NORME INTERNATIONALE

ISO/CEI 9798-1

Première édition
1991-09-01

Technologies de l'information — Techniques de sécurité — Mécanismes d'authentification d'entité —

Partie 1: Modèle général

ISO/IEC 9798-3:1993
https://standards.iteh.ai/catalog/standards/sist/a2ca8400-58c0-4a5d-a61d-cd0e194f685b/iso-iec-9798-3-1993

Information technology — Security techniques — Entity authentication mechanisms —
Part 1: General model

Numéro de référence
ISO/CEI 9798-1:1991(F)

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 des 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 9798-1 a été élaborée par le comité technique ISO/CEI JTC 1, *Technologies de l'information.*

L'ISO/CEI 9798 comprend les parties suivantes présentées sous le titre général *Technologies de l'information — Techniques de sécurité — Mécanismes d'authentification d'entité :*

— *Partie 1 : Modèle général*

— *Partie 2 : Authentification d'entité utilisant les techniques symétriques*

— *Partie 3 : Authentification d'entité utilisant un algorithme à clé publique*

L'annexe A de la présente partie de l'ISO/CEI 9798 est donnée uniquement à titre d'information.

Introduction

Les mécanismes d'authentification d'entité permettent la vérification de l'identité déclarée par une entité, par une autre entité.

L'authenticité de l'entité ne peut être assurée que pendant la durée de l'échange d'authentification. Pour garantir l'authenticité de données communiquées par la suite, l'échange d'authentification doit être utilisé conjointement avec un moyen de communication sûr (par exemple un service d'intégrité).

Un usurpateur d'identité peut rejouer, à une date ultérieure, un échange d'authentification valide (il s'agit là d'une forme d'imposture). Pour éviter un tel rejeu, on peut utiliser un paramètre variable dans le temps comme par exemple un dateur, un numéro d'ordre ou une question (challenge).

En règle générale, à des fins d'authentification les entités génèrent et échangent des messages normalisés appelés jetons. Il faut procéder à l'échange d'au moins un jeton pour que l'une des entités soit authentifiée par l'autre entité et l'échange d'au moins deux jetons pour une authentification réciproque. Un jeton supplémentaire peut s'avérer nécessaire dans le cas où une question (challenge) doit être envoyée pour engager l'échange d'authentification. L'authentification unilatérale offre à une entité l'assurance de l'identité de l'autre entité mais l'inverse n'est pas vrai. L'authentification mutuelle fournit à chacune des deux entités l'assurance de l'identité de l'autre.

Technologies de l'information — Techniques de sécurité — Mécanismes d'authentification d'entité —

Partie 1 : Modèle général

1 Domaine d'application

La présente partie de l'ISO/CEI 9798 spécifie les mécanismes d'authentification d'entité qui utilisent des techniques de sécurité. Ces mécanismes sont employés pour corroborer qu'une entité est bien celle qu'elle déclare être. Une entité à authentifier prouve son identité en montrant qu'elle connaît un secret. Les mécanismes sont définis par des échanges d'information entre entités et, dans les cas où cela s'avère nécessaire, par des échanges avec une tierce partie de confiance.

Les détails des mécanismes et le contenu des échanges d'authentification ne sont pas spécifiés dans la présente partie de l'ISO/CEI 9798 mais dans les parties suivantes de cette norme multi-parties.

2 Références normatives

Les normes suivantes contiennent des dispositions qui, par suite de la référence qui en est faite, constituent des dispositions valables pour la présente partie de l'ISO/CEI 9798. 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 9798 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 7498-2:1989, *Systèmes de traitement de l'information — Interconnexion de systèmes ouverts — Modèle de référence de base — Partie 2 : Architecture de sécurité.*

ISO/CEI 9594-8:1990, *Technologies de l'information — Interconnexion de systèmes ouverts — L'Annuaire — Partie 8 : Cadre général d'authentification.*

3 Définitions

3.1 La présente partie de l'ISO/CEI 9798 utilise les termes généraux suivants relatifs à la sécurité tels que définis dans la norme ISO 7498-2.

3.1.1 justificatifs d'identité.

3.1.2 clé.

3.1.3 signature.

3.2 La présente partie de l'ISO/CEI 9798 utilise les termes généraux suivants relatifs à la sécurité tels que définis dans la norme ISO/CEI 9594-8.

3.2.1 certificat utilisateur (certificat) (définition ASN.1 à inclure).

3.3 Pour les besoins de la présente partie de l'ISO/CEI 9798, les définitions suivantes s'appliquent.

3.3.1 initiateur d'authentification : Entité qui engage l'échange d'authentification.

3.3.2 répondeur d'authentification : Entité qui répond à l'initiateur de l'échange d'authentification.

3.3.3 identificateur distinctif : Information qui distingue une entité sans ambiguïté dans le processus d'authentification.

3.3.4 authentification d'entité : Confirmation qu'une entité est bien celle qu'elle déclare être.

3.3.5 paramètre variable dans le temps : Élément de donnée utilisé par une entité pour vérifier qu'un message n'est pas un rejeu.

3.3.6 jeton (échange *AI*) : Information d'authentification de l'échange transportée durant l'échange d'authentification.

3.4 La présente partie de l'ISO/CEI 9798 utilise les termes généraux suivants relatifs à la sécurité tels que définis dans la norme ISO/CEI 10181-2.

3.4.1 déclarant : Entité qui est ou qui représente une entité principale à des fins d'authentification, ainsi que les fonctions qu'implique un échange d'authentification au nom de cette entité. Un déclarant dispose des fonctions nécessaires pour s'engager dans des échanges d'authentification au nom d'une entité principale.

3.4.2 échange AI : Information échangée entre le déclarant et le vérificateur au cours du processus d'authentification de l'entité principale.

3.4.3 entité principale : Entité dont l'identité peut être authentifiée.

3.4.4 tierce partie de confiance : Autorité de sécurité, ou son agent, à laquelle d'autres entités accordent leur confiance en matière d'activités relatives à la sécurité. Dans le contexte de la présente Norme internationale, une tierce partie de confiance possède la confiance d'un déclarant et/ou d'un vérificateur à des fins d'authentification.

3.4.5 vérification AI : Information utilisée par le vérificateur pour vérifier une identité déclarée lors d'un échange *AI*.

3.4.6 vérificateur : Entité qui est ou qui représente l'entité réclamant une identité authentifiée. Un vérificateur dispose des fonctions nécessaires pour s'engager dans des échanges d'authentification.

4 Symboles

Les symboles suivants sont utilisés tout au long de la présente partie de l'ISO/CEI 9798 :

A est l'identificateur distinctif de l'entité *A*.

B est l'identificateur distinctif de l'entité *B*.

TP est l'identificateur distinctif de la tierce partie de confiance.

K_x est une clé secrète associée à l'entité *X*, utilisée uniquement dans les techniques cryptographiques symétriques.

P_x est une clé publique associée à l'entité *X*, utilisée uniquement dans les techniques cryptographiques asymétriques.

S_x est une clé secrète associée à l'entité *X*, utilisée uniquement dans les techniques cryptographiques asymétriques.

KID est un identificateur de clé.

N est un numéro d'ordre.

N_x est un numéro d'ordre fourni par l'entité *X*.

R est un aléa.

R_x est un aléa fourni par l'entité *X*.

T est un dateur.

T_x est un dateur fourni par l'entité *X*.

Y||*Z* est le résultat de la concaténation des éléments de données *Y* et *Z* dans cet ordre.

$eK_x(Z)$ est le résultat du chiffrement de la donnée *Z* avec un algorithme symétrique utilisant la clé K_x.

$dK_x(Z)$ est le résultat du déchiffrement de la donnée *Z* avec un algorithme symétrique utilisant la clé K_x.

$eK_{xy}(Z)$ est le résultat du chiffrement de la donnée *Z* avec une clé d'authentification symétrique K_{xy} partagée par les entités *X* et *Y*.

CredX sont les justificatifs d'identité de l'entité *X*.

CertX est le certificat d'une tierce partie de confiance pour l'entité *X*.

TokenXY est un jeton envoyé de l'entité *X* à l'entité *Y*.

$TokenXY_i$ est le ième jeton envoyé de l'entité *X* à l'entité *Y*.

TVP est un paramètre variable dans le temps.

$sS_x(Z)$ est la signature *Sig* de la donnée *Z* en utilisant la clé secrète S_x.

$vP_x(Sig)$ est le résultat du processus de vérification de la signature *Sig* en utilisant la clé publique de vérification P_x.

T_{exp} est la date et l'heure d'expiration des justificatifs d'identité.

5 Modèle d'authentification

Le modèle général des mécanismes d'authentification d'entité est décrit ci-dessous. Toutes les entités et tous les échanges ne doivent pas impérativement être présents dans chaque mécanisme d'authentification.

Concernant les protocoles d'authentification spécifiés dans les autres parties de la présente Norme internationale, dans le cas d'une authentification unilatérale, l'entité *A* est considérée être le déclarant tandis que l'entité *B* est considérée être le vérificateur. Dans le cas d'une authentification réciproque, les entités *A* et *B* jouent simultanément le rôle de déclarant et le rôle de vérificateur.

La tierce partie de confiance possède à la fois la confiance de l'entité *A* et celle de l'entité *B*.

Dans la figure 1 les lignes indiquent les flux d'information potentiels. Les entités *A* et *B* peuvent soit dialoguer directement avec la tierce partie de confiance, soit utiliser certaines informations fournies par la tierce partie de confiance.

Les détails des mécanismes d'authentification de la présente Norme internationale multiparties sont spécifiés dans les parties suivantes.

6 Exigences générales et contraintes

Pour qu'une entité puisse authentifier une autre entité, chacune d'elles doit utiliser un ensemble commun de techniques cryptographiques et de paramètres.

Au cours de la vie opérationnelle d'une clé, les valeurs de tous les paramètres variables dans le temps sur lesquels la clé agit (par exemple les dateurs et les numéros d'ordre) doivent être uniques.

Les identificateurs distinctifs des entités qui s'authentifient sont supposés être déjà disponibles ou avoir été fournis par d'autres moyens.

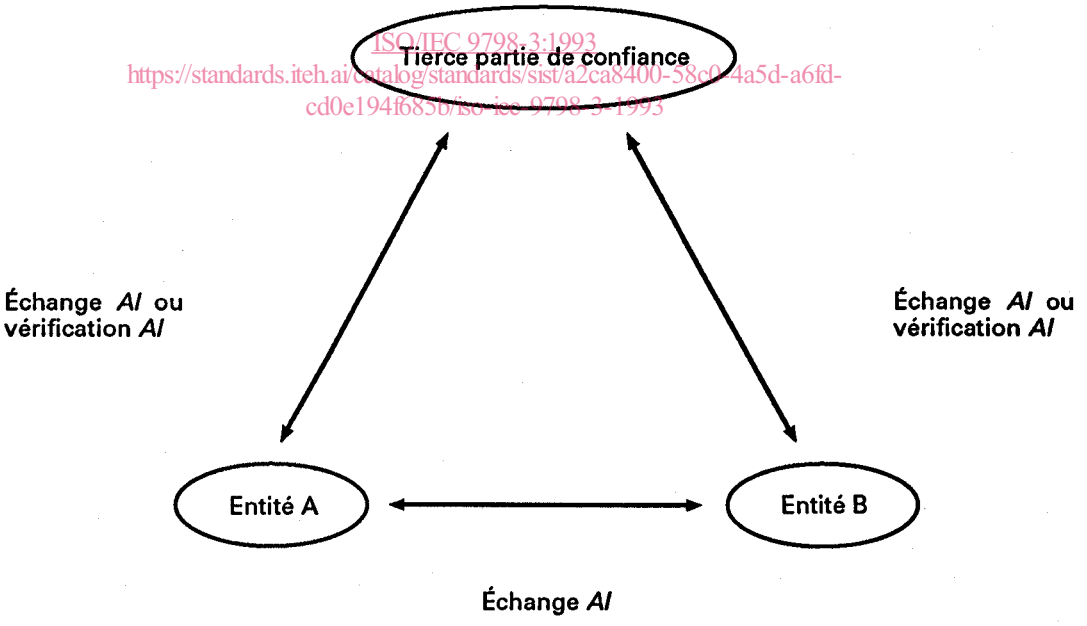

Figure 1 — Modèle d'authentification

Annexe A

(informative)

Bibliographie

[1] ISO 2382-8 : 1986, *Systèmes de taitement de l'information — Vocabulaire — Partie 08 : Contrôle, intégrité et sécurité.*

[2] ISO 2382-9 : 1984, *Traitement des données — Vocabulaire — Partie 09 : Communications des données.*

[3] ISO 7498 : 1984, *Systèmes de traitement de l'information — Interconnexion des systèmes ouverts — Modèle de référence de base.*

[4] ISO/CEI 9796 : — [1], *Technologies de l'information — Techniques de sécurité — Schéma de signature numérique rétablissant le message.*

[5] ISO/CEI 10181-1 : — [1], *Technologies de l'information — Interconnexion de systèmes ouverts — Cadres généraux pour la sécurité — Partie 1 : Aperçu général.*

[6] ISO/CEI 10181-2 : — [1], *Technologies de l'information — Interconnexion de systèmes ouverts — Cadres généraux pour la sécurité — Partie 2 : Cadre général d'authentification.*

1) À publier.