INTERNATIONAL
STANDARD

**ISO/IEC
9798-1**

Second edition
1997-08-01

Information technology — Security techniques — Entity authentication —

Part 1:
General

Technologies de l'information — Techniques de sécurité — Authentification d'entité —

Partie 1: Généralités

Reference number
ISO/IEC 9798-1:1997(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*, Subcommittee SC27, *IT Security techniques.*

This second edition cancels and replaces the first edition (ISO/IEC 9798-1:1991), which has been technically revised.

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

- *Part 3: Entity authentication using a public key algorithm*

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

- *Part 1: General*
- *Part 2: Mechanisms using symmetric encipherment algorithms*
- *Part 4: Mechanisms using a cryptographic check function*
- *Part 5: Mechanisms using asymmetric zero knowledge techniques*

> NOTE — The introductory element of the title of part 3 will be aligned with the introductory element of the titles of parts 1, 2, 4 and 5 at the next revision of part 3 of ISO/IEC 9798.

Further parts may follow.

Annexes A, B, C and D of this part of ISO/IEC 9798 are for information only.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Information technology — Security techniques — Entity authentication —

Part 1:
General

1 Scope

This part of ISO/IEC 9798 specifies an authentication model and general requirements and constraints for 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 subsequent parts.

Certain of the mechanisms specified in subsequent parts of ISO/IEC 9798 can be used to help provide non-repudiation services, mechanisms for which are specified in ISO/IEC 13888. The provision of non-repudiation services is beyond the scope of ISO/IEC 9798.

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: 1995, *Information technology — Open Systems Interconnection — The Directory — Part 8: Authentication framework.*

ISO/IEC 10181-2: 1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Authentication framework.*

ISO/IEC 13888-1 —[1]: *Information technology — Security techniques — Non-repudiation— Part 1: General.*

3 Definitions

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

3.1.1 cryptographic check value: information which is derived by performing a cryptographic transformation on the data unit.

3.1.2 masquerade: the pretence by an entity to be a different entity.

3.1.3 digital signature (signature): data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

3.2 ISO/IEC 9798 makes use of the following general security-related terms defined in ISO/IEC 10181-2:

3.2.1 claimant: an entity which is or represents a principal for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

3.2.2 principal: an entity whose identity can be authenticated.

[1] to be published