

Information technology — Security techniques — Entity authentication —

Part 2: Mechanisms using symmetric encipherment algorithms

ICS 35.040

National foreword

This British Standard reproduces verbatim ISO/IEC 9798-2(second edition):1999, including Technical Corrigendum February 2004, and implements it as the UK national standard. It supersedes BS ISO/IEC 9798-2:1994 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Information technology — Security techniques, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international publications referred to in this document may be found in the *BSI Catalogue* under the section entitled “International Standards Correspondence Index”, or by using the “Search” facility of the *BSI Electronic Catalogue* or of British Standards Online.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the ISO/IEC title page, pages ii and iii, a blank page, pages 1 to 11 and a back cover

The BSI copyright notice displayed in this document indicates when the document was last issued.

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Committee and comes into effect on 15 February 2000

© BSI 15 March 2004

Amendments issued since publication

Amd. No.	Date	Comments
15035 Technical Corrigendum No.1	15 March 2004	Changes made to Clause 4

**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.

