

ISO/IEC 9796-2:2002-10 (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	6
7.1 Signing a message.....	7
7.1.1 Overview	7
7.1.2 Message allocation	7
7.1.3 Message representative production	7
7.1.4 Signature production.....	7
7.2 Verifying a signature.....	8
7.2.1 Overview	8
7.2.2 Signature opening.....	8
7.2.3 Message recovery.....	8
7.2.4 Message assembly.....	8
7.3 Specifying a signature scheme	8
8 Digital signature scheme 1	9
8.1 Parameters.....	9
8.1.1 Modulus length.....	9
8.1.2 Trailer field options.....	9
8.1.3 Capacity	9
8.2 Message representative production	9
8.2.1 Hashing the message	9
8.2.2 Formatting	9
8.3 Message recovery.....	10
9 Digital signature scheme 2	11
9.1 Parameters.....	11
9.1.1 Modulus length.....	11
9.1.2 Salt length.....	11
9.1.3 Trailer field options.....	11
9.1.4 Capacity	12
9.2 Message representative production	12
9.2.1 Hashing the message	12
9.2.2 Formatting	12
9.3 Message recovery.....	12
10 Digital signature scheme 3	13
Annex A (normative) Public key system for digital signature	14
Annex B (normative) Mask generation function	18
Annex C (informative) On hash-function identifiers and the choice of the recoverable length of the message.....	20
Annex D (informative) Examples.....	21
Bibliography	47