

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

*Information technology — Security techniques — Entity authentication
mechanisms —*

Part 1: General model



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

AVA Documents
Document Sharing Hub

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.

© ISO/CEI 1991

Droits de reproduction réservés. 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 1993

Imprimé en Suisse

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 jeu, 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.

