INTERNATIONAL STANDARD

ISO/IEC 9798-4

First edition
1995-03-15

Information technology — Security techniques — Entity authentication —

Part 4:
Mechanisms using a cryptographic check function

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

Partie 4: Mécanismes utilisant une fonction cryptographique de vérification

Reference number
ISO/IEC 9798-4:1995(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 9798-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Sub-Committee SC27, *IT Security techniques*.

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

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

NOTE — The introductory element of the titles of parts 1 and 3 will be aligned with the introductory element of the titles of parts 2,4 and 5 at the next revision of parts 1 and 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.

Information technology — Security techniques — Entity authentication — Part 4: Mechanisms using a cryptographic check function

1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms using a cryptographic check function. Two mechanisms are concerned with the authentication of a single entity (unilateral authentication), while the remaining are mechanisms for mutual authentication of two entities.

The mechanisms specified in this part of ISO/IEC 9798 use time variant parameters such as time stamps, sequence numbers, or random numbers, to prevent valid authentication information from being accepted at a later time.

If a time stamp or sequence number is used, one pass is needed for unilateral authentication, while two passes are needed to achieve mutual authentication. If a challenge and response method employing random numbers is used, two passes are needed for unilateral authentication, while three passes are required to achieve mutual authentication.

Examples of cryptographic check functions are given in annex C.

2 Normative reference

The following standard contains provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9798. At the time of publication, the edition indicated was 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 edition of the standard indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 9798-1: 1991, *Information technology — Security techniques — Entity authentication mechanisms — Part 1: General model.*

3 Definitions and notation

For the purposes of this part of ISO/IEC 9798, the definitions and notation described in ISO/IEC 9798-1 apply. In addition the following definition and notation are used:

3.1 cryptographic check value: Information which is derived by performing a cryptographic transformation on the data unit [ISO 7498-2].

3.2 $f_K(Z)$: Cryptographic check value which is the result of applying the cryptographic check function f using as input a secret key K and an arbitrary data string Z.

3.3 $\begin{matrix} T_A \\ N_A \end{matrix}$: Time variant parameter originated by entity A which is either a time stamp T_A or a sequence number N_A.

4 Requirements

In the authentication mechanisms specified in this part of ISO/IEC 9798 an entity to be authenticated corroborates its identity by demonstrating its knowledge of a secret authentication key. This is achieved by the entity using its secret key with a cryptographic check function applied to specific data to obtain a cryptographic check value. The cryptographic check value can be checked by anyone knowing the entity's secret authentication key who can re-calculate the cryptographic check value and compare it with the value received.

The authentication mechanisms have the following requirements. If any one of these is not met then the authentication process may be compromised or it cannot be implemented.

a) A claimant authenticating itself to a verifier shares a common secret authentication key with that verifier. This key shall be known to the involved entities prior