NORME INTERNATIONALE

ISO/CEI 9594-8

Cinquième édition
2005-12-15

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'annuaire: Cadre général des certificats de clé publique et d'attribut

Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks

Numéro de référence
ISO/CEI 9594-8:2005(F)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax. + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Version française parue en 2006

Publié en Suisse

TABLE DES MATIÈRES

Avant propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et la CEI ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/CEI 9594-8 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 6, *Téléinformatique*, en collaboration avec l'UIT-T. Le texte identique est publié en tant que Rec. UIT-T X.509.

Cette cinquième édition constitue une révision technique de la quatrième édition (ISO/CEI 9594-8:2001), qui est provisoirement retenue pour soutenir les versions basées sur la quatrième édition.

L'ISO/CEI 9594 comprend les parties suivantes, présentées sous le titre général *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'annuaire*:

— *Partie 1: Aperçu général des concepts, modèles et services*

— *Partie 2: Les modèles*

— *Partie 3: Définition du service abstrait*

— *Partie 4: Procédures pour le fonctionnement réparti*

— *Partie 5: Spécification du protocole*

— *Partie 6: Types d'attributs sélectionnés*

— *Partie 7: Classes d'objets sélectionnées*

— *Partie 8: Cadre général des certificats de clé publique et d'attribut*

— *Partie 9: Duplication*

— *Partie 10: Utilisation de la gestion-systèmes pour l'administration de l'annuaire*

Introduction

La présente Recommandation | Norme internationale, associée à d'autres Recommandations | Normes internationales, a été produite en vue de faciliter l'interconnexion de systèmes de traitement de l'information pour la fourniture de services d'annuaire. Un ensemble de tels services, associés aux informations qu'ils détiennent, peut être considéré comme une entité intégrée, appelée *annuaire*. Les informations détenues par l'annuaire, appelées collectivement base d'information d'annuaire (DIB) sont utilisées en général pour faciliter les communications s'effectuant entre, ou concernant, des objets, tels que des entités d'application, des individus, des terminaux et des listes de répartition.

L'annuaire joue un rôle important dans l'interconnexion des systèmes ouverts; moyennant un minimum d'accords techniques en dehors des normes d'interconnexion proprement dites, il a pour but de permettre l'interconnexion de systèmes de traitement de l'information:

- de fournisseurs divers;
- sous des responsabilités de gestion diverses;
- de niveaux de complexité divers;
- d'âges divers.

De nombreuses applications ont des besoins de sécurité pour se protéger contre des menaces portant sur la communication des informations. Pratiquement tous les services de sécurité font appel à la connaissance fiable des identités des participants de la communication, c'est-à-dire à leur authentification.

La présente Recommandation | Norme internationale définit un cadre pour des certificats de clé publique. Ce cadre comprend la spécification des objets de données utilisés pour représenter les certificats proprement dits ainsi que les notifications de révocation de certificats émis et auxquels il ne doit plus être fait confiance. Le cadre de certificat de clé publique décrit dans la présente Spécification définit certains composants critiques d'une infrastructure de clé publique (PKI), mais pas la totalité d'une telle infrastructure. La présente Spécification fournit toutefois une base permettant d'édifier des infrastructures PKI complètes et leurs spécifications.

La présente Recommandation | Norme internationale définit de même un cadre pour des certificats d'attribut. Ce cadre contient la spécification des objets de données utilisés pour représenter les certificats proprement dits, ainsi que les notifications de révocation de certificat émis auxquels il ne doit plus être fait confiance. Le cadre de certificat d'attribut décrit dans la présente Spécification définit certains composants critiques d'une infrastructure de gestion de privilège (PMI), mais pas la totalité d'une telle infrastructure. La présente Spécification fournit toutefois une base permettant d'édifier des infrastructures PMI complètes et leurs spécifications.

Sont définis également les objets d'informations permettant de stocker les objets d'infrastructure PKI et PMI dans l'annuaire et de comparer des valeurs présentées avec les valeurs stockées.

La présente Recommandation | Norme internationale définit également un cadre pour la fourniture de services d'authentification par l'annuaire au bénéfice de ses utilisateurs.

La présente Recommandation | Norme internationale fournit les cadres de base permettant la définition de profils industriels par d'autres organismes de normalisation et par des forums industriels. L'utilisation d'un grand nombre des fonctionnalités optionnelles figurant dans ces cadres peut être rendue obligatoire dans certains environnements au moyen de profils. Cette cinquième édition révise et étend sur le plan technique la quatrième édition de la présente Recommandation | Norme internationale mais ne la remplace pas. Des implémentations peuvent continuer à déclarer la conformité avec la quatrième édition. Cette dernière ne sera toutefois plus prise en charge à partir d'une certaine date (c'est-à-dire que les comptes rendus de faute ne seront plus traités). Il est recommandé que les implémentations se conforment à la présente cinquième édition, et ce dès que possible.

La présente cinquième édition spécifie les versions 1, 2 et 3 des certificats de clé publique et les versions 1 et 2 des listes de révocation de certificats. La présente édition spécifie la version 2 des certificats d'attribut.

La fonction d'extensibilité a été introduite dans une version précédente avec la version 3 de certificat de clé publique et avec la version 2 de liste de révocation de certificats, et a été incorporée dans le certificat d'attribut dès sa création. Cette fonction est spécifiée au paragraphe 7. Il est prévu que tout développement de la présente édition pourra être intégré à l'aide de cette fonction, évitant ainsi de créer de nouvelles versions.

L'Annexe A, qui fait partie intégrante de la présente Recommandation | Norme internationale, fournit le module ASN.1 contenant toutes les définitions associées au cadre d'authentification.

L'Annexe B, qui fait partie intégrante de la présente Recommandation | Norme internationale, fournit des règles de génération et de traitement des listes de révocation de certificat.

L'Annexe C, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, fournit des exemples d'émission de liste CRL delta.

L'Annexe D, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, fournit des exemples de syntaxe de politiques de privilège et des exemples d'attribut de privilèges.

L'Annexe E, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, constitue une introduction au chiffrement avec clé publique.

L'Annexe F, qui fait partie intégrante de la présente Recommandation | Norme internationale, définit les identificateurs d'objets attribués aux algorithmes d'authentification et de chiffrement, en l'absence d'un enregistrement formel.

L'Annexe G, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, contient des exemples d'utilisation de contraintes de certification d'itinéraire.

L'Annexe H, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, fournit des indications quant aux applications validées pour les infrastructures PKI, au sujet du traitement de la politique de certificat au cours du processus de validation de l'itinéraire de certification.

L'Annexe I, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, fournit des indications quant à l'utilisation du bit contentCommitment dans l'extension de certificat keyUsage.

L'Annexe J, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, contient les définitions des éléments d'information par ordre alphabétique.

L'Annexe K, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, fournit la liste des amendements et des comptes rendus d'erreur qui ont été incorporés dans cette édition de la présente Recommandation | Norme internationale.

NORME INTERNATIONALE
RECOMMANDATION UIT-T

Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut

SECTION 1 – GÉNÉRALITÉS

1 Domaine d'application

La présente Recommandation | Norme internationale traite de certains besoins de sécurité dans les domaines de l'authentification et d'autres services de sécurité, en fournissant un ensemble de cadres sur la base desquels il est possible d'édifier des services complets. La présente Recommandation | Norme internationale définit de manière plus spécifique les cadres suivants:

- certificats de clé publique;
- certificats d'attribut;
- services d'authentification.

Le cadre de certificat de clé publique défini dans la présente Recommandation | Norme internationale englobe la définition des objets d'information pour une infrastructure de clé publique (PKI, *public key infrastructure*), incluant les certificats de clé publique et les listes de révocation de certificat (CRL, *certificate revocation list*). Le cadre de certificat d'attribut englobe la définition des objets d'information pour une infrastructure de gestion de privilège (PMI, *privilege management infrastructure*), incluant les certificats d'attribut et la liste de révocation de certificat d'attribut (ACRL, *attribute certificate revocation list*). La présente Spécification fournit également le cadre pour l'émission, la gestion, l'utilisation et la révocation de certificats. Les formats définis pour les deux types de certificats et pour tous les types de liste de révocation prévoient un procédé d'extension. La présente Recommandation | Norme internationale contient également un ensemble d'extensions normalisées pour chaque type; il est prévu que cet ensemble sera d'une utilité générale pour un certain nombre d'infrastructures PKI et PMI. Les composants du schéma, englobant les classes d'objets, les types d'attribut et les règles de concordance pour le stockage des objets PKI et PMI dans l'annuaire font partie de la présente Recommandation | Norme internationale. Il est prévu que d'autres organismes de normalisation (par exemple le comité TC 68 de l'ISO, l'IETF, etc.) définiront des éléments d'infrastructure PKI et PMI supplémentaires qui sortent de ces cadres, tels que les protocoles de gestion de clé et de certificat, les protocoles opérationnels ou d'autres certificats et extensions de liste CRL.

Le procédé d'authentification défini dans la présente Recommandation | Norme internationale possède un caractère générique et peut s'appliquer à une variété d'applications et d'environnements.

L'annuaire utilise les certificats de clé publique et les certificats d'attribut; le cadre d'utilisation de ces fonctionnalités par l'annuaire est également défini dans la présente Recommandation | Norme internationale. L'annuaire utilise une technologie de clé publique avec certificats pour fournir une authentification forte et des opérations avec signature et/ou chiffrement, ainsi que pour stocker des données signées et/ou chiffrées. Il peut utiliser des certificats d'attribut pour fournir un contrôle d'accès basé sur des règles. Bien que le cadre correspondant soit fourni dans la présente Spécification, la définition complète de l'utilisation de l'annuaire, des services associés qu'il fournit et de ses composants font l'objet d'une définition dans un ensemble complet de spécifications de l'annuaire.

La présente Recommandation | Norme internationale précise également les points suivants dans le cadre des services d'authentification:

- spécification du format des informations d'authentification contenues dans l'annuaire;
- description de la manière dont les informations d'authentification peuvent être obtenues à partir de l'annuaire;
- énoncé des hypothèses faites sur la manière dont les informations d'authentification sont créées et placées dans l'annuaire;
- définition de trois modes d'utilisation possibles des informations d'authentification par des applications en vue d'effectuer l'authentification et la description de la manière dont d'autres services de sécurité peuvent être pris en charge par une authentification.

La présente Recommandation | Norme internationale décrit deux niveaux d'authentification: l'authentification simple utilisant un mot de passe pour vérifier l'identité déclarée et l'authentification forte nécessitant des justificatifs créés au moyen de méthodes de chiffrement. L'authentification simple fournit une certaine protection contre les accès non autorisés, mais seule l'authentification forte devrait être utilisée pour fournir la base de services fiables. Elle n'est pas

conçue pour établir de ce fait un cadre d'authentification, mais peut être utilisée d'une manière générale pour des applications qui considèrent ces procédés comme adéquats.

L'authentification (comme d'autres services de sécurité) peut uniquement être fournie dans le contexte de la définition d'une politique de sécurité. Les utilisateurs d'une application ont la charge de définir leur propre politique de sécurité, pouvant être soumise aux contraintes des services fournis dans le cadre d'une norme.

Les normes de définition d'applications utilisant le cadre d'authentification ont la charge de spécifier les échanges de protocole nécessaires pour réaliser une authentification basée sur les informations d'authentification obtenues à partir de l'annuaire. Le protocole d'accès à l'annuaire (DAP, *directory access protocol*) utilisé par les applications pour obtenir des justificatifs à partir de l'annuaire est spécifié dans la Rec. UIT-T X.519 | ISO/CEI 9594-5.

2 Références normatives

Les Recommandations et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes Recommandations et Normes sont sujettes à révision et les parties prenantes aux accords fondés sur la présente Recommandation sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT tient à jour une liste des Recommandations de l'UIT-T en vigueur.

2.1 Recommandations | Normes internationales identiques

- Recommandation UIT-T X.411 (1999) | ISO/CEI 10021-4:1999, *Technologies de l'information – Systèmes de messagerie – Système de transfert de messages: définition et procédures du service abstrait*
- Recommandation UIT-T X.500 (2005) | ISO/CEI 9594-1:2005, *Technologies de l'information – Interconnexion de systèmes ouverts* (OSI) *– L'annuaire: aperçu général des concepts, modèles et services*
- Recommandation UIT-T X.501 (2005) | ISO/CEI 9594-2:2005, *Technologies de l'information – Interconnexion de systèmes ouverts* (OSI) *– L'annuaire: les modèles*
- Recommandation UIT-T X.511 (2005) | ISO/CEI 9594-3:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: Définition du service abstrait*
- Recommandation UIT-T X.518 (2005) | ISO/CEI 9594-4:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: Procédures pour le fonctionnement réparti*
- Recommandation UIT-T X.519 (2005) | ISO/CEI 9594-5:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: Spécification du protocole*
- Recommandation UIT-T X.520 (2005) | ISO/CEI 9594-6:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: Types d'attributs sélectionnés*
- Recommandation UIT-T X.521 (2005) | ISO/CEI 9594-7:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: Classes d'objets sélectionnées*
- Recommandation UIT-T X.525 (2005) | ISO/CEI 9594-9:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: Duplication*
- Recommandation UIT-T X.530 (2005) | ISO/CEI 9594-10:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: Utilisation de la gestion-systèmes pour l'administration de l'annuaire*
- Recommandation UIT-T X.660 (2004) | ISO/CEI 9834-1:2005, *Technologies de l'information – Interconnexion des systèmes ouverts* (OSI) *– Procédures opérationnelles des organismes d'enregistrement de l'OSI: Procédures générales et arcs sommitaux de l'arborescence des identificateurs d'objet ASN.1*
- Recommandation UIT-T X.680 (2002) | ISO/CEI 8824-1:2002, *Technologies de l'information – Notation de syntaxe abstraite numéro un (ASN.1): Spécification de la notation de base*
- Recommandation UIT-T X.681 (2002) | ISO/CEI 8824-2:2002, *Technologies de l'information – Notation de syntaxe abstraite numéro un (ASN.1): Spécification des objets informationnels*
- Recommandation UIT-T X.682 (2002) | ISO/CEI 8824-3:2002, *Technologies de l'information – Notation de syntaxe abstraite numéro un (ASN.1): Spécification des contraintes*
- Recommandation UIT-T X.683 (2002) | ISO/CEI 8824-4:2002, *Technologies de l'information – Notation de syntaxe abstraite numéro un (ASN.1): Paramétrage des spécifications de la notation de syntaxe abstraite numéro un*

- Recommandation UIT-T X.690 (2002) | ISO/CEI 8825-1:2002, *Technologies de l'information – Règles de codage ASN.1: Spécification des règles de codage de base (BER), des règles de codage canoniques (CER) et des règles de codage distinctives (DER)*
- Recommandation UIT-T X.691 (2002) ISO/CEI 8825-2:2002, *Technologies de l'information – Règles de codage ASN.1: Spécification des règles de codage compact (DER)*
- Recommandation UIT-T X.812 (1995) ISO/CEI 10181-3:1996, *Technologies de l'information – Interconnexion des systèmes ouverts (OSI) – Cadres de sécurité pour les systèmes ouverts: Cadre de contrôle d'accès*
- Recommandation UIT-T X.813 (1996) | ISO/CEI 10181-4:1997, *Technologies de l'information – Interconnexion des systèmes ouverts (OSI) – Cadres de sécurité pour les systèmes ouverts: Cadre de non-répudiation*
- Recommandation UIT-T X.880 (1994) | ISO/CEI 13712-1:1995, *Technologies de l'information – Opérations distantes: Concepts, modèle et notation*
- Recommandation UIT-T X.881 (1994) | ISO/CEI 13712-2:1995, *Technologies de l'information – Opérations distantes: Réalisations OSI – Définition du service de l'élément de service d'opérations distantes*

2.2 Paires de Recommandations | Normes internationales équivalentes par leur contenu technique

- Recommandation CCITT X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*

  ISO 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité.*

3 Définitions

Pour les besoins de la présente Recommandation | Norme internationale, les définitions suivantes s'appliquent.

3.1 Définitions relatives à l'architecture de sécurité du modèle de référence OSI

Les termes suivants sont définis dans la Rec. CCITT X.800 | ISO 7498-2:

a) asymétrique (chiffrement);
b) échange d'authentifications;
c) information d'authentification;
d) confidentialité;
e) justificatifs (ou habilitation);
f) cryptographie;
g) authentification de l'origine des données;
h) déchiffrement;
i) signature numérique
j) chiffrement;
k) clé;
l) mot de passe;
m) authentification de l'entité homologue;
n) symétrique (chiffrement).

3.2 Définitions relatives au modèle d'annuaire

Les termes suivants sont définis dans la Rec. UIT-T X.501 | ISO/CEI 9594-2:

a) attribut;
b) base d'informations d'annuaire;
c) arbre d'informations d'annuaire;
d) agent de système d'annuaire;
e) agent d'utilisateur d'annuaire;

f) nom distinctif;

g) entrée;

h) objet;

i) racine.

3.3 Définitions

Pour les besoins de la présente Recommandation | Norme internationale les termes suivants sont définis:

3.3.1 certificat d'attribut (AC, *attribute certificate*): structure de donnée, portant la signature numérique d'une autorité d'attribut, qui lie certaines valeurs d'attribut à des informations d'identification concernant son détenteur.

3.3.2 autorité d'attribut (AA): autorité qui attribue des privilèges par l'émission de certificats d'attribut.

3.3.3 liste de révocation d'autorité d'attribut (AARL, *attribute authority revocation list*): liste de révocation contenant une liste de références de certificats d'attribut concernant des autorités d'attribut qui ne sont plus considérées comme valides par l'autorité émettrice.

3.3.4 liste de révocation de certificat d'attribut (ACRL, *attribute certificate revocation list*): liste de révocation contenant une liste de références de certificats d'attribut qui ne sont plus considérés comme valides par l'autorité émettrice.

3.3.5 jeton d'authentification (jeton): information véhiculée pendant un échange d'authentification forte et pouvant être utilisée pour authentifier son émetteur.

3.3.6 autorité: entité responsable de l'émission de certificats. La présente Spécification définit les deux types suivants: les autorités de certification émettant des certificats de clé publique et les autorités d'attribut émettant des certificats d'attribut.

3.3.7 certificat d'autorité: certificat émis à destination d'une autorité (par exemple, une autorité de certification ou une autorité d'attribut).

3.3.8 liste CRL de base: liste CRL utilisée comme base pour la création d'une liste dCRL.

3.3.9 certificat d'autorité de certification: certificat émis par une autorité de certification pour une autre autorité de certification.

3.3.10 politique de certificat: ensemble nommé de règles indiquant la possibilité d'appliquer un certificat pour une communauté particulière et/ou une classe d'applications particulière avec des besoins de sécurité communs. Une politique de certificat particulière peut, par exemple, indiquer la possibilité d'application d'un certificat pour des transactions avec échange de données électroniques pour le commerce de biens dans une fourchette de prix donnée.

3.3.11 déclaration de pratique de certification (CPS, *certification practice statement*): déclaration des pratiques d'émission de certificats utilisées par une autorité de certification.

3.3.12 liste de révocation de certificat (CRL, *certificate revocation list*): liste signée indiquant un ensemble de certificats qui ne sont plus considérés comme valides par leur émetteur. Certains types de listes CRL spécifiques sont définis en plus du type générique de liste CRL, pour couvrir des domaines particuliers.

3.3.13 utilisateur de certificat: entité qui a besoin de connaître avec certitude les attributs et/ou la clé publique d'une autre entité.

3.3.14 numéro de série de certificat: valeur entière, non ambiguë pour l'autorité émettrice, qui est associée de manière biunivoque à un certificat émis par cette autorité.

3.3.15 système utilisant des certificats: implémentation de celles des fonctions définies dans la présente Spécification d'annuaire qui sont mises en œuvre par un utilisateur de certificat.

3.3.16 validation de certificat: processus consistant à s'assurer qu'un certificat était valide à un instant donné, impliquant éventuellement la construction et le traitement d'un itinéraire de certification avec la garantie que tous les certificats de l'itinéraire étaient valides (c'est-à-dire, non caducs ou révoqués) à l'instant donné.

3.3.17 autorité de certification (CA, *certification authority*): autorité jouissant de la confiance d'un ou de plusieurs utilisateurs pour la création et l'attribution de certificats. L'autorité de certification peut, de manière optionnelle, créer les clés des utilisateurs.

3.3.18 liste de révocation d'autorité de certification (CARL, *certification authority revocation list*): liste de révocation contenant une liste de certificats de clé publique émise pour des autorités de certification qui ne sont plus considérées comme valides par l'émetteur du certificat.

3.3.19 itinéraire de certification: séquence ordonnée de certificats concernant des objets contenus dans l'arbre DIT et qui peuvent être traités à partir de la clé publique de l'objet initial de l'itinéraire pour obtenir l'objet final de cet itinéraire.

3.3.20 point de répartition de liste CRL: élément de dictionnaire ou autre source de distribution de listes CRL; une telle liste distribuée par le biais d'un point de répartition de liste CRL peut contenir des éléments révoquant uniquement un sous-ensemble de la totalité des certificats émis par une autorité de certification ou peut contenir des éléments révoquant plusieurs autorités de certification.

3.3.21 certificat croisé: certificat d'attribut ou de clé publique dont l'émetteur et le sujet sont des autorités de certification ou des autorités d'attribut différentes. Des autorités de certification et des autorités d'attribut émettent des certificats destinés à d'autres autorités de certification et d'attribut, soit comme procédé d'autorisation de l'existence de l'autorité de certification sujette (par exemple, au sein d'une hiérarchie stricte), soit pour reconnaître l'existence de l'autorité de certification sujette ou de l'autorité d'attribut détentrice (par exemple dans un modèle de confiance réparti). La structure de certificat croisé est utilisée dans les deux cas.

3.3.22 système de chiffrement: ensemble de transformations d'un texte en clair pour obtenir un texte chiffré et réciproquement, le choix de la ou des transformations particulières à utiliser se faisant au moyen de clés. Les transformations sont définies en général par un algorithme mathématique.

3.3.23 confidentialité des données: ce service peut être utilisé pour protéger des données contre une divulgation non autorisée. Le service de confidentialité des données est pris en charge par le cadre d'authentification. Il peut être utilisé pour protéger des données contre les interceptions.

3.3.24 délégation: transfert d'un privilège d'une entité détentrice vers une autre entité.

3.3.25 itinéraire de délégation: séquence ordonnée de certificats qui peuvent, conjointement à l'authentification de l'identité du déclarant, être traités pour vérifier l'authenticité d'un privilège de ce déclarant.

3.3.26 liste CRL delta (liste dCRL): liste de révocation partielle contenant uniquement des éléments pour des certificats dont le statut de révocation a été modifié depuis la publication de la liste CRL de base référencée.

3.3.27 entité finale: il s'agit soit d'un sujet d'un certificat de clé publique qui utilise sa clé privée à d'autres fins que la signature de certificats, soit d'un détenteur de certificat d'attribut qui utilise ses attributs pour accéder à une ressource ou à une entité qui est un participant faisant confiance.

3.3.28 liste de révocation de certificat d'attribut d'entité finale (EARL, *end-entity attribute certificate revocation list*): liste de révocation contenant une liste de certificats d'attribut émis à destination de détenteurs, qui ne sont pas également des autorités d'attribut et qui ne sont plus considérés comme valides par l'émetteur du certificat.

3.3.29 liste de révocation de certificat de clé publique (EPRL, *end-entity public-key certificate revocation list*): liste de révocation contenant une liste de certificats de clé publique, émise à destination de sujets qui ne sont pas également des autorités de certification, et qui ne sont plus considérés comme valides par l'émetteur du certificat.

3.3.30 variables d'environnement: caractéristiques d'une politique nécessaires pour une décision d'autorisation, qui ne sont pas contenues dans des structures statiques mais qui sont accessibles localement par un vérificateur de privilège (par exemple, le jour et l'heure ou le solde actuel d'un compte).

3.3.31 liste CRL complète: liste de révocation complète contenant des éléments pour tous les certificats qui ont été révoqués pour le domaine d'application donné.

3.3.32 fonction de hachage: fonction (mathématique) qui fait correspondre un argument pris dans un domaine étendu (éventuellement très étendu) à une valeur appartenant à un domaine plus réduit. Une "bonne" fonction de hachage est telle que l'application de la fonction à un ensemble (étendu) d'arguments du premier domaine fournira des valeurs réparties de manière égale (apparemment aléatoire) dans le second domaine.

3.3.33 détenteur: entité qui a reçu la délégation d'un privilège, soit directement de la source d'autorité, soit indirectement par le biais d'une autre autorité d'attribut.

3.3.34 liste CRL indirecte (iCRL, *indirect CRL*): liste de révocation qui contient au moins une information de révocation concernant des certificats émis par des autorités autres que l'émetteur de cette liste.

3.3.35 agrément de clé: méthode de négociation en ligne de la valeur d'une clé sans transfert de cette dernière, même sous forme chiffrée, par exemple en utilisant la méthode Diffie-Hellman (se référer à l'ISO/CEI 11770-1 pour plus d'informations concernant les procédés d'agrément de clé).

3.3.36 méthode d'objet: action pouvant être invoquée pour une ressource (par exemple, un système de fichier peut disposer de méthodes objet de lecture, d'écriture et d'exécution).

3.3.37 fonction non réversible: fonction mathématique facile à calculer, mais qui, pour une valeur quelconque y du domaine image, il est difficile de trouver une valeur x du domaine source telle que f(x) = y. Il peut exister un nombre réduit de valeurs de y pour lesquelles le calcul de x est trivial.

3.3.38 mappage de politique: reconnaissance du fait que, lorsqu'une autorité de certification d'un domaine certifie une autorité de certification d'un autre domaine, une politique de certificat propre au deuxième domaine peut être considérée par l'autorité du premier domaine comme équivalente (mais pas nécessairement comme identique sous tous ses aspects) à une politique de certificat dans le premier domaine.

3.3.39 clé privée; clé secrète (déconseillé): (dans un système de chiffrement avec clé publique) celle des clés d'une paire de clés d'un utilisateur qui est connue uniquement par l'utilisateur concerné.

3.3.40 privilège: attribut ou propriété attribué par une autorité à un utilisateur.

3.3.41 déclarant de privilège: détenteur de privilège utilisant son certificat d'attribut de clé publique pour déclarer un privilège.

3.3.42 infrastructure de gestion de privilège (PMI, *privilege management infrastructure*): infrastructure qui peut prendre en charge la gestion des privilèges correspondant à un service complet d'autorisation et en relation avec une infrastructure de clé publique.

3.3.43 politique de privilège: politique qui définit dans ses grandes lignes les conditions sous lesquelles les vérificateurs de privilège peuvent fournir ou effectuer des services sensibles au profit ou pour le compte de déclarants de privilège qualifiés. La politique de privilège est liée à des attributs associés au service, ainsi qu'à des attributs associés aux déclarants de privilège.

3.3.44 vérificateur de privilège: entité effectuant la vérification de certificats conformément à une politique de privilège.

3.3.45 clé publique: (dans un système de chiffrement avec clé publique) celle des clés d'une paire de clés d'un utilisateur qui est connue de manière publique.

3.3.46 certificat de clé publique (PKC, *public key certificate)*: clé publique d'un utilisateur, associée à certaines autres informations qui sont rendues non falsifiables par signature numérique en utilisant la clé privée de l'autorité de certification émettrice.

3.3.47 infrastructure de clé publique (PKI, *public key infrastructure*): infrastructure pouvant prendre en charge la gestion de clés publiques afin de fournir des services d'authentification, de chiffrement, d'intégrité et de non répudiation.

3.3.48 participant faisant confiance: utilisateur ou agent qui fait confiance aux données contenues dans un certificat pour prendre des décisions.

3.3.49 certificat d'attribution de rôle: certificat contenant l'attribut de rôle qui assigne un ou plusieurs rôles au sujet/au détenteur du certificat.

3.3.50 certificat de spécification de rôle: certificat contenant l'attribution de privilèges à un rôle.

3.3.51 sensibilité: caractéristique d'une ressource liée à sa valeur ou à son importance.

3.3.52 authentification simple: authentification utilisant de simples accords de mot de passe.

3.3.53 politique de sécurité: ensemble de règles fixées par l'autorité de sécurité qui régit l'utilisation et la fourniture de services et de fonctionnalités de sécurité.

3.3.54 certificat d'autorité de certification autoémis: certificat d'attribut dont l'émetteur et le sujet sont la même autorité d'attribut. Une autorité d'attribut peut utiliser un certificat d'autorité de certification émis à l'ordre d'elle-même, par exemple afin de publier des informations de politique.

3.3.55 certificat autoémis: certificat dont l'émetteur et le sujet sont la même autorité de certification. Une autorité de certification peut utiliser des certificats émis à l'ordre d'elle-même, par exemple lors d'une opération de renouvellement de clé pour transférer la confiance de l'ancienne clé vers la nouvelle.

3.3.56 certificat autosigné: cas particulier de certificats autoémis pour lequel la clé privée utilisée par l'autorité de certification pour la signature du certificat correspond à la clé publique qui est certifiée au sein du certificat. Une autorité de certification peut, par exemple, utiliser un certificat signé par elle-même pour publier sa clé publique ou d'autres informations concernant son fonctionnement.

NOTE – L'utilisation des certificats autoémis et des certificats autosignés émis par des entités autres que les autorités de certification ne relève pas du domaine d'application de la présente Recommandation | Norme internationale.

3.3.57 source d'autorité (SOA, *source of authority*): autorité d'attribut auquel peut faire confiance un vérificateur de privilège pour une ressource donnée, en tant qu'autorité ultime pour l'attribution d'un ensemble de privilèges.

3.3.58 authentification forte: authentification utilisant des justificatifs obtenus par des moyens de chiffrement.

3.3.59 confiance: on peut dire d'une manière générale qu'une entité "fait confiance" à une autre entité si la première fait l'hypothèse que la deuxième se comportera exactement comme attendu (par la première). Il se peut que cette confiance s'applique uniquement pour une fonction donnée. Le rôle clé de la confiance dans ce cadre décrit la relation entre une entité effectuant l'authentification et une autorité; une entité sera certaine qu'elle peut faire confiance à l'autorité pour ne créer que des certificats valides et fiables.

3.3.60 ancre de confiance: une ancre de confiance se compose de l'ensemble des informations dont la liste figure ci-après, outre la clé publique: identificateur d'algorithme, paramètres de clé publique (le cas échéant), nom distinctif du détenteur de la clé publique associée (c'est-à-dire autorité de certification sujet) et à titre optionnel période de validité. L'ancre de confiance peut être fournie sous la forme d'un certificat autosigné. Un système utilisant des certificats se fie à une ancre de confiance; celle-ci permet de valider des certificats sur des itinéraires de certification.

4 Abréviations

Pour les besoins de la présente Recommandation | Norme internationale, les abréviations suivantes s'appliquent.

AA	Autorité d'attribut
AARL	Liste de révocation d'autorité d'attribut *(attribute authority revocation list)*
ACC	Certificat d'attribut (*attribute certificate)*
ACRL	Liste de révocation de certificat d'attribut *(attribute certificate revocation list)*
CA	Autorité de certification *(certification authority)*
CARL	Liste de révocation d'autorité de certification *(certification authority revocation list)*
CRL	Liste de révocation de certificat *(certificate revocation list)*
dCRL	Liste delta de révocation de certificat *(delta certificate revocation list)*
DIB	Base d'informations d'annuaire *(directory information base)*
DIT	Arbre d'informations d'annuaire *(directory information tree)*
DSA	Agent de système d'annuaire *(directory system agent)*
DUA	Agent utilisateur d'annuaire *(directory user agent)*
EARL	Liste de révocation de certificat d'attribut d'entité finale *(end-entity attribute certificate revocation list)*
EPRL	Liste de révocation de certificat de clé publique d'entité finale *(end-entity public-key certificate revocation list)*
iCRL	Liste indirecte de révocation de certificat *(indirect certificate revocation list)*
OCSP	Protocole de statut en ligne de certificat *(online certificate status protocol)*
PKC	Certificat de clé publique *(public-key certificate)*
PKCS	Système de chiffrement avec clé publique *(public-key cryptosystem)*
PKI	Infrastructure de clé publique *(public-key infrastructure)*
PMI	Infrastructure de gestion de privilège *(privilege management infrastructure)*
SOA	Source d'autorité *(source of authority)*

5 Conventions

La présente Spécification d'annuaire a été préparée, avec des exceptions mineures, conformément aux *Règles de présentation de texte commun UIT-T | ISO/CEI*, novembre 2001.

Le terme "Spécification d'annuaire" (comme dans "la présente Spécification d'annuaire") doit être considéré comme indiquant la Rec. UIT-T X.509 | ISO/CEI 9594-8. Le terme "Spécifications d'annuaire" doit être considéré comme indiquant les Recommandations de la série X.500 et la totalité des parties de l'ISO/CEI 9594.

La présente Spécification d'annuaire utilise le terme "*systèmes première édition*" pour faire référence à la première édition des Spécifications d'annuaire, c'est-à-dire l'édition 1988 des Recommandations X.500 du CCITT et de l'ISO/CEI 9594:1990. La présente Spécification d'annuaire utilise le terme "*systèmes deuxième édition*" pour faire référence à la deuxième édition des Spécifications d'annuaire, c'est-à-dire l'édition 1993 des Recommandations UIT-T X.500 et de l'ISO/CEI 9594:1995. La présente Spécification d'annuaire utilise le terme "*systèmes troisième*