

ISO/IEC 9798-2:2008-12 (E)

Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms

Contents		Page
Foreword		iv
1	Scope	1
2	Normative references	1
3	Terms and definitions	2
4	Symbols and notation	3
5	Requirements	3
6	Mechanisms not involving a trusted third party	4
6.1	Unilateral authentication	4
6.1.1	Mechanism 1 -- One-pass authentication	5
6.1.2	Mechanism 2 -- Two-pass authentication	5
6.2	Mutual authentication	6
6.2.1	Mechanism 3 -- Two-pass authentication	6
6.2.2	Mechanism 4 -- Three-pass authentication	7
7	Mechanisms involving a trusted third party	8
7.1	Mechanism 5 -- Four-pass authentication	8
7.2	Mechanism 6 -- Five-pass authentication	10
Annex A (normative) OIDs and ASN.1 syntax		12
Annex B (informative) Use of text fields		14
Annex C (informative) Properties of entity authentication mechanisms		15
Bibliography		16