualificatifs de politique afin d'aider les entités impliquées à comprendre les dispositions de la politique.

Certification croisée

Une autorité de certification peut être le sujet d'un certificat émis par une autre autorité de certification. Le certificat est appelé dans ce cas un certificat croisé, l'autorité de certification constituant le sujet du certificat est appelée autorité de certification sujette et l'autorité de certification qui émet le certificat croisé, autorité de certification intermédiaire (voir Figure 1). Le certificat croisé et le certificat de l'entité finale peuvent contenir tous deux une extension de politiques de certificat.

Les garanties et les obligations partagées par l'autorité de certification sujette, l'autorité de certification intermédiaire et l'utilisateur de certificat sont définies par la politique de certificat identifiée dans le certificat croisé, en accord avec lequel l'autorité de certification sujette peut agir comme ou pour le compte d'une entité finale. Les garanties et obligations partagées par le sujet du certificat, l'autorité de certification sujette et l'autorité de certification intermédiaire sont définies par la politique de certificat identifiée dans le certificat de l'entité finale, en accord avec lequel l'autorité de certification intermédiaire peut agir comme un utilisateur de certificat ou pour le compte de ce dernier.

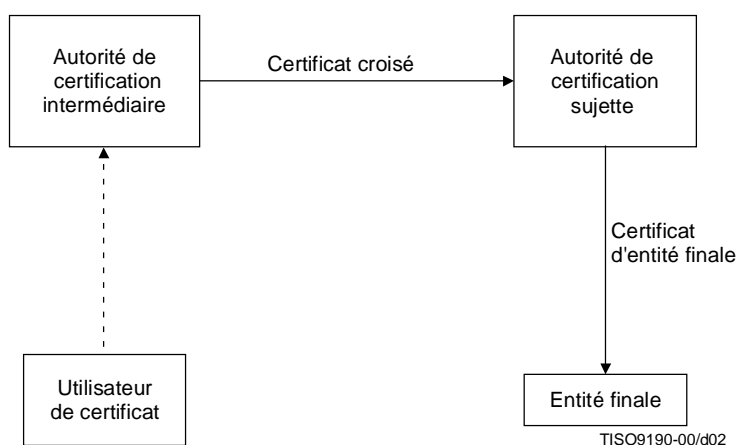


Figure 1 – Certification croisée

Un chemin de certification est considéré comme valide sous l'ensemble des politiques communes à tous les certificats du chemin.

Une autorité de certification intermédiaire peut être à son tour le sujet d'un certificat émis par une autre autorité de certification, ce qui conduit à la création de chemins de certification d'une longueur supérieure à deux certificats. Etant donné que la confiance est affectée par le niveau de diffusion en fonction de l'augmentation de la longueur des chemins de certificat, des mesures de contrôle sont nécessaires pour garantir que des certificats d'entité finale avec un niveau de confiance trop faible pour être accepté seront rejetés par l'utilisateur de certificat. Cette fonction fait partie de la procédure de traitement du chemin de certification.

Les deux cas particuliers suivants doivent être pris en considération en plus de la situation décrite précédemment:

- 1) l'autorité de certification n'utilise pas d'extension de politiques de certificat pour véhiculer ses prescriptions de politique à destination des utilisateurs de certificat; et
- 2) l'utilisateur de certificat ou l'autorité de certification intermédiaire délègue les tâches de vérification de politique à l'autorité suivante du chemin.

Dans le premier cas, le certificat ne doit contenir aucune extension de politiques de certificat et il s'ensuit que l'ensemble des politiques sous lequel le chemin est valide sera vide, le chemin pouvant toutefois être valide. Les utilisateurs de certificat doivent toujours s'assurer qu'ils utilisent le certificat en conformité avec les politiques des autorités du chemin.

Dans le deuxième cas, l'utilisateur de certificat ou l'autorité de certification doit fournir la valeur spéciale *any-policy* (toute politique) dans l'ensemble *initial-policy-set* (ensemble de politiques initiales) ou dans le certificat croisé. Lorsqu'un certificat contient la valeur spéciale *any-policy*, il ne peut contenir aucun autre identificateur de politique de certificat. Les identificateurs *any-policy* ne doivent posséder aucun qualificatif de politique associé.

L'utilisateur de certificat peut s'assurer que toutes ses obligations sont véhiculées conformément à la Recommandation | Norme internationale en positionnant l'indicateur *initial-explicit-policy* (politique initiale explicite). De cette manière, seules des autorités qui utilisent l'extension de politiques de certificat normalisée pour réaliser des liaisons sont acceptées sur le chemin et les utilisateurs de certificat ne sont soumis à aucune obligation supplémentaire. Etant donné que les autorités contractent des obligations lorsqu'elles agissent comme un utilisateur de certificat ou pour son compte, elles peuvent s'assurer que toutes leurs obligations sont véhiculées conformément à la Recommandation | Norme internationale en positionnant la composante **requireExplicitPolicy** (exigence de politique explicite) dans le certificat croisé.

Mappages de politiques

Certains chemins de certification peuvent franchir des frontières entre domaines de politique. Les garanties et obligations selon lesquelles est émis le certificat peuvent être matériellement équivalentes à tout ou partie des garanties et obligations selon lesquelles l'autorité de certification sujette émet des certificats destinés à des entités finales, même si les autorités de politique sous lesquelles agissent les deux autorités de certification peuvent avoir choisi des identificateurs non ambigus différents pour ces politiques matériellement équivalentes. L'autorité de certification intermédiaire peut, dans ce cas, faire figurer dans le certificat croisé une extension de mappages de politiques. Dans une telle extension, l'autorité de certification intermédiaire garantit à l'utilisateur de certificat qu'il continuera à bénéficier des garanties habituelles et qu'il doit continuer à remplir ses obligations habituelles, même si les entités suivantes du chemin de certification agissent dans un autre domaine de politique. L'autorité de certification intermédiaire doit indiquer un ou plusieurs mappages pour chacun des sous-ensembles de politiques sous lesquels est émis le certificat croisé; elle ne doit pas indiquer de mappage pour toute autre politique. Si un ou plusieurs certificats de politiques sous lesquels intervient l'autorité de certification sujette sont identiques à ceux sous lesquels intervient l'autorité de certification intermédiaire (c'est-à-dire s'ils possèdent le même identificateur non ambigu), alors ces identificateurs ne doivent pas figurer dans l'extension de mappages de politiques mais doivent être présents dans une extension de politiques de certificat.

Le mappage de politiques a pour effet, pour tous les certificats sur la suite du chemin de certification, de convertir tous les identificateurs de politique vers un identificateur de la politique équivalente, telle qu'elle est reconnue par l'utilisateur de certificat.

Les politiques ne seront pas mappées, dans un sens ou dans l'autre, avec la valeur spéciale *any-policy*.

Les utilisateurs de certificat peuvent établir s'ils peuvent ou non faire confiance à des certificats émis dans un domaine de politique autre que le leur, en dépit du fait qu'une autorité de certification intermédiaire fiable peut décider que sa politique est matériellement équivalente à leur propre politique. Ceci peut se faire en positionnant la valeur spéciale *initial-policy-mapping-inhibit* (inhibition de mappage de politique initiale) sur la procédure de validation de chemin. Une autorité de certification intermédiaire peut en outre agir de même pour le compte de ses utilisateurs de certificat. Elle peut positionner la valeur de la composante **inhibitPolicyMapping** (inhibition de mappage de politique) dans une extension de contraintes de politique pour s'assurer que les utilisateurs de certificat appliquent correctement cette prescription.

Traitement de chemin de certification

L'utilisateur de certificat a le choix entre deux stratégies:

- 1) il peut exiger que le chemin de certification soit valide conformément à l'un au moins des ensembles de politiques qu'il a déterminés à l'avance;
- 2) il peut demander au module de validation de chemin de lui rendre compte de l'ensemble de politiques pour lequel le chemin de certification est valide.

La première stratégie peut être préférable lorsque l'utilisateur de certificat connaît a priori l'ensemble de politiques acceptable pour l'utilisation prévue.

La deuxième stratégie peut être préférable lorsque l'utilisateur de certificat ne connaît pas a priori l'ensemble de politiques acceptable pour l'utilisation prévue.

Dans le premier cas, la procédure de validation du chemin de certification indiquera que le chemin est valide uniquement s'il est valide conformément à une ou plusieurs des politiques spécifiées dans l'ensemble *initial-policy-set* et renverra le sous-ensemble de l'ensemble *initial-policy-set* pour lequel le chemin est valide. Dans le deuxième cas, la procédure de validation du chemin de certification peut indiquer que le chemin n'est pas valide conformément à l'ensemble *initial-policy-set*, mais qu'il est valide pour un ensemble disjoint: l'ensemble *authorities-constrained-policy-set* (ensemble de politiques imposé par des autorités). L'utilisateur de certificat doit alors déterminer si l'emploi qu'il souhaite faire du certificat est en accord avec une ou plusieurs politiques de certificat pour lesquelles le chemin *est* effectivement valide. L'utilisateur de certificat peut forcer la procédure à renvoyer un résultat valide conformément à toute politique (non spécifiée) en positionnant la valeur de l'ensemble *initial-policy-set* sur *any-policy*.

Certificats auto-émis

Une autorité de certification peut émettre un certificat à sa propre intention dans les trois cas suivants:

- 1) comme procédé commode pour le codage de sa clé publique à des fins de communication à ses utilisateurs de certificat et pour son stockage par ces derniers;
- 2) pour certifier des utilisations de clés autres que pour la signature de certificat et de liste (par exemple, pour un horodatage);
- 3) pour remplacer ses certificats après expiration.

Ces types de certificat sont appelés certificats auto-émis; ils peuvent être reconnus par le fait qu'ils contiennent des noms d'émetteur et de sujet identiques. Les certificats auto-émis du premier type peuvent être vérifiés, à des fins de validation de chemin, au moyen de la clé publique qu'ils contiennent et seront ignorés s'ils sont rencontrés sur le chemin.

Les certificats auto-émis du deuxième type apparaissent exclusivement sous la forme de certificats en fin d'un chemin et seront traités en conséquence.

Les certificats auto-émis du troisième type (appelés également certificats intermédiaires auto-émis) peuvent apparaître comme certificats intermédiaires sur un chemin. La procédure correcte pour une autorité de certification qui remplace une clé au moment de son expiration consiste à demander l'émission de tous les certificats croisés, engagés dans des liaisons, dont elle a besoin pour remplacer sa clé publique avant d'utiliser la nouvelle clé. Si toutefois des certificats auto-émis sont rencontrés sur le chemin, ils seront traités comme des certificats intermédiaires avec l'exception suivante: ils ne contribuent pas au comptage de la longueur du chemin dans le traitement de la composante **pathLenConstraint** (contrainte de longueur de chemin) de l'extension **basicConstraints** (contraintes de base) et des valeurs de *skip-certificates* (certificats ignorés) associées aux indicateurs *policy-mapping-inhibit-pending* (attente de mappage de politique) et *explicit-policy-pending* (attente de politique explicite)."

Dans le paragraphe 12.2.2.6, après la deuxième phrase du premier paragraphe, ajouter le texte suivant:

"La présence de cette extension dans un certificat d'entité finale indique les politiques de certification pour lesquelles ce certificat est valide. La présence de cette extension dans un certificat émis par une autorité de certification vers une autre autorité de certification indique les politiques de certification pour lesquelles ce certificat peut être utilisé pour valider des chemins de certification."

Ajouter le texte suivant au paragraphe 12.2.2.6, après la première phrase du premier paragraphe:

"La liste des politiques de certification est utilisée pour déterminer la validité d'un chemin de certification, conformément à la description donnée au 12.4.3. Les informations facultatives qualifiant ces politiques de certification ne sont pas utilisées dans la procédure de traitement du chemin de certification, mais des qualificateurs pertinents sont fournis au certificat comme résultat de ce processus au moyen d'une application aidant à déterminer si un chemin valide est approprié à la transaction en question."

Dans le paragraphe 12.2.2.7, remplacer la phrase "Cette extension n'est jamais critique." par la phrase suivante:

"Cette extension peut, sur option de l'émetteur de certificat, être soit critique soit non critique. Il est recommandé qu'elle soit critique car, dans le cas contraire, un utilisateur de certificat peut ne pas interpréter correctement les prescriptions de l'autorité de certification émettrice."

Ajouter le nouveau paragraphe 12.4.2.4 suivant:

"12.4.2.4 Champ d'inhibition d'une politique quelconque

Ce champ spécifie une contrainte qui indique que la valeur any-policy (toute politique) n'est pas considérée comme une correspondance explicite pour d'autres politiques de certification pour la partie restante du chemin de certification.

**inhibitAnyPolicy ::= EXTENSION {
SYNTAX SkipCerts
IDENTIFIED BY {id-ce-inhibitAnyPolicy }}**

Cette extension peut, sur option de l'émetteur de certificat, être soit critique soit non critique. Il est recommandé qu'elle soit critique car, dans le cas contraire, un utilisateur de certificat peut ne pas interpréter correctement les prescriptions de l'autorité de certification émettrice."

Ajouter l'élément suivant à la liste des identificateurs d'objet du module d'extensions de certificat de l'Annexe A:

"id-ce-inhibitAnyPolicy OBJECT IDENTIFIER ::= {id-ce 54}"

Remplacer le paragraphe 12.4.3 par le texte suivant:

"12.4.3 Procédure de traitement du chemin de certification

Le traitement du chemin de certification s'effectue dans un système qui a besoin d'utiliser la clé publique d'une entité finale distante, par exemple pour vérifier une signature numérique générée par une telle entité. Les politiques de certificat, les contraintes de base, les contraintes de nom et les extensions de contraintes de politique ont été conçues pour faciliter une implémentation automatisée et autonome de la logique de traitement du chemin de certification.

L'exposé sommaire qui suit présente une procédure de validation des chemins de certification. Une implémentation sera fonctionnellement équivalente au comportement externe résultant de cette procédure. L'algorithme utilisé par une implémentation particulière pour fournir les sorties correctes à partir des entrées données n'est pas normalisé.

Les informations d'entrée de la procédure de traitement du chemin de certification sont les suivantes:

- a) un ensemble de certificats constituant un chemin de certification;
- b) une valeur fiable de clé publique ou d'identificateur de clé (si la clé est stockée de manière interne par le module de traitement du chemin de certification) utilisée pour vérifier le premier certificat du chemin de certification;
- c) un ensemble *initial-policy-set* constitué d'un ou plusieurs identificateurs de certificat de politique indiquant qu'une ou plusieurs politiques sont acceptables par l'utilisateur de certificat aux fins de traitement du chemin de certification; cet ensemble peut également prendre la valeur *any-policy*;
- d) une valeur d'indicateur *initial-explicit-policy*, spécifiant si un identificateur de politique acceptable doit figurer de manière explicite dans le champ d'extension de politiques de certificat pour tous les certificats du chemin;
- e) une valeur d'indicateur *initial-policy-mapping-inhibit* spécifiant si le mappage de politique est interdit sur le chemin de certification;
- f) la valeur d'indicateur *initial-inhibit-policy* qui indique si la valeur spéciale **anyPolicy**, présente dans une extension de politiques de certificat, est considérée comme pouvant remplacer une valeur quelconque de politique de certificat spécifique dans un ensemble contraint; et
- g) la date et l'heure actuelles (si ces dernières ne sont pas disponibles de manière interne dans le module de traitement du chemin de certification).

Les valeurs de c), d), e) et f) dépendront des prescriptions de politique du couple utilisateur-application qui utilise la clé publique certifiée de l'entité finale.

Noter qu'en raison de ces entrées individuelles dans le processus de validation de chemin, un utilisateur de certificat peut limiter à un ensemble donné de politiques de certificat la confiance qu'il accorde à une quelconque clé publique sécurisée. A cette fin, l'on peut veiller à ce qu'une clé publique donnée ne constitue l'entrée dans le processus que lorsque l'entrée *initial-policy-set* contient des politiques pour lesquelles l'utilisateur de certificat a confiance dans cette clé publique. Etant donné qu'une autre entrée dans le processus est le chemin de certification proprement dit, ce contrôle pourrait être exercé en mode transaction par transaction.

Les informations de sortie de la procédure sont les suivantes:

- a) indication de réussite ou d'échec de la validation du chemin de certification;
- b) en cas d'échec de la validation, un code diagnostic indiquant le motif de la défaillance;
- c) l'ensemble de politiques imposées par l'autorité et leurs qualificatifs associés, sous lesquelles le chemin de certification est valide ou la valeur spéciale *any-policy*;
- d) l'ensemble de politiques imposées par l'utilisateur constitué de l'intersection de l'ensemble *authorities-constrained-policy-set* et de l'ensemble *initial-policy-set*;
- e) l'indicateur *explicit-policy-indicator* signalant si l'utilisateur du certificat ou une autorité située sur le chemin exige qu'une politique acceptable soit identifiée dans chaque certificat du chemin;
- f) les détails de tout mappage de politique qui a été rencontré lors du traitement du chemin de certification.

NOTE – En cas de réussite de la validation, le système utilisant des certificats peut toutefois décider de ne pas employer le certificat en fonction des valeurs de qualificatif de politique ou d'autres informations figurant dans le certificat.

La procédure utilise les variables d'état suivantes:

- a) *authorities-constrained-policy-set* (ensemble de politiques imposées par l'autorité): table d'identificateurs et de qualificateurs de police extraite des certificats du chemin de certification (dans laquelle les rangées représentent les politiques, leurs qualificateurs et leur historique de mappage et dans laquelle les colonnes représentent des certificats faisant partie du chemin de certification);
- b) *permitted-subtrees* (sous-arbres autorisés): ensemble de spécifications de sous-arbre définissant les sous-arbres auxquels doit appartenir tout nom de sujet figurant dans des certificats suivants dans le chemin de certification, ou la valeur spéciale *unbounded* (non lié);
- c) *excluded-subtrees* (sous-arbres interdits): ensemble (éventuellement vide) de spécifications de sous-arbre (comportant chacune un nom de base de sous-arbre et des indicateurs de niveau minimal et maximal) définissant des sous-arbres auxquels ne doit pas appartenir tout nom de sujet figurant dans les certificats suivants dans le chemin de certification;
- d) *explicit-policy-indicator* (indicateur de politique explicite): indique si une politique acceptable doit figurer de manière explicite dans chaque certificat;
- e) *path-depth* (profondeur du chemin): nombre entier égal au nombre de certificats sur le chemin de certification, augmenté de un, pour lesquels le traitement a été effectué;
- f) *policy-mapping-inhibit-indicator* (indicateur d'inhibition de mappage de politique): indique si le mappage de politique est interdit;
- g) *inhibit-any-policy-indicator* (indicateur d'inhibition d'une politique quelconque): indique si la valeur spéciale **anyPolicy** est considérée comme pouvant remplacer une politique de certificat spécifique;
- h) *pending-constraints* (contraintes en attente): détails des contraintes de *politique explicite*, d'*inhibition de mappage de politique* ou d'*inhibition d'une politique quelconque*, qui ont été stipulées mais qui doivent prendre effet sur la suite du chemin. Il s'agit de trois indicateurs d'un bit appelés *explicit-policy-pending* (politique explicite en attente), *policy-mapping-inhibit-pending* (inhibition de mappage de politique en attente) et *inhibit-any-policy-pending* (inhibition d'une politique quelconque en attente) ainsi que pour chacun d'eux, d'un entier appelé *skip-certificates* qui donne le nombre de certificats restant à ignorer avant que les contraintes prennent effet.

La procédure implique une étape d'initialisation suivie d'une série d'étapes de traitement. L'étape d'initialisation comprend les actions suivantes:

- a) remplir les colonnes de rang zéro et un du tableau *authorities-constrained-policy-set* avec la valeur *any-policy*;

- b) initialisation de la variable *permitted-subtrees* avec la valeur *unbounded*;
- c) initialisation de la variable *excluded-subtrees* avec l'ensemble vide;
- d) initialisation de l'indicateur *explicit-policy-indicator* avec la valeur *initial-explicit-policy*;
- e) initialisation de la variable *path-depth* avec la valeur un;
- f) initialisation de l'indicateur *policy-mapping-inhibit-indicator* avec la valeur *initial-policy-mapping-inhibit*;
- g) initialisation des trois indicateurs *pending-constraints* sur "non positionné".

Les certificats sont ensuite traités un par un en commençant par le certificat utilisant la clé publique fiable d'entrée. Le dernier certificat est considéré comme étant le certificat final; tous les autres certificats sont considérés comme étant des certificats intermédiaires.

Les vérifications suivantes s'appliquent à un certificat:

- a) vérifier que la signature est correcte, que les dates sont valides, que la succession des noms de sujet de certificat et d'émetteur de certificat est correcte et que le certificat n'a pas été révoqué;
- b) si la contrainte d'extension de base est présente dans un certificat intermédiaire, vérifier que la composante **cA** est présente et positionnée sur "Vrai". Si la composante **pathLenConstraint** est présente, vérifier que le chemin de certification actuel respecte cette contrainte de longueur (en ignorant les certificats intermédiaires auto-émis);
- c) si l'extension de politiques de certificat n'est pas présente, positionner alors l'ensemble *authorities-constrained-policy-set* sur l'ensemble vide en supprimant toutes les lignes dans le tableau *authorities-constrained-policy-set*;
- d) si l'extension des politiques d'un certificat est présente, l'on rattache à chaque rangée de la table *authorities-constrained-policy-set* dont l'entrée dans la colonne [*path-depth*] contient la valeur P, les qualificatifs de politique associés à chaque politique P dans l'extension autre que **anyPolicy**. Si aucune rangée de la table *authorities-constrained-policy-set* ne contient la politique P dans son entrée de colonne [*path-depth*] mais que la valeur contenue dans *authorities-constrained-policy-set* [0, *path-depth*] soit *any-policy*, l'on ajoute une nouvelle rangée à la table en dupliquant la rangée n° 0 et en écrivant l'identificateur de politique P avec ses qualificatifs dans l'entrée de colonne [*path-depth*] de la nouvelle rangée;
- e) si l'extension des politiques d'un certificat est présente mais ne contient pas la valeur **anyPolicy**, ou si la variable d'état *inhibit-any-policy-indicator* est activée, l'on supprime toute rangée dont l'entrée de colonne [*path-depth*] contient la valeur *any-policy* ainsi que toute rangée dont l'entrée de colonne [*path-depth*] ne contient pas une des valeurs contenues dans l'extension des politiques du certificat;
- f) si l'extension des politiques d'un certificat est présente et contient la valeur **anyPolicy** et que la variable d'état *inhibit-any-policy-indicator* ne soit pas activée, l'on rattache les qualificatifs de politique associés à la valeur **anyPolicy** à chaque rangée de la table *authorities-constrained-policy-set* dont l'entrée de colonne [*path-depth*] contient la valeur *any-policy* ou une valeur qui n'est pas contenue dans l'extension des politiques du certificat;
- g) si le certificat n'est pas un certificat intermédiaire auto-émis, vérifier que le nom du sujet appartient à l'espace de noms indiqué par la valeur de *permitted-subtrees* et n'appartient pas à l'espace de noms indiqué par la valeur *excluded-subtrees*.

Les actions suivantes d'enregistrement de contrainte sont effectuées ensuite, dans le cas d'un certificat intermédiaire, afin de positionner la valeur correcte des variables d'état pour le traitement du certificat suivant:

- a) si l'extension **nameConstraints** (contraintes de nom) est présente dans le certificat avec une composante **permittedSubtrees** (sous-arbres autorisés), remplacer alors la valeur de la variable d'état *permitted-subtrees* par l'intersection de sa valeur précédente avec la valeur indiquée dans l'extension de certificat;
- b) si l'extension **nameConstraints** est présente dans le certificat avec une composante **excludedSubtrees** (sous-arbres interdits), remplacer alors la valeur de la variable d'état *excluded-subtrees* par l'union de sa valeur précédente avec la valeur indiquée dans l'extension de certificat;
- c) si l'indicateur *policy-mapping-inhibit-indicator* est positionné:
 - traiter toute extension de mappage de politique, pour chaque mappage identifié dans l'extension, en localisant toutes les lignes dans le tableau *authorities-constrained-policy-set* dont l'élément dans la colonne de rang [*path-depth*] est égal à la valeur de la politique de domaine de l'émetteur et en supprimant la colonne;

- d) si l'indicateur *policy-mapping-inhibit-indicator* n'est pas positionné:
- traiter de la manière suivante toute extension de mappage de politique, pour tout mappage figurant dans l'extension: localiser toutes les lignes dans le tableau *authorities-constrained-policy-set* dont l'élément de la colonne de rang *[path-depth]* est égal à la valeur de politique du domaine émetteur figurant dans l'extension et copier la valeur de politique du domaine sujet de l'extension dans l'élément de la colonne de rang *[path-depth+1]* de la même ligne. Si l'extension mappe une politique de domaine émetteur avec plusieurs politiques de domaine sujet, la ligne concernée doit alors être copiée et le nouvel élément ajouté à chaque colonne. Si la valeur de l'élément *authorities-constrained-policy-set* *[0, path-depth]* est égale à *any-policy*, copier alors tout identificateur de politique de domaine émetteur, pour l'extension de mappage de politique, dans la colonne de rang *[path-depth]*, en dupliquant les lignes si nécessaire et en conservant les qualificatifs s'ils sont présents, et copier la valeur de politique du domaine sujet de l'extension dans l'élément de la colonne de rang *[path-depth+1]* de la même ligne;
 - si l'indicateur *policy-mapping-inhibit-pending* est positionné et si le certificat n'est pas auto-émis, décrémenter alors la valeur correspondante de *skip-certificates* et positionner l'indicateur *policy-mapping-inhibit-indicator* si cette valeur devient nulle;
 - procéder comme suit si la contrainte **inhibitPolicyMapping** figure dans le certificat. Positionner l'indicateur *policy-mapping-inhibit-indicator* si la valeur de la composante **SkipCerts** (certificats ignorés) est nulle. Pour toute autre valeur de la composante **SkipCerts**, positionner l'indicateur *policy-mapping-inhibit-pending* et positionner la valeur correspondante de *skip-certificates* sur la plus petite des valeurs de la composante **SkipCerts** et de la valeur précédente de *skip-certificates* (si l'indicateur *policy-mapping-inhibit-pending* était déjà positionné);
- e) pour toute ligne non modifiée dans l'étape c) ou d) ci-dessus (et pour toute ligne dans le cas où aucune extension de mappage ne figure dans le certificat), copier la valeur de l'identificateur de politique de la colonne de rang *[path-depth]* dans la colonne de rang *[path-depth+1]* de la ligne;
- f) si l'indicateur *inhibit-any-policy* n'est pas positionné:
- si l'indicateur *inhibit-any-policy-pending* est positionné et si le certificat n'est pas auto-émis, décrémenter alors la valeur *skip-certificates* correspondante et positionner l'indicateur *inhibit-any-policy* si cette valeur devient nulle;
 - procéder comme suit si la contrainte **inhibitAnyPolicy** figure dans le certificat. Positionner l'indicateur *inhibit-any-policy-indicator* si la valeur de la composante **SkipCerts** (certificats ignorés) est nulle. Pour les autres valeurs de la composante **SkipCerts**, positionner l'indicateur *inhibit-any-policy-pending* et positionner les valeurs correspondantes de *skip-certificates* sur la plus petite des valeurs de la composante **SkipCerts** et de la valeur précédente de *skip-certificates* (si l'indicateur *inhibit-any-policy-pending* était déjà positionné);
- g) incrémenter la variable *path-depth*.

Les actions suivantes sont ensuite effectuées pour tous les certificats:

- a) si l'indicateur *explicit-policy-indicator* n'est pas positionné:
- si l'indicateur *explicit-policy-pending* est positionné et si le certificat n'est pas un certificat intermédiaire auto-émis, décrémenter la valeur *skip-certificates* correspondante et positionner l'indicateur *explicit-policy-indicator* si cette valeur devient nulle;
 - si la contrainte **requireExplicitPolicy** est présente dans le certificat, l'on effectue les opérations suivantes. Pour une valeur **SkipCerts** = 0, l'on active la variable d'état *explicit-policy-indicator*. Pour toute autre valeur de l'élément **SkipCerts**, l'on active l'indicateur *explicit-policy-pending* et l'on donne aux valeurs correspondantes de la variable *skip-certificates* la plus petite des valeurs de l'élément **SkipCerts** et la précédente valeur de *skip-certificates* (si l'indicateur *inhibit-any-policy-pending* était déjà activé);
 - si la composante **requireExplicitPolicy** est présente, et que le chemin de certification contient un certificat émis par une autorité de certification désignée, il est nécessaire que tous les certificats du chemin contiennent, dans l'extension relative aux politiques de certification, un identificateur de politique acceptable. Cet identificateur est celui de la politique de certification requise par l'utilisateur du chemin de certification, celui d'une politique qui a été déclarée équivalente à la première grâce à la fonction de mappage de politiques, ou la valeur spéciale *any-policy*. L'autorité de certification désignée est soit l'autorité émettrice du certificat contenant cette extension (si la valeur de la composante **requireExplicitPolicy** est zéro) soit une autorité de certification qui est titulaire d'un certificat subséquent dans le chemin de certification (tel qu'indiqué par une valeur non nulle).

Les actions suivantes sont effectuées pour les certificats d'entité finale:

- a) vérifier alors que le tableau *authorities-constrained-policy-set* n'est pas vide si l'indicateur *explicit-policy-indicator* est positionné. 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* et des valeurs nulles dans l'ensemble *user-constrained-policy-set* et dans le tableau *authorities-constrained-policy-set*.

Si aucun des contrôles ci-dessus ne produit d'échec concernant le certificat final, l'ensemble *user-constrained-policy-set* doit être calculé par formation de l'intersection de l'ensemble *authorities-constrained-policy-set* avec l'ensemble *initial-policy-set*. Si la valeur de l'état *authorities-constrained-policy-set* [0, *path-depth*] est *any-policy*, alors la valeur de l'ensemble *authorities-constrained-policy-set* est *any-policy*. Sinon, l'ensemble *authorities-constrained-policy-set* a, pour chaque rangée de la table, la valeur contenue dans la cellule la plus à gauche qui ne contient pas l'identificateur *any-policy*. La procédure doit ensuite se terminer avec renvoi d'une indication de succès ainsi que de l'indicateur *explicit-policy-indicator*, de la table *authorities-constrained-policy-set* et de la table *user-constrained-policy-set*. Si l'intersection des ensembles de contraintes d'autorité et de contraintes d'usager est vide, le chemin est valide conformément à la (aux) politique(s) contrainte(s) par l'autorité mais aucune de ces politiques n'est acceptable par l'utilisateur."

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