

ISO/IEC 9798-6:2010-12 (E)

Information technology - Security techniques - Entity authentication - Part 6: Mechanisms using manual data transfer

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