NORME INTERNATIONALE

ISO/CEI 9594-8

Troisième édition
1998-12-15

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

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

Numéro de référence
ISO/CEI 9594-8:1998(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.ch
Web www.iso.ch

Publiée par l'ISO en 2000

Version française parue en 2001

Imprimé en Suisse

TABLE DES MATIÈRES

Page

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.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 3.

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 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 de la présente partie de l'ISO/CEI 9594 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.

La Norme internationale 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 Recommandation UIT-T X.509.

Cette troisième édition annule et remplace la deuxième édition (ISO/CEI 9594-8:1995), qui a fait l'objet d'une révision mineure.

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 d'authentification*

— *Partie 9: Duplication*

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

Les annexes A et H constituent un élément normatif de la présente partie de l'ISO/CEI 9594. Les annexes B à G et I à K sont données uniquement à titre d'information.

Introduction

La présente Recommandation | Norme internationale a été élaborée, ainsi que d'autres Recommandations | Normes internationales, pour faciliter l'interconnexion des systèmes de traitement de l'information et permettre ainsi d'assurer des services d'annuaire. L'ensemble de tous ces systèmes, avec les informations d'annuaire qu'ils contiennent, peut être considéré comme un tout intégré, appelé *Annuaire*. Les informations de l'Annuaire, appelées collectivement base d'informations d'Annuaire (DIB) sont généralement utilisées pour faciliter la communication entre, avec ou à propos d'objets tels que des entités d'application, des personnes, des terminaux et des listes de distribution.

L'Annuaire joue un rôle important dans l'interconnexion des systèmes ouverts, dont le but est de permettre, moyennant un minimum d'accords techniques en dehors des normes d'interconnexion proprement dites, l'interconnexion des systèmes de traitement de l'information:

- provenant de divers fabricants;
- gérés différemment;
- de niveaux de complexité différents;
- de générations différentes.

Un grand nombre d'applications comportent des prescriptions de sécurité pour assurer leur protection contre les dangers susceptibles de porter atteinte à la communication de l'information. L'Annexe B contient une brève description des dangers généralement connus ainsi que des services et mécanismes de sécurité qu'on peut utiliser pour la protection contre ces dangers. Presque tous les services de sécurité reposent sur la fiabilité de la connaissance des identités des parties en communication, c'est-à-dire sur leur authentification.

La présente Recommandation | Norme internationale définit un cadre de fourniture de services d'authentification par l'Annuaire à ses utilisateurs. Ces derniers utilisent l'Annuaire lui-même ainsi que d'autres applications et services. L'Annuaire peut utilement contribuer à répondre à leur besoins en services d'authentification et autres services de sécurité car c'est un emplacement naturel à partir duquel les parties en communication peuvent obtenir les informations d'authentification des unes et des autres – connaissance sur laquelle repose l'authentification. L'Annuaire est un emplacement naturel du fait qu'il contient d'autres informations nécessaires à la communication et obtenues avant que celle-ci ait lieu. L'obtention, à partir de l'Annuaire, des informations d'authentification d'un éventuel correspondant de communication est, avec cette méthode, semblable à l'obtention d'une adresse. En raison de la vaste portée de l'Annuaire aux fins des communications, on prévoit que le présent cadre d'authentification sera largement utilisé par toute une gamme d'applications.

Cette troisième édition révise techniquement et améliore, mais ne remplace pas, la deuxième édition de la présente Recommandation | Norme internationale. Les implémentations peuvent encore revendiquer la conformité à la deuxième édition mais celle-ci finira par ne plus être prise en compte (c'est-à-dire que les erreurs signalées ne seront plus corrigées). Il est recommandé que les implémentations se conforment, dès que possible, à la présente troisième édition.

Cette troisième édition spécifie les versions 1 et 2 des protocoles de l'Annuaire.

Les première et deuxième éditions spécifiaient également la version 1. La plupart des services et protocoles spécifiés dans la présente édition sont conçus pour fonctionner selon la version 1. Lors de la négociation de celle-ci, on a traité les différences entre les services et entre les protocoles, définis dans les trois éditions, en utilisant les règles d'extensibilité définies dans l'édition actuelle de la Rec. UIT-T X.519 | ISO/CEI 9594-5. Certains services et protocoles améliorés, par exemple les erreurs signées, ne fonctionneront cependant pas avant que toutes les entités d'annuaire mises en jeu dans l'exploitation aient négocié la version 2.

Les réalisateurs voudront bien noter qu'un processus de résolution des erreurs existe et que des corrections pourront être apportées à la présente Recommandation | Norme internationale sous la forme de corrigenda techniques. Les mêmes corrections seront apportées à la présente Recommandation | Norme internationale sous la forme d'un *Guide du réalisateur*. Le Secrétariat du sous-comité peut fournir une liste des corrigenda techniques approuvés pour cette Recommandation | Norme internationale. Les corrigenda techniques publiés peuvent être obtenus auprès de votre organisation nationale de normalisation. Le Guide du réalisateur peut être obtenu par consultation du site Internet de l'UIT.

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

L'Annexe B, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, décrit les prescriptions de sécurité.

L'Annexe C, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, est une introduction à la cryptographie à clé publique.

L'Annexe D, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, décrit le système cryptographique RSA à clé publique.

L'Annexe E, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, décrit les fonctions de hachage.

L'Annexe F, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, décrit les dangers contre lesquels la protection est assurée par les méthodes d'authentification renforcée.

L'Annexe G, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, décrit la confidentialité des données.

L'Annexe H, qui fait partie intégrante de la présente Recommandation | Norme internationale, définit des identificateurs d'objet assignés aux algorithmes d'authentification et de chiffrement, en l'absence d'un registre formel.

L'Annexe I, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, contient une bibliographie.

L'Annexe J, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, contient des exemples d'emploi de contraintes sur le chemin de certification.

L'Annexe K, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, énumère les amendements et les relevés d'erreurs qui ont été intégrés dans la présente édition de la présente Recommandation | Norme internationale.

NORME INTERNATIONALE

RECOMMANDATION UIT-T

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

SECTION 1 – GÉNÉRALITÉS

1 Domaine d'application

La présente Recommandation | Norme internationale:

- spécifie la forme sous laquelle les informations d'authentification sont conservées par l'Annuaire;
- décrit la façon dont on peut obtenir de l'Annuaire ces informations d'authentification;
- énonce les hypothèses faites au sujet de la manière dont ces informations d'authentification sont constituées et au sujet de leur emplacement dans l'Annuaire;
- définit les trois manières dont les applications peuvent employer ces informations pour effectuer des authentifications et décrit la façon dont d'autres services de sécurité peuvent être assurés par l'authentification.

La présente Recommandation | Norme internationale décrit deux niveaux d'authentification: l'authentification simple, qui utilise un mot de passe pour la vérification de l'identité et l'authentification renforcée, qui fait intervenir des habilitations établies au moyen de techniques cryptographiques. Tandis que l'authentification simple n'offre qu'une protection limitée contre l'accès non autorisé, seule l'authentification renforcée devra servir de base à la prestation de services sûrs. Il ne s'agit pas d'en faire un cadre général d'authentification, mais ce niveau peut se prêter à une utilisation générale pour des applications qui considèrent que ces techniques sont appropriées.

On ne peut fournir d'authentification (et d'autres services de sécurité) que dans le contexte d'une politique de sécurité définie pour une application. Il appartient aux utilisateurs de cette application de définir leur propre politique de sécurité, qui peut dépendre des services fournis conformément à une norme.

Il appartient aux normes définissant des applications qui utilisent le cadre d'authentification de spécifier les échanges de protocole qu'il convient d'effectuer afin de parvenir à une authentification fondée sur l'information d'authentification obtenue de l'Annuaire. Le protocole utilisé par les applications pour obtenir des justificatifs de l'Annuaire est le protocole d'accès à l'Annuaire (DAP, *directory access protocol*) spécifié dans la Rec. UIT-T X.519 | ISO/CEI 9594-5.

La méthode d'authentification renforcée qui est spécifiée dans la présente Recommandation | Norme internationale repose sur des systèmes cryptographiques à clé (de codage) publique. C'est le principal avantage de ces systèmes que les certificats d'utilisateur puissent être conservés dans l'Annuaire et être obtenus par les utilisateurs de l'Annuaire de la même manière que d'autres informations de l'Annuaire. On admet que les certificats d'utilisateur sont constitués par des moyens indépendants et qu'ils peuvent ensuite être placés dans l'Annuaire. La production de certificats d'utilisateur est effectuée par une autorité de certification autonome qui est complètement distincte des agents DSA de l'Annuaire. En particulier, aucune exigence spéciale n'est prescrite aux fournisseurs de l'Annuaire pour mémoriser ou communiquer les certificats d'utilisateur de façon sûre.

Une brève introduction à la cryptographie à clé publique est donnée dans l'Annexe C.

En général, le cadre d'authentification ne dépend pas de l'utilisation d'un algorithme particulier pour autant qu'il possède les propriétés décrites à l'article 7. Il est possible dans la pratique d'utiliser un certain nombre d'algorithmes différents. Toutefois, deux utilisateurs qui désirent s'authentifier doivent utiliser le même algorithme cryptographique pour effectuer correctement l'authentification. De cette façon, dans le contexte d'un ensemble d'applications voisines, le choix d'un algorithme unique servira à élargir au maximum la communauté d'utilisateurs capables de s'authentifier et de communiquer en sécurité. Un exemple d'algorithme cryptographique de clé publique est spécifié dans l'Annexe D.

De même, deux utilisateurs qui désirent s'authentifier doivent utiliser la même fonction de hachage (voir 3.3.14) (utilisée pour former des justificatifs et des jetons d'authentification). De nouveau, en principe, on peut utiliser un certain nombre de variantes de fonction de hachage au prix d'un rétrécissement des communautés d'utilisateurs capables de s'authentifier. Une brève introduction aux fonctions de hachage et un exemple de fonction de hachage sont donnés dans l'Annexe E.

2 Références normatives

Les Recommandations et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y 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 | Norme internationale 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 (1995) | ISO/CEI 10021-4:1997, *Technologies de l'information – Systèmes de messagerie: système de transfert de messages: définition et procédures du service abstrait.*
- Recommandation UIT-T X.500 (1997) | ISO/CEI 9594-1:1999, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: vue d'ensemble des concepts, modèles et services*.
- Recommandation UIT-T X.501 (1997) | ISO/CEI 9594-2:1997, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: les modèles*.
- Recommandation UIT-T X.511 (1997) | ISO/CEI 9594-3:1997, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: définition du service abstrait*.
- Recommandation UIT-T X.518 (1997) | ISO/CEI 9594-4:1997, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: procédures pour le fonctionnement réparti*.
- Recommandation UIT-T X.519 (1997) | ISO/CEI 9594-5:1997, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: spécification du protocole*.
- Recommandation UIT-T X.520 (1997) | ISO/CEI 9594-6:1997, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: types d'attributs sélectionnés*.
- Recommandation UIT-T X.521 (1997) | ISO/CEI 9594-7:1997, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: classes d'objets sélectionnées*.
- Recommandation UIT-T X.525 (1997) | ISO/CEI 9594-9:1999, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: duplication*.
- Recommandation UIT-T X.530 (1997) | ISO/CEI 9594-10:1999, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: utilisation de la gestion de systèmes pour l'administration de l'Annuaire.*
- Recommandation X.660 du CCITT (1992) | ISO/CEI 9834-1:1993, *Technologies de l'information – Interconnexion des systèmes ouverts – Procédures pour le fonctionnement des autorités d'enregistrement OSI: Procédures générales.*
- Recommandation UIT-T X.680 (1994) | ISO/CEI 8824-1:1995, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification de la notation de base.*
- Recommandation UIT-T X.681 (1994) | ISO/CEI 8824-2:1995, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des objets informationnels.*
- Recommandation UIT-T X.682 (1994) | ISO/CEI 8824-3:1995, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des contraintes.*
- Recommandation UIT-T X.683 (1994) | ISO/CEI 8824-4:1995, *Technologies de l'information – Notation de syntaxe abstraite numéro un: paramétrage des spécifications de la notation de syntaxe abstraite numéro un.*

– Recommandation UIT-T X.690 (1994) | ISO/CEI 8825-1:1995, *Technologies de l'information – Règles de codage de la notation de syntaxe abstraite numéro un: spécification des règles de codage de base, des règles de codage canoniques et des règles de codage distinctives.*

– Recommandation UIT-T X.690[1)] Cor.2 | ISO/CEI 8825-1[1)] Cor.2.

– 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 X.800 du CCITT (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 des systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité.*

2.3 Autres références

– ISO/CEI 11770-1:1996, *Technologies de l'information – Techniques de sécurité – Partie 1: Cadre général*.

– POSTEL (J.B.), Internet Protocol (Protocole Internet), RFC 791, *Internet Activities Board*, 1981.

– CROCKER (D.H.), Standard for the Format of ARPA Internet Text Messages (Norme pour le format des messages de l'agence ARPA en mode texte sur le réseau Internet), RFC 822, *Internet Activities Board*, 1982.

– MOCKAPETRIS (P.), Domain Names – Implementation and Specification (Noms de domaines – Mise en œuvre et spécification), RFC 1035, *Internet Activities Board*, 1987.

– BERNERS-LEE (T.), *Universal Resource Identifiers in WWW* (Identificateurs universels de ressource dans le réseau WWW), RFC 1630, *Internet Activities Board*, 1994.

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. X.800 du CCITT et l'ISO 7498-2:

a) asymétrique (chiffrement);

b) échange d'authentifications;

c) information d'authentification;

d) confidentialité;

e) habilitation;

f) cryptographie;

g) authentification de l'origine des données;

h) déchiffrement;

i) chiffrement;

j) clé;

k) mot de passe;

l) authentification de l'entité homologue;

m) symétrique (chiffrement).

---

1) Actuellement à l'état de projet.

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 relatives au cadre d'authentification

Les termes suivants sont définis dans la présente Recommandation | Norme internationale.

3.3.1 certificat d'attributs: ensemble d'attributs d'un utilisateur associé à quelques autres informations, qui est rendu infalsifiable par la signature numérique créée au moyen de la clé privée de l'autorité de certification qui a émis ce certificat.

3.3.2 jeton d'authentification; jeton: information acheminée au cours d'un échange d'authentification renforcée, qui peut être utilisée pour authentifier son expéditeur.

3.3.3 certificat d'utilisateur; certificat de clé publique; certificat: clé publique d'un utilisateur, ainsi que certaines autres informations, rendue infalsifiable par chiffrement avec la clé secrète de l'autorité de certification qui l'a délivrée.

3.3.4 certificat d'autorité de certification: certificat délivré par une autorité de certification pour une autre autorité de certification.

3.3.5 politique de certification: ensemble nommé de règles qui indique l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'application particulière ayant des exigences de sécurité communes. Par exemple, une politique de certification donnée peut indiquer l'applicabilité d'un type de certificat à l'authentification de transactions électroniques par transfert de données pour le courtage de marchandises dans une fourchette de prix déterminée.

3.3.6 utilisateur de certificat: entité qui a besoin de connaître, avec certitude, la clé publique d'une autre entité.

3.3.7 système utilisateur de certificat: mise en œuvre des fonctions définies dans la présente spécification d'Annuaire et employées par un utilisateur de certificat.

3.3.8 autorité de certification: autorité chargée par un ou par plusieurs utilisateurs de créer et d'attribuer les certificats. Cette autorité peut, facultativement, créer les clés d'utilisateur.

3.3.9 chemin de certification: séquence ordonnée de certificats d'objets contenus dans l'arbre DIT, qui peut être traitée pour obtenir la clé publique de l'objet final contenu dans le chemin, en même temps que celle de l'objet initial contenu dans le chemin.

3.3.10 point de répartition de liste CRL: entrée de répertoire ou autre source de répartition pour des listes d'annulation de certificat (CRL). Une liste CRL répartie à partir d'un point de répartition CRL peut contenir des entrées d'annulation pour un sous-ensemble seulement de l'ensemble complet des certificats émis par une même autorité de certification ou des entrées d'annulation pour plusieurs autorités de certification.

3.3.11 système cryptographique; cryptosystème: recueil de transformations du texte en clair au texte chiffré et réciproquement, les transformations particulières à utiliser étant sélectionnées par des clés. Les transformations sont normalement définies par un algorithme mathématique.

3.3.12 liste CRL delta: liste CRL partielle, n'indiquant que les modifications intervenues depuis une création de liste CRL antérieure.

3.3.13 entité finale: entité titulaire de certificat qui se sert de sa clé publique pour un autre usage que la signature de certificats.

3.3.14 fonction (de) hachage: fonction (mathématique) qui met en correspondance les valeurs d'un grand (et éventuellement très grand) domaine avec une gamme de valeurs plus petite. Une "bonne" fonction de hachage est telle que les résultats de l'application de la fonction à un (grand) ensemble de valeurs du domaine seront régulièrement (et apparemment aléatoirement) répartis sur toute l'étendue de ce domaine.

3.3.15 agrément de clé: méthode de négociation directe d'une valeur de clé sans transfert de la clé, même sous forme chiffrée, par exemple par la méthode de Diffie-Hellman (on trouvera de plus amples renseignements sur les mécanismes d'agrément de clé dans l'ISO/CEI 11770-1).

3.3.16 fonction à une voie: fonction (mathématique) f qui est facile à calculer mais pour laquelle, à une valeur générale y de l'étendue, il est difficile de faire correspondre par le calcul une valeur x du domaine telle que f(x) = y. Il peut exister un petit nombre de valeurs de y pour lesquelles la détermination de x n'est pas difficile à obtenir par le calcul.

3.3.17 équivalence de politiques: reconnaissance du fait que, lorsqu'une autorité de certification d'un domaine donné certifie une autorité de certification dans un autre domaine, une certaine politique de certification dans ce second domaine peut être considérée, par l'autorité de certification du premier domaine, comme équivalente (mais non nécessairement identique à tous points de vue) à une politique de certification particulière dans le premier domaine.

3.3.18 clé publique: clé d'une paire de clés d'utilisateur qui est publiquement connue (dans un système cryptographique à clé publique).

3.3.19 clé privée; clé secrète (déconseillé): clé d'une paire de clés d'utilisateur qui n'est connue que de cet utilisateur (dans un système cryptographique à clé publique).

3.3.20 authentification simple: authentification obtenue au moyen de simples arrangements de mot de passe.

3.3.21 politique de sécurité: ensemble de règles établies par l'organisme de sécurité qui régit l'utilisation et la fourniture de services et de facilités de sécurité.

3.3.22 authentification renforcée: authentification obtenue au moyen de justificatifs déterminés par cryptographie.

3.3.23 confiance: généralement, on peut dire qu'une entité se fie à une deuxième entité lorsqu'elle (la première entité) formule l'hypothèse que la deuxième entité se comportera exactement comme le prévoit la première entité. Cette confiance ne peut s'appliquer qu'à une fonction particulière. Le rôle principal de la confiance dans le cadre d'authentification consiste à décrire la relation entre une entité d'authentification et une autorité de certification; une entité d'authentification doit être certaine de pouvoir se fier à l'autorité de certification pour qu'elle crée uniquement des certificats valides et fiables.

3.3.24 numéro de série de certificat: valeur entière, unique pour l'autorité de certification qui l'émet et associée sans ambiguïté au certificat émis par cette autorité.

4 Abréviations

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

CA	Autorité de certification (*certification authority*)
CRL	Liste d'annulation de certificats (*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 d'utilisateur d'annuaire (*directory user agent*)
PKCS	Système cryptographique à clé publique (*public key cryptosystem*)

5 Conventions

A quelques exceptions mineures près, la présente Spécification d'Annuaire a été élaborée conformément aux directives concernant la "présentation des textes communs UIT-T | ISO/CEI", qui figurent dans le Guide relatif à la coopération entre l'UIT-T et l'ISO/CEI JTC 1, mars 1993.

Le terme "Spécification d'Annuaire" (comme dans "la présente Spécification d'Annuaire") s'entend selon l'acception de la présente Recommandation | Norme internationale. Le terme "Spécifications d'Annuaire" s'entend selon l'acception de toutes les Recommandations de la série X.500 | ISO/CEI 9594.

La présente Spécification d'Annuaire utilise le terme "systèmes de l'édition 1988" pour désigner les systèmes conformes à la première édition (1988) des Spécifications d'Annuaire, c'est-à-dire à l'édition 1988 des Recommandations de la série X.500 du CCITT et de l'ISO/CEI 9594:1990. La présente Spécification d'Annuaire utilise le terme "systèmes de l'édition 1993" pour désigner les systèmes conformes à la deuxième édition (1993) des Spécifications d'Annuaire, c'est-à-dire l'édition 1993 des Recommandations UIT-T de la série X.500 et de l'ISO/CEI 9594:1995. Les systèmes conformes à la présente troisième édition des Spécifications d'Annuaire sont désignés par le terme "systèmes de l'édition 1997".

Cette Spécification d'Annuaire présente la notation ASN.1 en caractères gras de la police Times Roman, 9 points. Lorsque des types et des valeurs ASN.1 sont cités dans le texte normal, ils en sont différenciés par leur présentation en caractères gras Times Roman, 9 points. Les noms des procédures, normalement cités lors de la spécification des sémantèmes de traitement, sont différenciés du texte normal par une présentation en caractères gras de la police Helvetica. Les autorisations de contrôle d'accès sont présentées en caractères italiques de la police Helvetica.

Si, dans une liste, les points sont numérotés (au lieu d'utiliser des tirets ou des lettres), ils sont considérés comme des étapes d'une procédure.

La notation utilisée dans la présente Spécification d'Annuaire est définie dans le Tableau 1 ci-après.

Tableau 1 – Notation

Notation	Signification
Xp	Clé publique d'un utilisateur X.
Xs	Clé privée de X.
Xp[I]	Chiffrement d'une certaine information, I, au moyen de la clé publique de X.
Xs[I]	Chiffrement de I au moyen de la clé privée de X.
X{I}	Signature de I par l'utilisateur X. Elle se compose de l'information I, assortie d'un sommaire chiffré.
CA(X)	Autorité de certification de l'utilisateur X.
CA^n (X)	(où n>1): CA(CA(...n fois...(X)))
X_1«X_2»	Certificat de l'utilisateur X_2 émis par l'autorité de certification X_1.
X_1«X_2» X_2«X_3»	Chaîne de certificats (pouvant être de longueur arbitraire) où chaque élément est le certificat pour l'autorité de certification qui a produit le certificat suivant. Il est fonctionnellement équivalent au certificat ci-après: X_1«X_{n+1}». Par exemple, la possession de A«B»B«C» fournit la même capacité que A«C», à savoir la possibilité de découvrir Cp étant donné Ap.
X_1p • X_1«X_2»	Opération de dévoilement d'un certificat (ou d'une chaîne de certificats) pour en extraire une clé publique. C'est un opérateur infixe dont l'opérande gauche est la clé publique d'une autorité de certification, et dont l'opérande droit est un certificat délivré par cette autorité de certification. Le résultat est la clé publique de l'utilisateur dont le certificat est l'opérande droit. Par exemple: Ap • A«B» B«C» indique l'opération de l'utilisation de la clé publique de A pour obtenir la clé publique Bp de B, à partir de son certificat, suivie de l'utilisation de Bp pour dévoiler le certificat de C. Le résultat de l'opération est la clé publique Cp de C.
A→B	Chemin de certification de A vers B, composé d'une chaîne de certificats débutant par: CA(A)«CA^2(A)» et finissant par CA(B)«B».
NOTE – Dans ce tableau, les symboles X, X_1, X_2, etc., remplacent les noms des utilisateurs; le symbole I remplace une information quelconque.	

SECTION 2 – AUTHENTIFICATION SIMPLE

6 Procédure d'authentification simple

L'authentification simple vise à fournir une autorisation locale reposant sur un nom distinctif d'utilisateur, sur un mot de passe faisant l'objet (facultativement) d'un accord bilatéral et sur un accord bilatéral quant aux modalités d'emploi et de traitement de ce mot de passe dans un domaine donné. L'utilisation de l'authentification simple est essentiellement destinée à l'emploi local, c'est-à-dire pour authentification d'entités homologues entre un agent DUA et un agent DSA. L'authentification simple peut être réalisée de plusieurs manières:

a) transfert du nom distinctif et du mot de passe (facultatif) de l'utilisateur en clair (sans protection) au destinataire pour évaluation;

b) transfert du nom distinctif de l'utilisateur, du mot de passe de l'utilisateur et d'un numéro aléatoire et/ou d'une indication horaire, qui sont tous protégés par application d'une fonction à une voie;

c) transfert de l'information protégée décrite en b) ainsi que d'un numéro aléatoire et (ou) d'une indication horaire, qui sont tous protégés par application d'une fonction à une voie.

NOTE 1 – Il n'est pas exigé que les fonctions à une voie appliquées soient différentes.

NOTE 2 – La signalisation des procédures de protection des mots de passe pourra faire l'objet d'une extension de la présente Recommandation | Norme internationale.

Quand les mots de passe ne sont pas protégés, un niveau de sécurité minimal est assuré pour empêcher un accès non autorisé. Ce niveau ne doit pas être considéré comme la base de services sûrs. La protection du nom distinctif et du mot de passe de l'utilisateur assure une plus grande sécurité. Les algorithmes à utiliser pour le mécanisme de protection sont en général des fonctions à une voie sans chiffrement, qui sont très simples à mettre en œuvre.

La Figure 1 montre la procédure générale à appliquer pour obtenir une authentification simple.

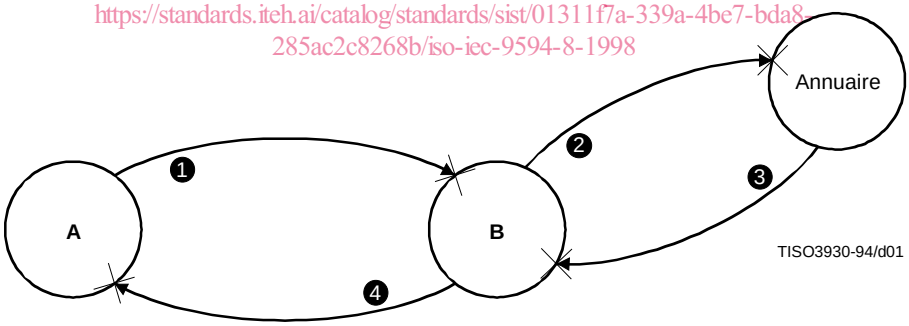

Figure 1 – Procédure d'authentification simple sans protection

Les étapes de cette procédure sont les suivantes:

1) un expéditeur A envoie son nom distinctif et son mot de passe à un destinataire B;

2) B envoie le nom distinctif visé et le mot de passe de A à l'Annuaire, où le mot de passe est comparé avec celui qui est contenu en tant qu'attribut **UserPassword** dans l'entrée d'annuaire concernant A (au moyen de l'opération Compare de l'Annuaire);

3) l'Annuaire confirme (ou infirme) à B que les habilitations sont valides;

4) le succès (ou l'échec) de l'authentification est communiqué à A.

La forme fondamentale d'authentification simple ne comporte que l'étape 1); elle peut aussi comporter l'étape 4) après que B a vérifié le nom distinctif et le mot de passe.