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

Part 2:

**Mechanisms using symmetric encipherment
algorithms**

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

Partie 2: Mécanismes utilisant des algorithmes de chiffrement symétriques



Contents

1 Scope 1

2 Normative references 1

3 Definitions and notation..... 1

4 Requirements 2

5 Mechanisms not involving a trusted third party..... 2

5.1 Unilateral authentication..... 2

5.1.1 One pass authentication 3

5.1.2 Two pass authentication 3

5.2 Mutual authentication..... 4

5.2.1 Two pass authentication..... 4

5.2.2 Three pass authentication 5

6 Mechanisms involving a trusted third party 6

6.1 Four pass authentication 6

6.2 Five pass authentication..... 7

Annex A (informative) Use of text fields 10

Bibliography 11

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 9798-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 9798-2:1994), which has been technically revised. Note, however, that implementations which comply with ISO/IEC 9798-2 (1st edition) will be compliant with ISO/IEC 9798-2 (2nd edition).

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 3: Mechanisms using digital signature techniques*
- *Part 4: Mechanisms using a cryptographic check function*
- *Part 5 : Mechanisms using zero knowledge techniques*

Further parts may follow.

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

Information technology — Security techniques — Entity authentication —

Part 2: Mechanisms using symmetric encipherment algorithms

1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms using symmetric encipherment algorithms. Four of the mechanisms provide entity authentication between two entities where no trusted third party is involved; two of these are mechanisms to unilaterally authenticate one entity to another, while the other two are mechanisms for mutual authentication of two entities. The remaining mechanisms require a trusted third party for the establishment of a common secret key, and realize mutual or unilateral entity authentication.

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 or more than once.

If no trusted third party is involved and 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 no trusted third party is involved and 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. If a trusted third party is involved, any additional communication between an entity and the trusted third party requires two extra passes in the communication exchange.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9798. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, 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 normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 9798-1:1997, *Information technology — Security techniques — Entity authentication — Part 1: General*.

ISO/IEC 11770-2:1996, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*.

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.