

ISO/IEC 9798-6:2005-08 (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	2
5	Requirements	3
6	Mechanisms using a short check-value	4
6.1	General	4
6.2	Mechanism 1 - One device with simple input, one device with simple output	4
6.2.1	Requirements	4
6.2.2	Specification of data exchanged	4
6.2.3	Manual authentication certificates	5
6.3	Mechanism 2 - Devices with simple input capabilities	6
6.3.1	Requirements	6
6.3.2	Specification of data exchanged	6
7	Mechanisms using a MAC	7
7.1	General	7
7.2	Mechanism 3 - Devices with simple output capabilities	7
7.2.1	General	7
7.2.2	Requirements	7
7.2.3	Specification of data exchanged in mechanism 3a	7
7.2.4	Specification of data exchanged in mechanism 3b	9
7.3	Mechanism 4 - One device with simple input, one device with simple output	10
7.3.1	General	10
7.3.2	Requirements	10
7.3.3	Specification of data exchanged in mechanism 4a	10
7.3.4	Specification of data exchanged in mechanism 4b	11
Annex A (informative) Using manual authentication protocols for the exchange of secret keys		12
A.1	General	12
A.2	Authenticated Diffie-Hellman key agreement	12
A.3	Authenticated Diffie-Hellman key agreement using a manual authentication certificate	12
A.3.1	General	12
A.3.2	Stage 1	13
A.3.3	Stage 2 (initiated by either device at some later time)	13
A.4	More than two components	13
Annex B (informative) Using manual authentication protocols for the exchange of public keys		14
B.1	General	14
B.2	Requirements	14

B.3	Private key generated in device	14
B.4	Private key generated externally	15
Annex C (informative) On mechanism security and choices for parameter lengths		16
C.1	General	16
C.2	Use of mechanisms 1 and 2	16
C.3	Use of mechanisms 3 and 4	17
Annex D (informative) A method for generating short check-values		18
D.1	General	18
Bibliography		20