

ISO/IEC 9798-5:2009-12 (E)

Information technology - Security techniques - Entity authentication - Part 5: Mechanisms using zero-knowledge techniques

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Terms and definitions	1
3	Notation, symbols and abbreviated terms	4
4	Mechanisms based on identities	7
4.1	Security requirements for the environment	7
4.2	Key production	8
4.3	Unilateral authentication exchange	10
5	Mechanisms based on integer factorization	12
5.1	Security requirements for the environment	12
5.2	Key production	12
5.3	Unilateral authentication exchange	13
6	Mechanisms based on discrete logarithms with respect to prime numbers	15
6.1	Security requirements for the environment	15
6.2	Key production	15
6.3	Unilateral authentication exchange	16
7	Mechanisms based on discrete logarithms with respect to composite numbers	17
7.1	Security requirements for the environment	17
7.2	Key production	18
7.3	Unilateral authentication exchange	19
8	Mechanisms based on asymmetric encryption systems	20
8.1	Security requirements for the environment	20
8.2	Unilateral authentication exchange	21
8.3	Mutual authentication exchange	22
9	Mechanism based on discrete logarithms with respect to elliptic curves	23
9.1	Security requirements for the environment	23
9.2	Key production	24
9.3	Unilateral authentication exchange	24
Annex A (normative) Object identifiers		26
Annex B (informative) Principles of zero-knowledge techniques		28
Annex C (informative) Guidance on parameter choice and comparison of the mechanisms		31
Annex D (informative) Numerical examples		41
Bibliography		52