

BS ISO/IEC 9798-4:1999

Incorporating corrigenda September 2009 and July 2012



BSI Standards Publication

Information technology - Security techniques - Entity authentication

Part 4: Mechanisms using a cryptographic
check function

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

National foreword

This British Standard is the UK implementation of ISO/IEC 9798-4:1999, incorporating corrigenda September 2009 and July 2012. It supersedes BS ISO/IEC 9798-4:1995 which is withdrawn.

ISO/IEC corrigendum September 2009 introduces two changes to the text: it inserts a bibliography, and adds a new paragraph to Clause 3.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

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

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

© The British Standards Institution 2012. Published by BSI Standards Limited 2012

ISBN 978 0 580 76594 0

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 May 2012.

Amendments/corrigenda issued since publication

Date	Text affected
31 August 2012	Implementation of ISO/IEC corrigendum July 2012: Foreword and Clause 4 have been amended, Annex B has been inserted.

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

**Part 4:
Mechanisms using a cryptographic check
function**

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

Partie 4: Mécanismes utilisant une fonction cryptographique de vérification

Reference number
ISO/IEC 9798-4:1999(E)



PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 1999

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 734 10 79
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Contents

1	Scope	1
2	Normative references	1
3	Definitions and notation	1
4	Requirements	1
5	Mechanisms	2
5.1	Unilateral authentication	2
5.1.1	One pass authentication	2
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
Annex A	Use of text fields	7
Annex B	Object Identifiers	7
Bibliography		8