NORME INTERNATIONALE ISO/CEI 9594-8:1998
RECTIFICATIF TECHNIQUE 1

Publié 2000-12-15
Version française parue en 2001

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'annuaire: Cadre d'authentification

RECTIFICATIF TECHNIQUE 1

Information technology — Open Systems Interconnection — The Directory: Authentication framework

TECHNICAL CORRIGENDUM 1

Le Rectificatif technique 1 à la Norme internationale ISO/CEI 9594-8:1998 a été élaboré par le comité technique ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 6, *Téléinformatique*.

ICS 35.100.70 **Réf. nº ISO/CEI 9594-8:1998/Cor.1:2000(F)**

Imprimé en Suisse

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:

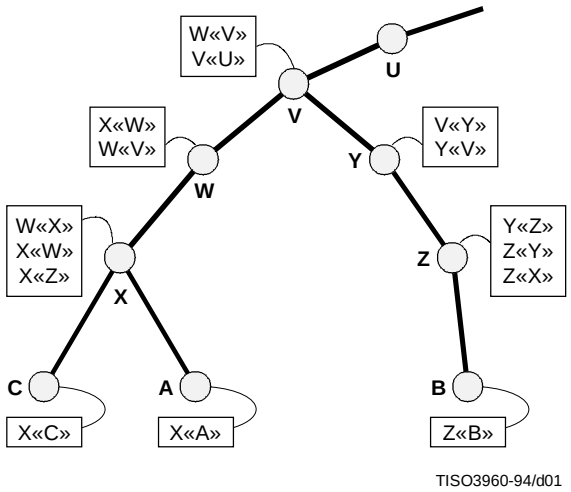

Figure 4 – Exemple fictif de chemin de certification

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.

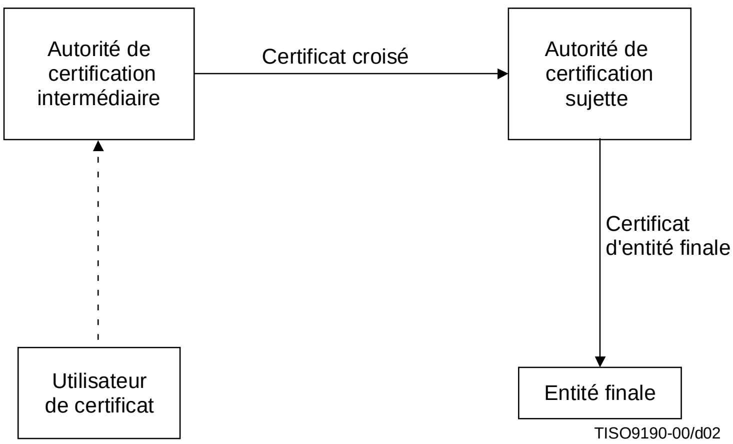

Figure 1 – Certification croisée

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 Recommadation | 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).