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

Part 6:

Mechanisms using manual data transfer

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

Partie 6: Mécanismes utilisant un transfert manuel de données

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.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2010

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 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	3
5 Overall requirements	4
6 Mechanisms using a short check-value	5
6.1 General	5
6.2 Mechanism 1 – One device with simple input, one device with simple output	5
6.3 Mechanism 2 – Devices with simple input capabilities	7
7 Mechanisms using a manual transfer of a short digest-value or a short key	8
7.1 General	8
7.2 Mechanism 3 – One device with simple input, one device with simple output	8
7.3 Mechanism 4 – One device with simple input, one device with simple output	10
7.4 Mechanism 5 – Devices with simple input capabilities	11
7.5 Mechanism 6 – Devices with simple input capabilities	13
8 Mechanisms using a MAC	15
8.1 General	15
8.2 Mechanism 7 – Devices with simple output capabilities	15
8.3 Mechanism 8 – One device with simple input, one device with simple output	18
Annex A (normative) ASN.1 modules	20
Annex B (informative) Using manual authentication protocols for the exchange of secret keys	21
Annex C (informative) Using manual authentication protocols for the exchange of public keys	23
Annex D (informative) On mechanism security and choices for parameter lengths	25
Annex E (informative) A method for generating short check-values	28
Annex F (informative) Comparative analysis in security and efficiency of mechanisms 1–8	30
Annex G (informative) Methods for generating short digest-values	33
Bibliography	34