NORME INTERNATIONALE

ISO/CEI 9594-8

Deuxième édition
1995-09-15

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO/IEC 9594-8:1995
https://standards.iteh.ai/catalog/standards/sist/cf/cee9d-08d4-4c6c-84a0-cd2e6b1e45be/iso-iec-9594-8-1995

Numéro de référence
ISO/CEI 9594-8:1995(F)

Sommaire

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 9594-8:1995
https://standards.iteh.ai/catalog/standards/sist/cf7cee9d-08d4-4c6c-84a0-cd2e6b1e45bc/iso-iec-9594-8-1995

© ISO/CEI 1995

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

ISO/CEI Copyright Office • Case postale 56 • CH-1211 Genève 20 • Suisse

Version française tirée en 1996

Imprimé en Suisse

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 9594-8:1995
https://standards.iteh.ai/catalog/standards/sist/cf7cee9d-08d4-4c6c-84a0-cd2e6b1e45be/iso-iec-9594-8-1995

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment ensemble un système consacré à la normalisation internationale considérée comme un tout. 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 différents 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 ou 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 projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour approbation, avant leur acceptation comme Normes internationales. Les Normes internationales sont approuvées conformément aux procédures qui requièrent l'approbation de 75 % au moins des organismes nationaux votants.

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 21, *Interconnexion des systèmes ouverts, gestion des données et traitement distribué ouvert,* en collaboration avec l'IUT-T. Le texte identique est publié en tant que Recommandation IUT-T X.509.

Il convient que les personnes mettant en application la présente partie de l'ISO/CEI 9594 notent qu'il existe un processus de résolution de défaut et que des corrections peuvent être appliquées au présent texte sous forme de rectificatifs techniques. Une liste des rectificatifs techniques approuvés pour la présente partie de l'ISO/CEI 9594 peut être obtenue auprès du secrétariat du sous-comité. Les rectificatifs techniques publiés sont disponibles auprès de votre organisation nationale de normalisation.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 9594-8:1995
https://standards.iteh.ai/catalog/standards/sist/cf7cee9d-08d4-4c6c-84a0-cd2e6b1e45be/iso-iec-9594-8-1995

Cette deuxième édition révise et améliore techniquement l'ISO/CEI 9594-8:1990. Elle incorpore également le Rectificatif technique 1:1991. Les mises en application peuvent encore se réclamer en conformité avec la première édition de la présente partie de l'ISO/CEI 9594. Toutefois, il arrivera un moment où la première édition n'aura plus de raison d'être (c'est-à-dire que les défauts détectés ne seront plus résolus). Il est recommandé que les mises en application soient conformes à cette deuxième édition le plus tôt possible.

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: Vue d'ensemble des concepts, modèles et services*

— *Partie 2: Modèles*

— *Partie 3: Définitions de service abstrait*

— *Partie 4: Procédures pour le fonctionnement réparti*

— *Partie 5: Spécifications du protocole*

— *Partie 6: Types d'attributs sélectionnés*

— *Partie 7: Classes d'objets sélectionnés*

— *Partie 8: Cadre d'authentification*

— *Partie 9: Duplication*

L'annexe A fait partie intégrante de la présente partie de l'ISO/CEI 9594. Les annexes B à J sont données uniquement à titre d'information.

Introduction

La présente Recommandation | Norme internationale a été élaborée, de concert avec les 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 ces systèmes, avec les informations d'annuaire qu'ils contiennent, peut être considéré comme un tout intégré, appelé l'*Annuaire*. Les informations contenues dans l'Annuaire, appelées collectivement base d'informations d'Annuaire (DIB) sont généralement utilisées pour faciliter la communication entre des objets tels que entités d'application, individus, terminaux, listes de distribution, ainsi que les communications avec ces objets ou au sujet de ces objets.

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; et
- d'âges différents.

Un grand nombre d'applications comportent des exigences 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 menaces généralement connues ainsi que les services et les mécanismes de sécurité qu'on peut utiliser pour la protection contre ces dernières. En fin de compte, 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

La présente Recommandation | Norme internationale définit un cadre d'authentification pour assurer la prestation des services d'authentification par l'Annuaire à ses utilisateurs. Ces utilisateurs comprennent l'Annuaire lui-même ainsi que d'autres applications et services. L'Annuaire peut utilement contribuer à répondre à leurs besoins en authentification et en d'autres services de sécurité car c'est un emplacement naturel à partir duquel les parties en communication peuvent obtenir l'information d'authentification des uns et des autres: connaissance sur laquelle repose l'authentification. L'Annuaire est l'emplacement naturel du fait qu'il détient d'autres informations qui sont nécessaires à la communication et qui sont obtenues avant l'établissement de la communication. L'obtention de l'information d'authentification d'un partenaire d'une communication potentielle à partir de l'Annuaire est, avec cette approche, semblable à l'obtention d'une adresse. En raison du domaine étendu recouvert par l'Annuaire, on prévoit que ce cadre d'authentification sera très utilisé par toute une gamme d'applications.

Cette seconde édition révise techniquement et améliore, mais ne remplace pas, la première édition de la présente Recommandation | Norme internationale. Les mises en œuvre peuvent encore prétendre à la conformité à la première édition.

Cette seconde édition spécifie la version 1 des protocoles et services de l'Annuaire. La première édition spécifie également version 1. On a traité les différences entre les services et les protocoles définis dans les deux éditions en utilisant les règles d'extensibilité définies dans la présente version de la Rec. X.519 | ISO/CEI 9594-5.

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 exigences 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 RSA cryptographique de clé publique.

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

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 de consignation.

L'Annexe J, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, recense les modifications et les rapports de défaut qui ont été incorporés dans cette édition de la présente Recommandation | Norme internationale.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 9594-8:1995
https://standards.iteh.ai/catalog/standards/sist/cf7cee9d-08d4-4c6c-84a0-cd2e6b1e45be/iso-iec-9594-8-1995

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION — INTERCONNEXION DE SYSTÈMES OUVERTS (OSI) — L'ANNUAIRE: CADRE D'AUTHENTIFICATION

SECTION 1 – CONSIDÉRATIONS GÉNÉRALES

1 Domaine d'application

La présente Spécification | Norme internationale:

- spécifie la forme sous laquelle l'information d'authentification est conservée par l'Annuaire;
- décrit la façon dont on peut obtenir de l'Annuaire cette information d'authentification;
- établit les hypothèses faites au sujet de la manière dont est constituée cette information d'authentification et de son emplacement dans l'Annuaire;
- définit trois manières dont les applications peuvent employer cette information d'authentification pour effectuer des authentifications et explique comment d'autres services de sécurité peuvent être assurés par l'authentification.

La présente Recommandation | Norme internationale contient les descriptions de deux niveaux d'authentification: l'authentification simple qui utilise un mot de passe pour la vérification de l'identité et l'authentification poussée qui fait intervenir des accréditations 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 poussée devra servir de base à la prestation de services sûrs. Il ne s'agit pas ici d'établir un cadre général d'authentification. Celui-ci peut toutefois se prêter à une utilisation générale pour des applications qui jugent que ces techniques sont appropriées.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 9594-8:1995
https://standards.iteh.ai/catalog/standards/sist/cf7ee9d-08d4-4cbc-84a0-ed2e6b1e45be/iso-iec-9594-8-1995

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 particulière. Il appartient aux utilisateurs de cette application de définir leur propre politique de sécurité qui peut dépendre des services fournis par une norme.

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

La méthode d'authentification poussée 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 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 sont mis en place dans l'Annuaire par leur créateur. La génération de certificats d'utilisateur est effectuée par une autorité de certification autonome qui est complètement distincte des 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 en 7.1. 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 des 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 hachage [voir 3.3 f)] (utilisée pour former des accréditations et des jetons d'authentification). De nouveau, en principe, on peut utiliser un certain nombre de variantes de fonction hachage au prix d'un rétrécissement des communautés des 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 I 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 I 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 I Normes internationales identiques

- Recommandation UIT-T X.500 (1993) I ISO/CEI 9594-1:1995, *Technologie de l'information – Interconnexion des systèmes ouverts – L'Annuaire: Vue d'ensemble des concepts, modèles et services.*
- Recommandation UIT-T X.501 (1993) I ISO/CEI 9594-2:1995, *Technologie de l'information – Interconnexion des systèmes ouverts – L'Annuaire: Les modèles.*
- Recommandation UIT-T X.511 (1993) I ISO/CEI 9594-3:1995, *Technologie de l'information – Interconnexion des systèmes ouverts – L'Annuaire: Définition du service abstrait.*
- Recommandation UIT-T X.518 (1993) I ISO/CEI 9594-4:1995, *Technologie de l'information – Interconnexion des systèmes ouverts – L'Annuaire: Procédures pour le fonctionnement réparti.*
- Recommandation UIT-T X.519 (1993) I ISO/CEI 9594-5:1995, *Technologie de l'information – Interconnexion des systèmes ouverts – L'Annuaire: Spécifications du protocole.*
- Recommandation UIT-T X.520 (1993) I ISO/CEI 9594-6:1995, *Technologie de l'information – Interconnexion des systèmes ouverts – L'Annuaire: Types d'attributs sélectionnés.*
- Recommandation UIT-T X.521 (1993) I ISO/CEI 9594-7:1995, *Technologie de l'information – Interconnexion des systèmes ouverts – L'Annuaire: Classes d'objets sélectionnées.*
- Recommandation UIT-T X.525 (1993) I ISO/CEI 9594-9:1995, *Technologie de l'information – Interconnexion des systèmes ouverts – L'Annuaire: Duplication.*
- Recommandation UIT-T X.680 (1994) I ISO/CEI 8824-1:1995, *Technologie de l'information – Interconnexion des systèmes ouverts – Notation de syntaxe abstraite numéro un: Spécification de la notation de base.*
- Recommandation UIT-T X.681 (1994) I ISO/CEI 8824-2:1995, *Technologie de l'information – Interconnexion des systèmes ouverts – Notation de syntaxe abstraite numéro un: Spécification des objets informationnels.*
- Recommandation UIT-T X.682 (1994) I ISO/CEI 8824-3:1995, *Technologie de l'information – Interconnexion des systèmes ouverts – Notation de syntaxe abstraite numéro un: Spécification des contraintes.*
- Recommandation UIT-T X.683 (1994) I ISO/CEI 8824-4:1995, *Technologie de l'information – Interconnexion des systèmes ouverts – Notation de syntaxe abstraite numéro un: Paramétrage des spécifications de la notation de syntaxe abstraite nº 1.*
- Recommandation UIT-T X.690 (1994) I ISO/CEI 8825-1:1995, *Technologie de l'information – Interconnexion des systèmes ouverts – Règles de codage de l'ASN.1: Spécification des règles de codage de base, des règles de codage canoniques et des règles de codage distinctives.*
- Recommandation UIT-T X.880 (1994) I ISO/CEI 13712-1:1995, *Technologie de l'information – Opérations distantes: Concepts, modèle et notations.*
- Recommandation UIT-T X.881 (1994) I ISO/CEI 13712-2:1995, *Technologie de l'information – Opérations distantes: Réalisation OSI – Définition du service de l'élément de service d'opérations distantes.*

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

- Recommandation UIT-T 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.*

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 9594-8:1995
https://standards.iteh.ai/catalog/standards/sist/7...8...
cd2e6b1e45be/iso-iec-9594-8-1995

3 Définitions

Pour les besoins de la présente Recommandation I 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 I ISO 7498-2:

a) *asymétrique (chiffrement)*;

b) *échange d'authentifications*;

c) *information d'authentification*;

d) *confidentialité*;

e) *justificatif d'identité*;

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)*.

3.2 Définitions relatives au modèle d'Annuaire

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

a) *attribut*;

b) *base d'informations d'Annuaire*;

ISO/IEC 9594-8:1995
https://standards.iteh.ai/catalog/standards/sist/cf7cee9d-08d4-4c6c-84a0-ad2b6b1e45be/iso-iec-9594-8-1995

c) *arbre d'informations d'Annuaire*;

d) *agent de système d'Annuaire*;

e) *agent d'utilisateur d'Annuaire*;

f) *nom distintif*;

g) *entrée*;

h) *objet*;

i) *racine*.

3.3 Définitions relatives au cadre d'authentification

Les termes suivants sont définis dans la présente Recommandation I Norme internationale:

3.3.1 jeton d'authentification (jeton): Information acheminée au cours d'un échange d'authentifications, qui peut être utilisée à authentifier son expéditeur.

3.3.2 certificat d'utilisateur (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.

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

3.3.4 itinéraire de certification: Séquence ordonnée de certificats d'objets dans le DIT qui en plus de la clé publique de l'objet initial dans l'itinéraire, peut être traitée pour obtenir celle de l'objet final dans l'itinéraire.

3.3.5 système cryptographique: 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.

3.3.6 fonction hachage: Fonction (mathématique) qui met en correspondance les valeurs d'un grand (et éventuellement très grand) domaine avec une gamme 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 la gamme.

3.3.7 fonction à une voie: Fonction (mathématique) f qui est facile à calculer mais pour laquelle, à une valeur générale y de la gamme, 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.

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

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

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

3.3.11 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.

3.3.12 authentification poussée: Authentification obtenue au moyen d'accréditations déterminées par cryptographie.

3.3.13 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 certaine fonction particulière. Le rôle de confiance qui revient à la clé 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.

3.3.14 numéro de série de certificat: Valeur entière, unique pour la CA qui l'émet et associée sans ambiguïté au certificat émis par cette CA.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

4 Abréviations

ISO/IEC 9594-8:1995
https://standards.iteh.ai/catalog/standards/sist/cf7cee9d-08d4-4c6c-84a0-cd2e6b1e45be/iso-iec-9594-8-1995

Les abréviations suivantes sont utilisées dans la présente Recommandation | Norme internationale:

CA	Autorité de certification (*certification authority*)
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

Sauf exceptions mineures, 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, de mars 1993.

Le terme «Spécification d'Annuaire» (comme dans «la présente Spécification d'Annuaire») s'entend selon l'acception de la Rec. UIT-T X.509 | ISO/CEI 9594-8. Le terme «Spécifications d'Annuaire» s'entend selon l'acception des Recommandations de la série X.500 et de toutes les parties de l'ISO/CEI 9594.

Dans la présente Spécification d'Annuaire le terme «systèmes de l'édition 1988» désigne les systèmes conformes à l'édition précédente (1988), c'est-à-dire l'édition 1988 des Recommandations de la série X.500 du CCITT et ISO/CEI 9594: édition 1990. Pour les systèmes conformes aux Spécifications actuelles d'Annuaire on utilise le terme «systèmes de l'édition 1993».

Si, dans une liste, les points sont numérotés (au lieu d'utiliser des tirets ou des lettres), ils seront alors 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 I avec un sommaire chiffré attaché.
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 produit le suivant. Il est fonctionnellement équivalent au certificat suivant $X_1<<X_{n+1}>>$. 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.
$X_1p \bullet X_1<<X_2>>$	Opération de dévoilement d'un certificat (ou d'une chaîne de certificats) pour en extraire une clé publique. C'est un opérateur d'infixe, dont l'opérande de gauche est la clé publique d'une autorité de certification, et dont l'opérande de droite est un certificat délivré par cette autorité de certification. Le résultat est la clé publique de l'utilisateur dont le certificat est l'opérande de droite. 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	Itinéraire de certification de A en B composé d'une chaîne de certificats, débutant avec: $CA(A)<<CA^2(A)>>$ et finissant avec CA(B)<<B>>.
NOTE – Dans ce tableau, les symboles X, X_1, X_2, etc., remplacent les noms des usagers; le symbole I remplace toute information arbitraire.	

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 9594-8:1995
https://standards.iteh.ai/catalog/standards/sist/cf7cee9d-08d4-4c6c-84a0-cd2e6b1e45be/iso-iec-9594-8-1995

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, un mot de passe faisant l'objet (facultativement) d'un accord bilatéral et 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 DUA et un DSA. L'authentification simple peut être réalisée de plusieurs manières:

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

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

NOTES

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

2 La signalisation des procédures de protection des mots de passe pourra faire l'objet d'un complément au présent document.

Quand les mots de passe ne sont pas protégés, un niveau de sécurité minimal est assuré pour empêcher un accès non autorisé. Il ne doit pas être considéré comme la base de services sûrs. La protection du nom distinctif de l'utilisateur et du mot de passe assure une sécurité plus grande. 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.

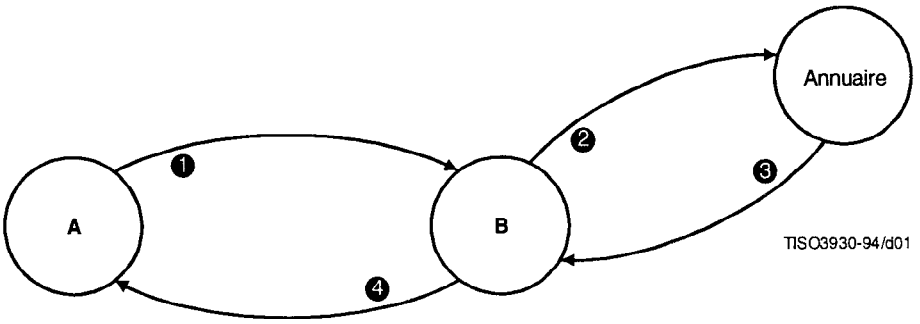


Figure 1 – Procédure d'authentification simple sans protection

Les étapes de cette procédure sont les suivantes:

1) un utilisateur expéditeur A envoie son nom distinctif et son mot de passe à un utilisateur 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 détenu en tant qu'attribut **UserPassword** dans l'entrée d'annuaire concernant A (en utilisant l'opération Compare de l'Annuaire);
3) l'Annuaire confirme (ou dément) à B que les accréditations sont valides;
4) le succès (ou l'échec) de l'authentification est communiqué à A.

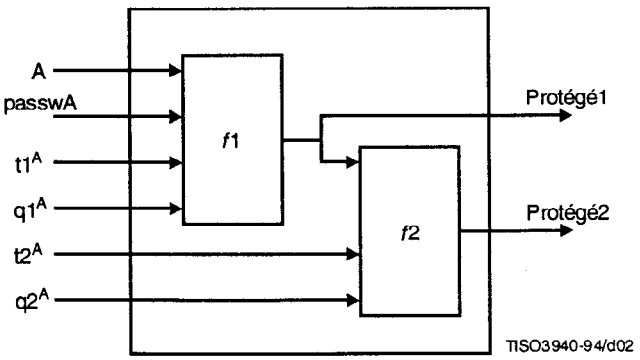
iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

ISO/IEC 9594-8:1995
https://standards.iteh.ai/catalog/standards/sist/cf7cee9d-08d4-4c6c-84a0-cd2e6b1e45be/iso-iec-9594-8-1995

6.1 Génération de l'information d'identification protégée

La Figure 2 montre deux méthodes de production d'une information d'identification protégée. $f1$ et $f2$ sont des fonctions à une voie (identiques ou différentes) et les indications horaires et les nombres aléatoires sont facultatifs et dépendent d'accords bilatéraux.



A	Nom distinctif de l'utilisateur
t^A	Indications horaires
$passw^A$	Mot de passe de A
q^A	Numéros aléatoires avec inclusion d'un compteur (facultatif)

Figure 2 – Authentification simple protégée

6.2 Procédure d'authentification simple protégée

La Figure 3 montre la procédure d'authentification simple protégée.

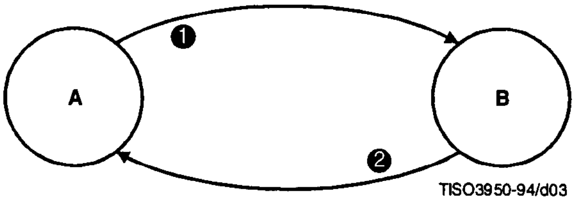


Figure 3 – Procédure d'authentification simple protégée

Cette procédure comporte les étapes suivantes (avec, initialement, utilisation de $f1$ seulement):

1) L'utilisateur d'origine (utilisateur A) envoie à l'utilisateur B son information d'identification protégée (Authenticator1). La protection est assurée par application de la fonction à une voie ($f1$) de la Figure 2, où l'indication horaire et (ou) le nombre aléatoire (s'il est utilisé) ont pour objet de réduire au minimum les répétitions et de cacher le mot de passe.

   La protection du mot de passe de A a la forme:

   Protected1 = $f1$ ($t1^A$, $q1^A$, A, passwA)

   L'information transmise à B prend la forme:

   Authenticator1 = $t1^A$, $q1^A$, A, Protected1

   B vérifie l'information d'identification protégée offerte par A en produisant une copie locale protégée du mot de passe de A (de la forme de Protected1) (au moyen du nom distinctif et, facultativement, d'une indication horaire et/ou d'un nombre aléatoire fourni par A, ainsi qu'une copie locale du mot de passe de A). B compare l'information d'identification visée (Protected1) avec la valeur produite localement, afin de s'assurer de leur égalité.

2) B confirme (ou dément) à A la vérification de l'information d'identification protégée.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 9594-8:1995
cd2e6b1e45be/iso-iec-9594-8-1995

La procédure peut être modifiée de manière à assurer une plus grande protection (au moyen de $f1$ et $f2$). Les principales différences sont les suivantes:

1) A envoie son information d'identification protégée supplémentaire (Authenticator2) à B. Une protection supplémentaire est obtenue en appliquant une autre fonction $f2$ comme le montre la Figure 2. La protection supplémentaire prend la forme:

   Protected2 = $f2$ ($t2^A$, $q2^A$, Protected1)

   L'information transmise à B prend la forme:

   Authenticator2 = $t1^A$, $t2^A$, $q1^A$, $q2^A$, A, Protected2

   Pour comparaison, B émet la valeur locale du mot de passe protégé additionnellement de A et la compare (pour en contrôler l'égalité) avec celle de Protected2 [le principe étant le même que pour l'étape 1) du 6.4.1].

2) B confirme (ou dément) à A la vérification de l'information d'identification protégée.

NOTE – Les procédures définies dans les présents articles sont spécifiées en fonction de A et B. Appliqué à l'Annuaire (spécifié dans les Rec. UIT-T X.511 | ISO/CEI 9594-3 et UIT-T X.518 | ISO/CEI 9594-4), A pourrait être un DUA lié à un DSA, B ou bien A pourrait être un DSA lié à un autre DSA, B.

6.3 Type d'attribut de mot de passe d'utilisateur

Un type d'attribut de mot de passe d'utilisateur contient le mot de passe d'un objet. Une valeur d'attribut pour le mot de passe de l'utilisateur est une chaîne spécifiée par l'objet.

```
userPassword           ATTRIBUTE  ::=    {
    WITH SYNTAX                          OCTET STRING (SIZE (0..ub-user-password))
    EQUALITY MATCHING RULE               octetStringMatch
    ID                                   id-at-userPassword }
```