ISO/IEC 14888-3:2006-11 (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 2

4 Symbols 2

5 General model 4
5.1 Parameter generation process 4
5.1.1 Certificate-based mechanisms 4
5.1.2 Identity-based mechanisms 4
5.1.3 Parameter selection 5
5.1.4 Validity of domain parameters and verification key 5
5.2 Signature process 6
5.2.1 Producing the randomizer 7
5.2.2 Producing the pre-signature 7
5.2.3 Preparing the message for signing 7
5.2.4 Computing the witness (the first part of the signature) 7
5.2.5 Computing the assignment 7
5.2.6 Computing the second part of the signature 8
5.2.7 Constructing the appendix 8
5.2.8 Constructing the signed message 8
5.3 Verification process 9
5.3.1 Retrieving the witness 10
5.3.2 Preparing message for verification 10
5.3.3 Retrieving the assignment 10
5.3.4 Recomputing the pre-signature 10
5.3.5 Recomputing the witness 10
5.3.6 Verifying the witness 10

6 Certificate-based mechanisms 11
6.1 DSA 11
6.1.1 Parameters 12
6.1.2 Generation of signature key and verification key 12
6.1.3 Signature process 12
6.1.4 Verification process 13
6.2 KCDSA 14
6.2.1 Parameters 15
6.2.2 Generation of signature key and verification key 15
6.2.3 Signature process 15
6.2.4 Verification process 16
6.3 Pointcheval/Vaudenay algorithm 17
6.3.1 Parameters 17
6.3.2 Generation of signature key and verification key 18
6.3.3 Signature process 18
6.3.4 Verification process 19

6.4 EC-DSA 19
6.4.1 Parameters 20
6.4.2 Generation of signature key and verification key 20
6.4.3 Signature process 20
6.4.4 Verification process 21
6.5 EC-KCDSA 22
6.5.1 Parameters 22
6.5.2 Generation of signature key and verification key 23
6.5.3 Signature process 23
6.5.4 Verification process 24
6.6 EC-GDSA 24
6.6.1 Parameters 25
6.6.2 Generation of signature key and verification key 25
6.6.3 Signature process 25
6.6.4 Verification process 26

7 Identity-based mechanisms 27
7.1 IBS-1 27
7.1.1 Parameters 28
7.1.2 Generation of master key and signature/verification key 28
7.1.3 Signature process 28
7.1.4 Verification process 29
7.2 IBS-2 30
7.2.1 Parameters 30
7.2.2 Generation of master key and signature/verification key 30
7.2.3 Signature process 30
7.2.4 Verification process 31

Annex A (normative) ASN.1 module 33

Annex B (normative) Conversion functions (I) 36

B.1 Conversion from a field element to an integer (FE2I) 36
B.2 Conversion from an integer to a field element (I2FE) 36
B.3 Conversion from a field element to a bit sequence (FE2BS) 36
B.4 Conversion from a bit sequence to an integer (BS2I) 36
B.5 Conversion from an integer to a bit sequence (I2BS) 37
B.6 Conversion between an integer and an octet string (I2OS & OS2I) 37

Annex C (informative) Conversion functions (II) 38

C.1 Conversion from an integer to a point (I2P) 38

Annex D (normative) Generation of DSA domain parameters 40

D.1 Generation of the prime p and q 40
D.2 Generation of the generator G 41
D.2.1 Unverifiable generation of G 41
D.2.2 Verifiable generation of G 41

Annex E (informative) The Weil and Tate pairings 42

E.1 The functions f, g and d 42
E.2 The Weil pairing 43
E.3 The Tate pairing 43

Annex F (informative) Numerical examples 45

F.1 DSA mechanism 45
F.1.1 Example 1 45
F.1.2 Example 2 46
F.2 KCDSA mechanism 48

F.2.1 Parameters 48
F.2.2 Signature key and verification key 49
F.2.3 Per message data 49
F.2.4 Signature 49
F.2.5 Verification 49
F.3 Pointcheval-Vaudenay mechanism 49
F.3.1 Parameters 49
F.3.2 Signature key and verification key 49
F.3.3 Per message data 50
F.3.4 Signature 50
F.3.5 Verification 50
F.4 EC-DSA mechanism 50
F.4.1 Example 1: Field F2 m , m =191 50
F.4.2 Example 2: Field FP , 192-bit Prime P 51
F.5 EC-KCDSA mechanism 52
F.5.1 Example 1: Field F2 m , m =163 52
F.5.2 Example 2: Field FP, 192-bit Prime P 53
F.5.3 Example 2: Field FP m , 32-bit P and m = 5 54
F.6 EC-GDSA mechanism 55
F.6.1 Domain and User Parameters 55
F.6.2 Example 1: Field FP , 192-bit Prime P 55
F.7 IBS-1 mechanism 56
F.7.1 Example 1: Field Fp , 512-bit Prime p 56
F.7.2 Example 2: Field Fp , 512-bit Prime p 58
F.8 IBS-2 mechanism 60
F.8.1 Example 1: Field Fp , 512-bit Prime p 60

Annex G (informative) Comparison of the signature schemes 64

G.1 Symbols and abbreviated terms for comparing the signature schemes 64
G.2 Comparison of the signature schemes 64

Annex H (informative) Claimed features for choosing a mechanism 66

Bibliography 67