

ISO/IEC 9796-3:2006-09 (E)

Information technology - Security techniques - Digital signature schemes giving message recovery - Part 3: Discrete logarithm based mechanisms

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols, notation and conventions	4
4.1	Symbols and notation	4
4.2	Conversion functions and mask generation functions	6
4.3	Legend for figures	6
5	Binding between signature mechanisms and hash-functions	7
6	Framework for digital signatures giving message recovery	7
6.1	Processes	7
6.2	Parameter generation process	8
6.3	Signature generation process	8
6.4	Signature verification process	9
7	General model for digital signatures giving message recovery	9
7.1	Requirements	9
7.2	Summary of functions and procedures	10
7.3	User key generation process	11
7.4	Signature generation process	11
7.5	Signature verification process	14
8	NR (Nyberg-Rueppel message recovery signature)	17
8.1	Domain parameter and user keys	17
8.2	Signature generation process	17
8.3	Signature verification process	18
9	ECNR (Elliptic Curve Nyberg-Rueppel message recovery signature)	19
9.1	Domain parameter and user keys	19
9.2	Signature generation process	19
9.3	Signature verification process	20
10	ECMR (Elliptic Curve Miyaji message recovery signature)	21
10.1	Domain parameter and user keys	21
10.2	Signature generation process	22
10.3	Signature verification process	23
11	ECAO (Elliptic Curve Abe-Okamoto message recovery signature)	23
11.1	Domain parameter	23
11.2	User keys	24
11.3	Signature generation process	24
11.4	Signature verification process	26

12	ECPV (Elliptic Curve Pintsov-Vanstone message recovery signature)	27
12.1	Domain and user parameters	27
12.2	Signature generation process	28
12.3	Signature verification process	29
13	ECKNR (Elliptic Curve KCDSA/Nyberg-Rueppel message recovery signature)	31
13.1	Domain parameter and user keys	31
13.2	Signature generation process	31
13.3	Signature verification process	32
Annex A (informative) Mathematical conventions		34
A.1	Bit strings	34
A.2	Octet strings	34
A.3	Finite fields	34
A.4	Elliptic curves	35
Annex B (normative) Conversion functions		36
B.1	Octet string / bit string conversion: OS2BSP and BS2OSP	36
B.2	Bit string / integer conversion: BS2IP and I2BSP	36
B.3	Octet string / integer conversion: OS2IP and I2OSP	36
B.4	Finite field element / integer conversion: FE2IPF	36
B.5	Octet string / finite field element conversion: OS2FEFP and FE2OSPF	37
B.6	Elliptic curve / octet string conversion: EC2OSPE and OS2ECPE	37
Annex C (normative) Mask generation functions (Key derivation functions)		39
C.1	Allowable mask generation functions	39
C.2	MGF1	39
C.3	MGF2	39
Annex D (informative) Example method for producing the data input		40
D.1	Splitting the message and producing the data input	40
D.2	Checking the redundancy	40
Annex E (normative) ASN.1 module		42
E.1	Formal definition	42
E.2	Use of subsequent object identifiers	43
Annex F (informative) Numerical examples		44
F.1	Numerical examples for NR	44
F.2	Numerical examples for ECNR	47
F.3	Numerical examples for ECMR	51
F.4	Numerical examples for ECAO	54
F.5	Numerical examples for ECPV	59
F.6	Numerical examples for ECKNR	62
Annex G (informative) Summary of properties of mechanisms		66
Annex H (informative) Correspondence of schemes		68
Bibliography		69