

ISO/IEC 14888-3:2016-03 (E)

Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms

Contents		Page
Foreword		vi
Introduction		vii
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and abbreviated terms	3
5	General model	5
5.1	Parameter generation process	5
5.1.1	Certificate-based mechanisms	5
5.1.2	Identity-based mechanisms	5
5.1.3	Parameter selection	6
5.1.4	Validity of domain parameters and verification key	7
5.2	Signature process	7
5.2.1	General	7
5.2.2	Producing the randomizer	8
5.2.3	Producing the pre-signature	8
5.2.4	Preparing the message for signing	8
5.2.5	Computing the witness (the first part of the signature)	8
5.2.6	Computing the assignment	8
5.2.7	Computing the second part of the signature	9
5.2.8	Constructing the appendix	9
5.2.9	Constructing the signed message	9
5.3	Verification process	10
5.3.1	General	10
5.3.2	Retrieving the witness	10
5.3.3	Preparing message for verification	11
5.3.4	Retrieving the assignment	11
5.3.5	Recomputing the pre-signature	11
5.3.6	Recomputing the witness	11
5.3.7	Verifying the witness	11
6	Certificate-based mechanisms	12
6.1	General	12
6.1	6.1	12
	General	12
6.2	DSA	13
6.2.1	General	13
6.2.2	Parameters	13
6.2.3	Generation of signature key and verification key	14
6.2.4	Signature process	14
6.2.5	Verification process	15
6.3	KCDSA	16
6.3.1	General	16
6.3.2	Parameters	16
6.3.3	Generation of signature key and verification key	17
6.3.4	Signature process	17
6.3.5	Verification process	18

6.4	Pointcheval/Vaudenay algorithm.....	19
6.4.1	General.....	19
6.4.2	Parameters.....	19
6.4.3	Generation of signature key and verification key.....	19
6.4.4	Signature process.....	19
6.4.5	Verification process.....	20
6.5	SDSA.....	21
6.5.1	General.....	21
6.5.2	Parameters.....	22
6.5.3	Generation of signature key and verification key.....	22
6.5.4	Signature process.....	22
6.5.5	Verification process.....	23
6.6	EC-DSA.....	24
6.6.1	General.....	24
6.6.2	Parameters.....	24
6.6.3	Generation of signature key and verification key.....	25
6.6.4	Signature process.....	25
6.6.5	Verification process.....	26
6.7	EC-KCDSA.....	27
6.7.1	General.....	27
6.7.2	Parameters.....	27
6.7.3	Generation of signature key and verification key.....	28
6.7.4	Signature process.....	28
6.7.5	Verification process.....	29
6.8	EC-GDSA.....	30
6.8.1	General.....	30
6.8.2	Parameters.....	30
6.8.3	Generation of signature key and verification key.....	30
6.8.4	Signature process.....	30
6.8.5	Verification process.....	31
6.9	EC-RDSA.....	32
6.9.1	General.....	32
6.9.2	Parameters.....	33
6.9.3	Generation of signature key and verification key.....	33
6.9.4	Signature process.....	33
6.9.5	Verification process.....	34
6.10	EC-SDSA.....	35
6.10.1	General.....	35
6.10.2	Parameters.....	35
6.10.3	Generation of signature key and verification key.....	35
6.10.4	Signature process.....	36
6.10.5	Verification process.....	36
6.11	EC-FSDSA.....	37
6.11.1	General.....	37
6.11.2	Parameters.....	38
6.11.3	Generation of signature key and verification key.....	38
6.11.4	Signature process.....	38
6.11.5	Verification process.....	39
7	Identity-based mechanisms.....	40
7.1	General.....	40
7.1	7.1.....	
	General.....	40
7.2	IBS-1.....	41
7.2.1	General.....	41
7.2.2	Parameters.....	41
7.2.3	Generation of master key and signature/verification key.....	41
7.2.4	Signature process.....	41
7.2.5	Verification process.....	42

7.3	IBS-2.....	43
7.3.1	General.....	43
7.3.2	Parameters.....	43
7.3.3	Generation of master key and signature/verification key.....	43
7.3.4	Signature process.....	43
7.3.5	Verification process.....	44
Annex A	(normative) Object identifier.....	46
Annex B	(normative) Conversion functions (I).....	49
Annex C	(informative) Conversion functions (II).....	54
Annex D	(normative) Generation of DSA domain parameters.....	56
Annex E	(informative) The Weil and Tate pairings.....	58
Annex F	(informative) Numerical examples.....	61
Annex G	(informative) Comparison of the signature schemes.....	127
Annex H	(informative) Claimed features for choosing a mechanism.....	129
Bibliography	130