JTC 1

INTERNATIONAL STANDARD

ISO/IEC 9798-1

First edition
1991-09-01

Information technology — Security techniques — Entity authentication mechanisms —

Part 1:
General model

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

Partie 1: Modèle général

Reference number
ISO/IEC 9798-1:1991(E)

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 9798-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

ISO/IEC 9798 consists of the following parts, under the general title *Information technology — Security techniques — Entity authentication mechanisms*:

- *Part 1: General model*
- *Part 2: Entity authentication using symmetric techniques*
- *Part 3: Entity authentication using a public key algorithm*

Annex A of this part of ISO/IEC 9798 is for information only.

ISO/IEC Copyright Office • Case Postale 56 • CH-1211 Genève 20 • Switzerland
Printed in Switzerland

Introduction

Entity authentication mechanisms allow the verification, of an entity's claimed identity, by another entity.

The authenticity of the entity can be ascertained only for the instant of the authentication exchange. To guarantee the authenticity of subsequent communicated data, the authentication exchange must be used in conjunction with a secure means of communication (e.g. an integrity service).

An impersonator may replay, at a later date, a valid authentication exchange (this is a form of masquerade). To prevent such a replay, a time variant parameter, such as a time stamp, a sequence number, or a challenge may be used.

Generally, for authentication purposes, the entities generate and exchange standardized messages, called tokens. It takes at least the exchange of one token for one of the entities to be authenticated by the other entity and at least the exchange of two tokens for mutual authentication. An additional token may be needed, if a challenge has to be sent to initiate the authentication exchange. Unilateral authentication provides one entity with assurance of the other's identity but not vice versa. Mutual authentication provides both entities with assurance of each other's identity.

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

1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms which use security techniques. These mechanisms are used to corroborate that an entity is the one that is claimed. An entity to be authenticated proves its identity by showing its knowledge of a secret. The mechanisms are defined as exchanges of information between entities and, where required, exchanges with a trusted third party.

The details of the mechanisms and the contents of the authentication exchanges are not specified in this part of ISO/IEC 9798 but in the following parts of this multi-part International Standard.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9798. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 9798 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 7498-2 : 1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*

ISO/IEC 9594-8 : 1990, *Information technology – Open Systems Interconnection – The Directory – Part 8: Authentication framework.*

3 Definitions

3.1 This part of ISO/IEC 9798 makes use of the following general security-related terms defined in ISO 7498-2.

3.1.1 **credentials.**

3.1.2 **key.**

3.1.3 **signature.**

3.2 This part of ISO/IEC 9798 makes use of the following general security-related term defined in ISO/IEC 9594-8.

3.2.1 **user certificate** (certificate) (to include the ASN.1 definition).

3.3 For the purpose of this part of ISO/IEC 9798, the following definitions apply.

3.3.1 **authentication initiator:** The entity that initiates the authentication exchange.

3.3.2 **authentication responder:** The entity that responds to the initiator of the authentication exchange.

3.3.3 **distinguishing identifier:** Information which unambiguously distinguishes an entity in the authentication process.

3.3.4 **entity authentication:** The corroboration that an entity is the one claimed.

3.3.5 **time variant parameter:** A data item used by an entity to verify that a message is not a replay.

3.3.6 **token (exchange *AI*):** Exchange authentication information conveyed during an authentication exchange.

3.4 This part of ISO/IEC 9798 will make use of the following general security-related terms defined in ISO/IEC 10181-2.

3.4.1 **claimant:** An entity which is or represents a principal for the purposes of authentication, together with the functions involved in an authentication exchange on behalf of that entity. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

3.4.2 exchange authentication information (exchange *AI*): Information exchanged between the claimant and the verifier during the process of authenticating the principal.

3.4.3 principal: An entity whose identity can be authenticated.

3.4.4 trusted third party: A security authority, or its agent, trusted by other entities with respect to security-related activities. In the context of this International Standard, a trusted third party is trusted by a claimant and/or a verifier for the purposes of authentication.

3.4.5 verification authentication information (verification *AI*): Information used by the verifier to verify an identity claimed through exchange *AI*.

3.4.6 verifier: An entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.

4 Notation

Throughout this part of ISO/IEC 9798 the following notation is used:

A is the distinguishing identifier of entity A.

B is the distinguishing identifier of entity B.

TP is the distinguishing identifier of the trusted third party.

K_x is a secret key associated with entity X, used only in symmetric cryptographic techniques.

P_x is a public key associated with entity X, used only in asymmetric cryptographic techniques.

S_x is a secret key associated with entity X, used only in asymmetric cryptographic techniques.

KID is a key identifier.

N is a sequence number.

N_x is a sequence number issued by entity X.

R is a random number.

R_x is a random number issued by entity X.

T is a time stamp.

T_x is a time stamp issued by entity X.

$Y \| Z$ is the result of the concatenation of the data items Y and Z in that order.

$eK_x(Z)$ is the result of the encipherment of data Z with a symmetric algorithm using the key K_x.

$dK_x(Z)$ is the result of the decipherment of data Z with a symmetric algorithm using the key K_x.

$eK_{xy}(Z)$ is the result of the encipherment of data Z with a symmetric authentication key K_{xy}, shared between entities X and Y.

$CredX$ are the credentials of entity X.

$CertX$ is a trusted third party's certificate for entity X.

$TokenXY$ is a token sent from entity X to entity Y.

$TokenXY_i$ is the i th token sent from entity X to entity Y.

TVP is a time variant parameter.

$sS_x(Z)$ is the signature Sig of data Z using the secret key S_x.

$vP_x(Sig)$ is the result of the verification process of signature Sig using the public verification key P_x.

T_{exp} is the expiry date and time for credentials.

5 Authentication model

The general model for entity authentication mechanisms is shown below. It is not essential that all the entities and exchanges are present in every authentication mechanism.

For the authentication protocols specified in the other parts of this International Standard, for unilateral authentication, entity A is considered the claimant, whereas entity B is considered the verifier. For mutual authentication, A and B take at the same time, the role of the claimant and the role of the verifier.

The trusted third party is trusted by both entity *A* and entity *B*.

In figure 1 the lines indicate potential information flow. Entities *A* and *B* may either directly interact with the trusted third party, or use some information issued by the trusted third party.

The details of the authentication mechanisms of this multi – part International Standard are specified in the subsequent parts.

6 General requirements and constraints

In order that an entity can authenticate another entity, both shall use a common set of data cryptographic techniques and parameters.

During the operational life of a key, the values of all time – variant parameters on which the key operates (e.g. time stamps and sequence numbers) shall be unique.

It is assumed that the distinguishing identifiers of the authenticating entities are already available or have been delivered by some other means.

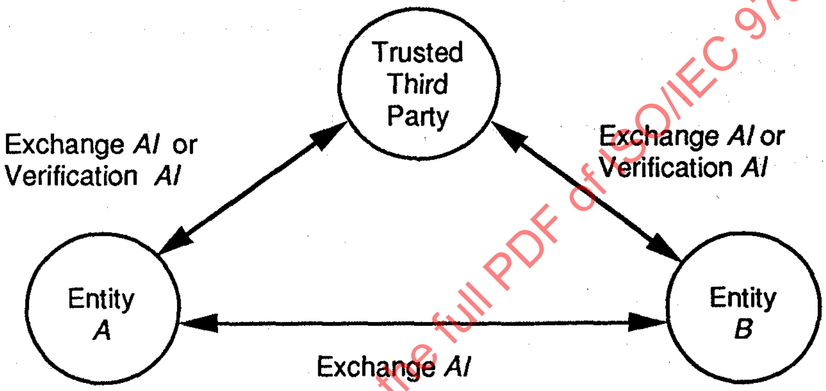
Trusted Third Party
Exchange *AI* or Verification *AI*
Exchange *AI* or Verification *AI*
Entity *A*
Entity *B*
Exchange *AI*

Figure 1 - Authentication model

Annex A
(informative)

Bibliography

[1] ISO 2382-8 : 1986, *Information processing systems – Vocabulary – Part 08: Control, integrity and security.*

[2] ISO 2382-9 : 1984, *Data processing – Vocabulary – Part 09: Data communication.*

[3] ISO 7498 : 1984, *Information processing systems – Open Systems Interconnection – Basic Reference Model.*

[4] ISO/IEC 9796 : – [1] *Information technology – Security techniques – Digital signature scheme giving message recovery.*

[5] ISO/IEC 10181-1 : – [1] *Information technology – Open Systems Interconnection – Security frameworks – Part 1: Frameworks overview.*

[6] ISO/IEC 10181-2 : –[1], *Information technology – Open Systems Interconnection – Security frameworks – Part 2: Authentication framework*

[1] To be published.