

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

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