

ISO/IEC 9796-2:2010-12 (E)

Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and abbreviated terms	3
5	Converting between bit strings and integers	5
6	Requirements	5
7	Model for signature and verification processes	7
7.1	General	7
7.2	Signing a message	7
7.2.1	Overview	7
7.2.2	Message allocation	7
7.2.3	Message representative production	8
7.2.4	Signature production	8
7.3	Verifying a signature	8
7.3.1	Overview	8
7.3.2	Signature opening	8
7.3.3	Message recovery	8
7.3.4	Message assembly	9
7.4	Specifying a signature scheme	9
8	Digital signature scheme 1	9
8.1	General	9
8.2	Parameters	9
8.2.1	Modulus length	9
8.2.2	Trailer field options	10
8.2.3	Capacity	10
8.3	Message representative production	10
8.3.1	Hashing the message	10
8.3.2	Formatting	10
8.4	Message recovery	11
9	Digital signature scheme 2	12
9.1	General	12
9.2	Parameters	12
9.2.1	Modulus length	12
9.2.2	Salt length	12
9.2.3	Trailer field options	12
9.2.4	Capacity	13
9.3	Message representative production	13
9.3.1	Hashing the message	13
9.3.2	Formatting	13

9.4	Message recovery	13
10	Digital signature scheme 3	14
Annex A (normative) ASN.1 module		15
A.1	General	15
A.2	Use of subsequent object identifiers	17
Annex B (normative) Public key system for digital signature		18
B.1	Terms and definitions	18
B.2	Symbols and abbreviations	18
B.3	Key production	19
B.3.1	Public verification exponent	19
B.3.2	Secret prime factors and public modulus	19
B.3.3	Private signature exponent	20
B.4	Signature production function	20
B.5	Signature opening function	20
B.6	Alternative signature production function	21
B.7	Alternative signature opening function	21
Annex C (normative) Mask generation function		22
C.1	Symbols and abbreviations	22
C.2	Requirements	22
C.3	Specification	22
C.3.1	Parameters	22
C.3.2	Mask generation	22
Annex D (informative) On hash-function identifiers and the choice of the recoverable length of the message		23
Annex E (informative) Examples		24
E.1	Examples with public exponent 3	24
E.1.1	Example of key production process	24
E.1.2	Examples with total recovery	25
E.1.3	Examples with partial recovery	31
E.2	Examples with public exponent 2	38
E.2.1	Example of key production process	38
E.2.2	Examples with total recovery	38
E.2.3	Examples with partial recovery	44
Bibliography		53