NORME INTERNATIONALE

ISO/CEI 9594-8

Première édition
1990-12-15

Technologies de l'information — Interconnexion de systèmes ouverts — L'Annuaire —

Partie 8:
Cadre général d'authentification

Information technology — Open Systems Interconnection — The Directory —

Part 8: Authentication framework

Numéro de référence
ISO/CEI 9594-8:1990(F)

Version française tirée en 1991

Imprimé en Suisse

Sommaire

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 les 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 le titre général *Technologies de l'information — Interconnexion de systèmes ouverts — l'Annuaire*, l'ISO/CEI 9594 est composée des parties suivantes :

- *Partie 1 : Aperçu général des concepts, modèles et services*
- *Partie 2 : Modèles*
- *Partie 3 : Définition de service abstrait*
- *Partie 4 : Procédures d'exploitation répartie*
- *Partie 5 : Spécifications de protocoles*
- *Partie 6 : Types d'attribut sélectionnés*
- *Partie 7 : Classes d'objet sélectionnées*
- *Partie 8 : Cadre général d'authentification*

L'annexe G de la présente partie de l'ISO/CEI 9594 est normative. Les annexes A, B, C, D, E, F et H sont informatives.

Introduction

0.1 La présente partie de l'ISO/CEI 9594, ainsi que les autres parties ont été élaborées pour faciliter l'interconnexion de systèmes de traitement de l'information pour fournir des services d'Annuaire. L'ensemble de ces systèmes, ainsi que les informations d'Annuaire qu'ils détiennent, peuvent être considérés comme un tout intégré, appelé l'«Annuaire». Les informations détenues par l'Annuaire, appelées Base d'informations d'Annuaire (DIB), sont généralement utilisées pour faciliter la communication entre, avec ou sur des objets tels que entités d'application, individus, terminaux, listes de diffusion.

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

- provenant de divers fabricants ;
- gérés différemment ;
- de niveaux de complexité différents ; et
- d'âges différents.

0.3 Un grand nombre d'applications ont besoin de sécurité pour assurer une protection contre des menaces sur la communication des informations. L'annexe A décrit brièvement les menaces les plus courantes ainsi que les services et les mécanismes qui peuvent être utilisés pour assurer une protection contre ces menaces. En pratique tous les services de sécurité s'appuient sur l'authentification qui est le fait que l'identité des parties communicantes est connue de manière fiable.

0.4 La présente partie de l'ISO/CEI 9594 définit un cadre général pour la fourniture de services d'authentification par l'Annuaire à ses utilisateurs. Ces utilisateurs comprennent l'Annuaire lui-même aussi bien que d'autres applications et services. L'Annuaire peut utilement répondre aux besoins d'authentification et d'autres services de sécurité parce que c'est de là que les parties communicantes peuvent obtenir des informations d'authentification les unes sur les autres, ces informations étant la base de l'authentification. En effet, l'Annuaire détient d'autres informations nécessaires à la communication et obtenues avant que la communication ait lieu. L'obtention, à partir de l'Annuaire, d'informations d'authentification, relatives à un partenaire potentiel de la communication, ressemble à l'obtention d'une adresse. Grâce à la portée étendue de l'Annuaire, il est prévu que le cadre d'authentification, défini dans la présente partie de l'ISO/CEI 9594, soit largement utilisé par toute une gamme d'applications.

Technologies de l'information — Interconnexion de systèmes ouverts — L'Annuaire

Partie 8 :
Cadre général d'authentification

Section 1 : Généralités

1 Domaine d'application

1.1 La présente partie de l'ISO/CEI 9594 :

— spécifie le format des informations d'authentification détenues par l'Annuaire ;

— décrit comment peuvent être obtenues les informations d'authentification, à partir de l'Annuaire ;

— établit les hypothèses faites sur la façon dont les informations d'authentification sont formées et entrées dans l'Annuaire ;

— définit trois façons dont les applications peuvent utiliser ces informations d'authentification pour réaliser l'authentification et décrit comment d'autres services de sécurité peuvent être assurés par l'authentification.

1.2 La présente partie de l'ISO/CEI 9594 décrit deux niveaux d'authentification : l'authentification simple, fondée sur l'utilisation d'un mot de passe pour vérifier une identité déclarée ; et l'authentification forte, impliquant des justificatifs d'identité formés en utilisant des techniques de chiffrement. Alors que l'authentification simple assure une protection limitée contre l'accès non autorisé, seule l'authentification forte devrait servir de base à la fourniture de services de sécurité. Il n'est pas question de faire de ces techniques une règle générale pour réaliser l'authentification mais elles peuvent être utilisées par les applications qui les jugent appropriées.

1.3 L'authentification (ainsi que d'autres services de sécurité) ne peuvent être fournis que dans le contexte d'une politique de sécurité définie. Il appartient aux utilisateurs d'une application de définir leur propre politique de sécurité qui peut être limitée aux services définis par une norme.

1.4 Il appartient aux normes où sont définies des applications utilisant le cadre général d'authentification de spécifier les échanges de protocole à exécuter pour réaliser l'authentification fondée sur les informations d'authentification obtenues de l'Annuaire. Le protocole utilisé par les applications pour obtenir, de l'Annuaire, des justificatifs d'identité est le protocole d'accès à l'Annuaire (DAP) spécifié dans l'ISO/CEI 9594-5.

1.5 L'authentification forte définie dans la présente partie de l'ISO/CEI 9594 est fondée sur des systèmes de chiffrement à clé publique. L'avantage majeur de ces systèmes est que les certificats d'utilisateur peuvent être détenus dans l'Annuaire en tant qu'attributs pouvant être communiqués librement à l'intérieur du système d'Annuaire et livrés aux utilisateurs de l'Annuaire par les mêmes méthodes que d'autres informations d'Annuaire. Il est supposé que les certificats d'utilisateurs sont créés par des moyens externes et entrés dans l'Annuaire par leur créateur. La création des certificats est assurée par une autorité de certification qui est complètement indépendante des DSA de l'Annuaire. En particulier, rien n'est exigé des fournisseurs de l'Annuaire pour que le stockage et la communication des certificats d'utilisateurs soient sûrs. L'annexe B présente brièvement les systèmes de chiffrement à clé publique.

1.6 Le cadre général d'authentification n'impose pas l'utilisation d'un algorithme de chiffrement particulier, pourvu que celui qui est utilisé ait les propriétés décrites en 6.1. Plusieurs algorithmes différents peuvent être utilisés. Cependant deux utilisateurs souhaitant s'authentifier doivent adopter le même algorithme pour que l'authentification soit réalisée correctement. Ainsi, dans le contexte d'un ensemble d'applications, le choix d'un algorithme unique permettra d'élargir au maximum la communauté des utilisateurs capables de s'authentifier et de communiquer en toute sécurité. L'annexe C donne un exemple d'algorithme de chiffrement à clé publique.

1.7 De même, deux utilisateurs souhaitant s'authentifier doivent utiliser la même fonction de condensation (voir 3.3 f)) dans la formation de justificatifs d'identité et de jetons d'authentification. En principe, plusieurs fonctions de condensation différentes pourraient être utilisées au prix d'un rétrécissement de la communauté des utilisateurs capables de s'authentifier. L'annexe D présente brièvement les fonctions de condensation ainsi qu'un exemple de fonction de condensation.

2 Références normatives

Les normes suivantes contiennent des dispositions qui, par suite de la référence qui est en faite, constituent des dispositions valables pour la présente partie de l'ISO/CEI 9594. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute norme est sujette à révision et les parties prenantes des accords fondés sur la présente partie de l'ISO/CEI 9594 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur à un moment donné.

ISO 7498-2:1987, *Systèmes de traitement de l'information — Interconnexion de systèmes ouverts — Modèle de référence de base — Partie 2 : Architecture de sécurité.*

ISO/CEI 8824:1990, *Technologies de l'information — Interconnexion de systèmes ouverts — Spécification de la notation de syntaxe abstraite numéro 1 (ASN.1).*

ISO/CEI 8825:1990, *Technologies de l'information — Interconnexion de systèmes ouverts — Spécification des règles de codage de base pour la notation de syntaxe abstraite numéro 1 (ASN.1).*

ISO/CEI 10021-3:1990, *Technologies de l'information — Communication de texte — Systèmes d'échange de texte en mode message — Partie 3 : Conventions pour la définition de service abstrait.*

3 Définitions

3.1 La présente partie de l'ISO/CEI 9594 utilise les termes suivants, définis dans l'ISO 7498-2 :

a) chiffrement asymétrique ;

b) échange d'authentification ;

c) information d'authentification ;

d) confidentialité ;

e) justificatif d'identité ;

f) chiffrement ;

g) authentification de l'origine des données ;

h) déchiffrement ;

i) chiffrement ;

j) clé ;

k) mot de passe ;

l) authentification de l'entité homologue ;

m) chiffrement symétrique.

3.2 La présente partie de l'ISO/CEI 9594 utilise les termes suivants, définis dans l'ISO/CEI 9594-2 :

a) attribut ;

b) base d'informations d'Annuaire (DIB) ;

c) arbre d'informations d'Annuaire (DIT) ;

d) nom distinctif ;

e) entrée ;

f) objet ;

g) racine.

3.3 Dans le cadre de la présente partie de l'ISO/CEI 9594, les définitions suivantes sont également utilisées :

3.3.1 jeton d'authentification (jeton) : Informations véhiculées au cours d'un échange d'authentification forte et pouvant être utilisées pour authentifier l'expéditeur.

3.3.2 certificat d'utilisateur (certificat) : Clés publiques d'un utilisateur, avec d'autres informations, rendues infalsifiables par chiffrement avec la clé privée de l'autorité de certification qui émet le certificat.

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

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

3.3.5 système de chiffrement : Transformations de texte en clair en cryptogramme et vice-versa, la (les) transformation(s) particulière(s) à utiliser étant choisie(s) par des clés. Les transformations sont normalement définies par un algorithme mathématique.

3.3.6 fonction de condensation : Fonction mathématique qui met en correspondance des valeurs d'une plage très étendue avec celle d'une plage plus petite. Une bonne fonction de condensation est telle que les résultats de l'application de la fonction seront répartis sur la plage (apparemment de façon aléatoire).

3.3.7 fonction univoque : Fonction mathématique f facile à calculer mais, pour laquelle, il est difficile de trouver une valeur x telle que f(x) = y, y étant une valeur générale de la plage. Il peut y avoir très peu de valeurs y pour lesquelles il est aisé de calculer x.

3.3.8 clé publique : Dans un système de chiffrement à clé publique, la clé d'une paire de clés d'utilisateur qui est rendue publique.

3.3.9 clé privée (ou clé secrète) : Dans un système de chiffrement à clé publique, la clé d'une paire de clés d'utilisateur qui n'est connue que de l'utilisateur.

3.3.10 authentification simple : Authentification fondée sur des mots de passe simples.

3.3.11 politique de sécurité : Ensemble de règles établies par l'autorité de sécurité régissant l'utilisation et la fourniture de services et facilités de sécurité.

3.3.12 authentification forte : Authentification fondée sur des justificatifs d'identité déterminés par chiffrement.

3.3.13 confiance : Une entité fait confiance à une autre entité quand la première suppose que la seconde se comportera comme elle s'y attend. Cette confiance ne peut s'appliquer que pour quelques fonctions spécifiques. Dans le cadre général d'authentification, le rôle de la confiance est de décrire les relations entre une entité utilisant l'authentification et une autorité de certification ; une entité utilisant l'authentification doit être sûre que l'autorité de certification ne crée que des certificats valides et fiables.

3.3.14 numéro de série de certificat : Entier, unique à l'intérieur du domaine de l'autorité de certification qui l'émet, associé sans ambiguïté à un certificat émis par cette autorité de certification.

4 Notation et abréviations

4.1 Le tableau 1 définit la notation utilisée dans la présente partie de l'ISO/CEI 9594.

NOTE — Dans le tableau, les symboles X, X_1 et X_2 désignent des utilisateurs ; I désigne une information quelconque.

Tableau 1 — Notation

Notation	Signification
Xp	Clé publique d'un utilisateur X
Xs	Clé privée de X
Xp [I]	Chiffrement d'une information, I, en utilisant la clé publique de X
Xs [I]	Chiffrement de I en utilisant la clé privée de X
X{I}	Signature de I par X, se composant de I et d' un résumé 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 certificat (de longueur arbitraire) dont chaque élément est le certificat pour l'autorité de certification qui a produit le suivant. Il est équivalent au certificat X_1<<Xn+1>>. Par exemple, la possession de A<<B>>B<<C>> fournit la même capacité que A<<C>>, à savoir, la possibilité de trouver Cp, Ap étant donné.
X_1p . X_1 <<X_2>>	Opération de révélation d'un certificat (ou d'une chaîne de certificats) pour en extraire une clé publique. C'est un opérateur d'infixe dont l'opérande gauche est la clé publique d'une autorité de certification, et l'opérande droit est un certificat émis par cette autorité. Le résultat est la clé publique de l'utilisateur dont le certificat est l'opérande droit. Par exemple : Ap . A <<B>> B <<C>> indique les opérations d'après lesquelles la clé publique de B, Bp, est obtenue en utilisant la clé publique de A, à partir du certificat de B, le certificat de C est ensuite révélé en utilisant Bp. Le résultat de l'opération est la clé publique de C, Cp.
A → B	Chemin de certification allant de A à B, formé d''une chaîne de certificats, commençant par CA(A) <<CA^2(A)>> et se terminant par CA(B)<<B>>.

Section 2 : Authentification simple

5 Procédure d'authentification simple

5.1 L'authentification simple vise à fournir une autorisation locale fondée sur un nom distinctif d'utilisateur, un mot de passe accepté par accord bilatéral (en option) et une entente mutuelle sur les modalités d'emploi de ce mot de passe dans un domaine unique. L'utilisation de l'authentification simple est avant tout destinée à un usage local uniquement, c'est-à-dire à l'authentification de l'entité homologue entre un DUA et un DSA ou entre un DSA et un autre DSA. L'authentification simple peut être réalisée de diverses manières :

a) l'envoi au destinataire, qui les évalue, du nom distinctif de l'utilisateur et (en option) du mot de passe en clair (non protégé) ;

b) l'envoi du nom distinctif de l'utilisateur, du mot de passe, d'un numéro aléatoire et/ou d'une indication horaire, protégés par l'application d'une fonction univoque ;

c) l'envoi des informations définies en b) en même temps qu'un numéro aléatoire et/ou qu'une indication horaire, protégés par l'application d'une fonction univoque.

NOTES

1 Il n'est pas nécessaire que les fonctions univoques appliquées soient différentes.

2 Les procédures de protection des mots de passe peuvent faire l'objet d'additifs à la présente Norme internationale.

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

5.3 La figure 1 représente la procédure générale d'authentification simple.

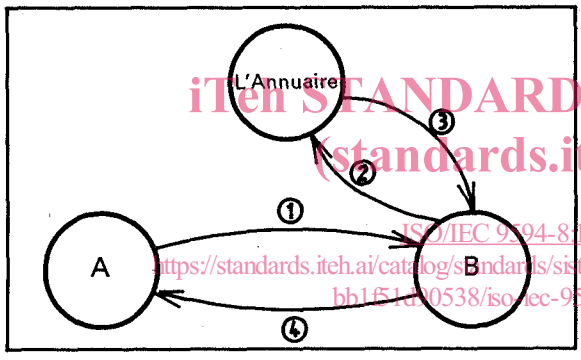


Figure 1 — Procédure d'authentification simple non protégée

5.3.1 La procédure comporte les étapes suivantes :

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

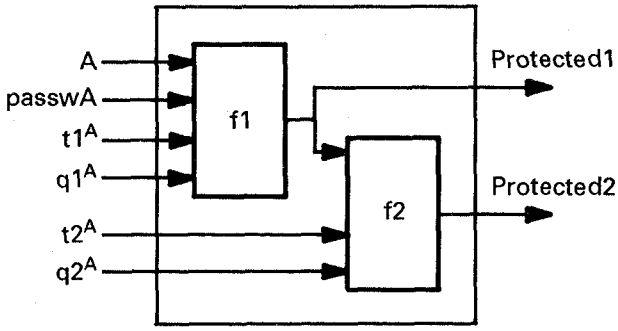
2) B envoie le nom distinctif et le mot de passe présentés à l'Annuaire où le mot de passe est comparé à celui détenu par l'Annuaire en tant qu'attribut UserPassword de l'entrée A (ceci est réalisé en utilisant l'opération d'Annuaire Compare) ;

3) l'Annuaire confirme (ou infirme) à B que le justificatif d'identité est valide ;

4) le résultat de l'authentification (succès ou échec) peut être transmis à A.

5.3.2 La forme d'authentification simple la plus élémentaire ne comprend que l'étape 1) et peut inclure l'étape 4) après que B ait vérifié le nom distinctif et le mot de passe.

5.4 La figure 2 montre deux manières de produire des informations d'identification protégées. f1 et f2 sont des fonctions univoques (identiques ou différentes) ; les indications horaires et les numéros aléatoires sont optionnels et font l'objet d'accords bilatéraux.



Légende

A = nom distinctif d'utilisateur
t^A = indications horaires
passwA = mot de passe de A
q^A = numéros aléatoires, avec (en option) un compteur

Figure 2 — Authentification simple protégée

5.4.1 La figure 3 montre la procédure d'authentification simple protégée.

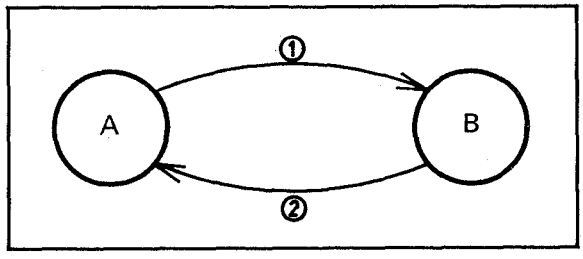


Figure 3 — Procédure d'authentification simple protégée

La procédure comporte les étapes suivantes :

1) un expéditeur A envoie ses informations protégées (Authenticator1) à B. La protection est obtenue en appliquant la fonction (f1) de la figure 2, où l'indication horaire et/ou le numéro aléatoire sont utilisés (s'ils le sont) pour minimiser le risque de rejouer et pour cacher le mot de passe.

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

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

Les informations envoyées à B ont la forme :

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

B vérifie les informations d'identification protégées envoyées par A en produisant une copie protégée locale du mot de passe de A (ayant la forme Protected1) ; ceci est réalisé en utilisant le nom distinctif, une indication horaire et/ou un numéro aléatoire fournis par A, en même temps qu'une copie locale du mot de passe de A. B compare les informations d'identification présentées (Protected1) aux valeurs produites localement ;

2) B confirme ou infirme à A la vérification des informations d'identification protégées.

5.4.2 La procédure décrite en 5.4.1 peut être modifiée pour offrir une plus grande protection en utilisant f1 et f2. Les principales différences sont :

1) A envoie à B ses informations d'identification protégées supplémentaires (Authenticator2). La protection supplémentaire est réalisée en utilisant une autre fonction, f2, comme le montre la figure 2. La protection a la forme :

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

Les informations envoyées à B ont la forme :

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

B produit une valeur locale du mot de passe protégé supplémentaire de A et le compare à celui de Protected2 (comme dans l'étape 1 de 5.4.1) ;

2) B confirme ou infirme à A la vérification des informations d'identification protégées.

NOTE — Les procédures définies dans les paragraphes précédents utilisent les termes A et B. Appliquées à l'Annuaire (voir ISO/CEI 9594-3 et ISO/CEI 9594-4), A pourrait être un DUA lié à un DSA, B ; autre possibilité, A pourrait être un DSA lié à un autre DSA, B.

5.5 Un type d'attribut UserPassword contient le mot de passe d'un objet. La valeur d'attribut est une chaîne de caractères définie par l'objet.

```
UserPassword ::=    ATTRIBUTE
                    WITH ATTRIBUTE-SYNTAX
                    OCTET STRING (SIZE (0..ub-user-password))
                    MATCHES FOR EQUALITY
```


5.6 La macro ASN.1 suivante peut être utilisée pour définir le type de données obtenu par l'application d'une fonction univoque à un autre type de données :


```
PROTECTED MACRO ::= SIGNATURE
```

Section 3 : Authentification forte

6 Principes de base de l'authentification forte

6.1 L'authentification forte est abordée dans la présente partie de l'ISO/CEI 9594 en utilisant les propriétés des systèmes de chiffrement à clé publique (PKCS). Ces systèmes, également décrits comme asymétriques, font intervenir une paire de clés, une clé privée et une clé publique, au lieu d'une seule clé comme c'est le cas dans les systèmes de chiffrement classiques. L'annexe B présente brièvement ces systèmes de chiffrement et les propriétés qui les rendent utiles pour l'authentification. Pour qu'un PKCS soit utilisable dans ce cadre général d'authentification, les deux clés doivent pouvoir être utilisées pour le chiffrement, la clé privée étant utilisée pour déchiffrer si la clé publique a été utilisée et la clé publique étant utilisée si la clé privée a été utilisée. En d'autres termes, Xp . Xs = Xs . Xp, avec Xp/Xs étant des fonctions de chiffrement/déchiffrement utilisant les clés publique et privée de l'utilisateur X.

NOTE — D'autres types de PKCS pourraient faire l'objet d'additifs à la présente partie de l'ISO/CEI 9594 ; c'est-à-dire, des PKCS n'exigeant pas la propriété de permutabilité et qui peuvent être pris en charge sans que la présente partie de l'ISO/CEI 9594 soit beaucoup modifiée.

6.2 Le cadre général d'authentification défini dans la présente partie de l'ISO/CEI 9594 n'impose pas l'utilisation d'un système de chiffrement particulier. Ce cadre général vise à être applicable à tout système de chiffrement à clé publique approprié et à intégrer les modifications apportées aux méthodes résultant du progrès des techniques mathématiques ou des capacités des ordinateurs. Cependant, deux utilisateurs souhaitant s'authentifier doivent choisir le même algorithme de chiffrement pour que l'authentification soit réalisée correctement.