ISO/IEC 14888-3:2018 (E)

IT Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Symbols and abbreviated terms

5 General model

5.1 Parameter generation process
5.1.1 Certificate-based mechanisms
5.1.1.1 Generation of domain parameters
5.1.1.2 Generation of signature key and verification key
5.1.2 Identity-based mechanisms
5.1.2.1 Notation
5.1.2.2 Generation of domain parameters
5.1.2.3 Generation of master key
5.1.2.4 Generation of signature key and verification key
5.1.3 Parameter selection
5.1.3.1 Selecting parameter size
5.1.3.2 Selecting a hash-function
5.1.4 Validity of domain parameters and verification key
5.2 Signature process
5.2.1 General
5.2.2 Producing the randomizer
5.2.3 Producing the pre-signature
5.2.4 Preparing the message for signing
5.2.5 Computing the witness (the first part of the signature)
5.2.6 Computing the assignment
5.2.7 Computing the second part of the signature
5.2.8 Constructing the appendix
5.2.9 Constructing the signed message
5.3 Verification process
5.3.1 General
5.3.2 Retrieving the witness
5.3.3 Preparing message for verification
5.3.4 Retrieving the assignment
5.3.5 Recomputing the pre-signature
5.3.6 Recomputing the witness
5.3.7 Verifying the witness

6 Certificate-based mechanisms

6.1 General
6.2 DSA
6.2.1 General
6.2.2 Parameters
6.2.3 Generation of signature key and verification key
6.2.4 Signature process
6.2.4.1 Producing the randomizer

6.2.4.2 Producing the pre-signature
6.2.4.3 Preparing the message for signing
6.2.4.4 Computing the witness
6.2.4.5 Computing the assignment
6.2.4.6 Computing the second part of the signature
6.2.4.7 Constructing the appendix
6.2.4.8 Constructing the signed message
6.2.5 Verification process
6.2.5.1 General
6.2.5.2 Retrieving the witness
6.2.5.3 Preparing the message for verification
6.2.5.4 Retrieving the assignment
6.2.5.5 Recomputing the pre-signature
6.2.5.6 Recomputing the witness
6.2.5.7 Verifying the witness
6.3 KCDSA
6.3.1 General
6.3.2 Parameters
6.3.3 Generation of signature key and verification key
6.3.4 Signature process
6.3.4.1 Producing the randomizer
6.3.4.2 Producing the pre-signature
6.3.4.3 Preparing the message for signing
6.3.4.4 Computing the witness
6.3.4.5 Computing the assignment
6.3.4.6 Computing the second part of the signature
6.3.4.7 Constructing the appendix
6.3.4.8 Constructing the signed message
6.3.5 Verification process
6.3.5.1 General
6.3.5.2 Retrieving the witness
6.3.5.3 Preparing the message for verification
6.3.5.4 Retrieving the assignment
6.3.5.5 Recomputing the pre-signature
6.3.5.6 Recomputing the witness
6.3.5.7 Verifying the witness
6.4 Pointcheval/Vaudenay algorithm
6.4.1 General
6.4.2 Parameters
6.4.3 Generation of signature key and verification key
6.4.4 Signature process
6.4.4.1 Producing the randomizer
6.4.4.2 Producing the pre-signature
6.4.4.3 Preparing message for signing
6.4.4.4 Computing the witness
6.4.4.5 Computing the assignment
6.4.4.6 Computing the signature
6.4.4.7 Constructing the appendix
6.4.4.8 Constructing the signed message
6.4.5 Verification process
6.4.5.1 General
6.4.5.2 Retrieving the witness
6.4.5.3 Preparing the message for verification
6.4.5.4 Retrieving the assignment
6.4.5.5 Recomputing the pre-signature
6.4.5.6 Recomputing the witness
6.4.5.7 Verifying the witness
6.5 SDSA
6.5.1 General
6.5.2 Parameters
6.5.3 Generation of signature key and verification key
6.5.4 Signature process
6.5.4.1 Producing the randomizer
6.5.4.2 Producing the pre-signature

6.5.4.3 Preparing message for signing
6.5.4.4 Computing the witness
6.5.4.5 Computing the assignment
6.5.4.6 Computing the second part of the signature
6.5.4.7 Constructing the appendix
6.5.4.8 Constructing the signed message
6.5.5 Verification process
6.5.5.1 General
6.5.5.2 Retrieving the witness
6.5.5.3 Preparing message for verification
6.5.5.4 Retrieving the assignment
6.5.5.5 Recomputing the pre-signature
6.5.5.6 Recomputing the witness
6.5.5.7 Verifying the witness
6.6 EC-DSA
6.6.1 General
6.6.2 Parameters
6.6.3 Generation of signature key and verification key
6.6.4 Signature process
6.6.4.1 Producing the randomizer
6.6.4.2 Producing the pre-signature
6.6.4.3 Preparing message for signing
6.6.4.4 Computing the witness
6.6.4.5 Computing the assignment
6.6.4.6 Computing the second part of the signature
6.6.4.7 Constructing the appendix
6.6.4.8 Constructing the signed message
6.6.5 Verification process
6.6.5.1 General
6.6.5.2 Retrieving the witness
6.6.5.3 Preparing message for verification
6.6.5.4 Retrieving the assignment
6.6.5.5 Recomputing the pre-signature
6.6.5.6 Recomputing the witness
6.6.5.7 Verifying the witness
6.7 EC-KCDSA
6.7.1 General
6.7.2 Parameters
6.7.3 Generation of signature key and verification key
6.7.4 Signature process
6.7.4.1 Producing the randomizer
6.7.4.2 Producing the pre-signature
6.7.4.3 Preparing the message for signing
6.7.4.4 Computing the witness
6.7.4.5 Computing the assignment
6.7.4.6 Computing the second part of the signature
6.7.4.7 Constructing the appendix
6.7.4.8 Constructing the signed message
6.7.5 Verification process
6.7.5.1 General
6.7.5.2 Retrieving the witness
6.7.5.3 Preparing the message for verification
6.7.5.4 Retrieving the assignment
6.7.5.5 Recomputing the pre-signature
6.7.5.6 Recomputing the witness
6.7.5.7 Verifying the witness
6.8 EC-GDSA
6.8.1 General
6.8.2 Parameters
6.8.3 Generation of signature key and verification key
6.8.4 Signature process
6.8.4.1 Producing the randomizer
6.8.4.2 Producing the pre-signature
6.8.4.3 Preparing message for signing

6.8.4.4 Computing the witness
6.8.4.5 Computing the assignment
6.8.4.6 Computing the second part of the signature
6.8.4.7 Constructing the appendix
6.8.4.8 Constructing the signed message
6.8.5 Verification process
6.8.5.1 General
6.8.5.2 Retrieving the witness
6.8.5.3 Preparing message for verification
6.8.5.4 Retrieving the assignment
6.8.5.5 Recomputing the pre-signature
6.8.5.6 Recomputing the witness
6.8.5.7 Verifying the witness
6.9 EC-RDSA
6.9.1 General
6.9.2 Parameters
6.9.3 Generation of signature key and verification key
6.9.4 Signature process
6.9.4.1 Producing the randomizer
6.9.4.2 Producing the pre-signature
6.9.4.3 Preparing message for signing
6.9.4.4 Computing the witness
6.9.4.5 Computing the assignment
6.9.4.6 Computing the second part of the signature
6.9.4.7 Constructing the appendix
6.9.4.8 Constructing the signed message
6.9.5 Verification process
6.9.5.1 Retrieving the witness
6.9.5.2 Preparing message for verification
6.9.5.3 Retrieving the assignment
6.9.5.4 Recomputing the pre-signature
6.9.5.5 Recomputing the witness
6.9.5.6 Verifying the witness
6.10 EC-SDSA
6.10.1 General
6.10.2 Parameters
6.10.3 Generation of signature key and verification key
6.10.4 Signature process
6.10.4.1 Producing the randomizer
6.10.4.2 Producing the pre-signature
6.10.4.3 Preparing message for signing
6.10.4.4 Computing the witness
6.10.4.5 Computing the assignment
6.10.4.6 Computing the second part of the signature
6.10.4.7 Constructing the appendix
6.10.4.8 Constructing the signed message
6.10.5 Verification process
6.10.5.1 General
6.10.5.2 Retrieving the witness
6.10.5.3 Preparing message for verification
6.10.5.4 Retrieving the assignment
6.10.5.5 Recomputing the pre-signature
6.10.5.6 Recomputing the witness
6.10.5.7 Verifying the witness
6.11 EC-FSDSA
6.11.1 General
6.11.2 Parameters
6.11.3 Generation of signature key and verification key
6.11.4 Signature process
6.11.4.1 Producing the randomizer
6.11.4.2 Producing the pre-signature
6.11.4.3 Preparing message for signing
6.11.4.4 Computing the witness
6.11.4.5 Computing the assignment

6.11.4.6 Computing the second part of the signature
6.11.4.7 Constructing the appendix
6.11.4.8 Constructing the signed message
6.11.5 Verification process
6.11.5.1 General
6.11.5.2 Retrieving the witness
6.11.5.3 Preparing message for verification
6.11.5.4 Retrieving the assignment
6.11.5.5 Recomputing the pre-signature
6.11.5.6 Recomputing the witness
6.11.5.7 Verifying the witness
6.12 SM2
6.12.1 General
6.12.2 Parameters
6.12.3 Generation of signature key and verification key
6.12.4 Signature process
6.12.4.1 Producing the randomizer
6.12.4.2 Producing the pre-signature
6.12.4.3 Preparing message for signing
6.12.4.4 Computing the witness
6.12.4.5 Computing the assignment
6.12.4.6 Computing the second part of the signature
6.12.4.7 Constructing the appendix
6.12.4.8 Constructing the signed message
6.12.5 Verification process
6.12.5.1 General
6.12.5.2 Retrieving the witness
6.12.5.3 Preparing message for verification
6.12.5.4 Retrieving the assignment
6.12.5.5 Recomputing the pre-signature
6.12.5.6 Recomputing the witness
6.12.5.7 Verifying the witness

7 Identity-based mechanisms

7.1 General
7.2 IBS-1
7.2.1 General
7.2.2 Parameters
7.2.3 Generation of master key and signature/verification key
7.2.4 Signature process
7.2.4.1 Producing the randomizer
7.2.4.2 Producing the pre-signature
7.2.4.3 Preparing message for signing
7.2.4.4 Computing the witness
7.2.4.5 Computing the assignment
7.2.4.6 Computing the second part of the signature
7.2.4.7 Constructing the appendix
7.2.4.8 Constructing the signed message
7.2.5 Verification process
7.2.5.1 General
7.2.5.2 Retrieving the witness
7.2.5.3 Preparing message for verification
7.2.5.4 Retrieving the assignment
7.2.5.5 Recomputing the pre-signature
7.2.5.6 Recomputing the witness
7.2.5.7 Verifying the witness
7.3 IBS-2
7.3.1 General
7.3.2 Parameters
7.3.3 Generation of master key and signature/verification key
7.3.4 Signature process
7.3.4.1 Producing the randomizer
7.3.4.2 Producing the pre-signature
7.3.4.3 Preparing message for signing

7.3.4.4 Computing the witness
7.3.4.5 Computing the assignment
7.3.4.6 Computing the second part of the signature
7.3.4.7 Constructing the appendix
7.3.4.8 Constructing the signed message
7.3.5 Verification process
7.3.5.1 General
7.3.5.2 Retrieving the witness
7.3.5.3 Preparing message for verification
7.3.5.4 Retrieving the assignment
7.3.5.5 Recomputing the pre-signature
7.3.5.6 Recomputing the witness
7.3.5.7 Verifying the witness
7.4 Chinese IBS
7.4.1 General
7.4.2 Parameters
7.4.3 Generation of master key and signature/verification key
7.4.4 Signature process
7.4.4.1 Producing the randomizer
7.4.4.2 Producing the pre-signature
7.4.4.3 Preparing message for signing
7.4.4.4 Computing the witness
7.4.4.5 Computing the assignment
7.4.4.6 Computing the second part of the signature
7.4.4.7 Constructing the appendix
7.4.4.8 Constructing the signed message
7.4.5 Verification process
7.4.5.1 General
7.4.5.2 Retrieving the witness
7.4.5.3 Preparing message for verification
7.4.5.4 Retrieving the assignment
7.4.5.5 Recomputing the pre-signature
7.4.5.6 Recomputing the witness
7.4.5.7 Verifying the witness

Annex A (normative) Object identifiers

Annex B (normative) Conversion functions (I)

B.1 Conversion from a field element to an integer: FE2I(r, x)
B.2 Conversion from an integer to a field element: I2FE(r, x)
B.3 Conversion from a field element to a binary string: FE2BS(r, x)
B.4 Conversion from a binary string to an integer: BS2I(g, x)
B.5 Conversion from an integer to a binary string: I2BS(g, x)
B.6 Conversion between an integer and an octet string: I2OS(h, x) & OS2I(h, M)

Annex C (informative) Conversion functions (II)

Annex D (normative) Generation of DSA domain parameters

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

Annex E (informative) The Weil and Tate pairings

E.1 General
E.2 The functions f, g and d
E.3 The Weil pairing
E.4 The Tate pairing
E.5 The reduced Tate pairing

Annex F (informative) Numerical examples

F.1 General
F.2 DSA mechanism
F.2.1 Example 1: 2 048-bit Prime p, SHA-224

F.2.1.1 General
F.2.1.2 Parameters
F.2.1.3 Signature key and verification key
F.2.1.4 Per message data
F.2.1.5 Signature
F.2.1.6 Verification
F.2.2 Example 2: 3 072-bit Prime p, SHA-256
F.2.2.1 General
F.2.2.2 Parameters
F.2.2.3 Signature key and verification key
F.2.2.4 Per message data
F.2.2.5 Signature
F.2.2.6 Verification
F.3 KCDSA mechanism
F.3.1 Example 1: 2 048-bit Prime p, 224-bit Prime q, SHA-224
F.3.1.1 General
F.3.1.2 Parameters
F.3.1.3 Signature key and verification key
F.3.1.4 Per message data
F.3.1.5 Signature
F.3.1.6 Verification
F.3.2 Example 2: 3 072-bit Prime p, 256-bit Prime q, SHA-256
F.3.2.1 General
F.3.2.2 Parameters
F.3.2.3 Signature key and verification key
F.3.2.4 Per message data
F.3.2.5 Signature
F.3.2.6 Verification
F.3.3 Example 3: 2 048-bit Prime p, 224-bit Prime q, SHA-256
F.3.3.1 General
F.3.3.2 Parameters
F.3.3.3 Signature key and verification key
F.3.3.4 Per message data
F.3.3.5 Signature
F.3.3.6 Verification
F.3.4 Example 4: 2 048-bit Prime p, 224-bit Prime q, SHA-256 (Same parameter as in F.3.3. However, F.3.4 is provided additionally to be consistent with[36])
F.3.4.1 General
F.3.4.2 Parameters
F.3.4.3 Signature key and verification key
F.3.4.4 Per message data
F.3.4.5 Signature
F.3.4.6 Verification
F.4 Pointcheval/Vaudenay mechanism
F.4.1 General
F.4.2 Example 1: 2 048-bit Prime p, SHA-224
F.4.2.1 Parameters
F.4.2.2 Signature key and verification key
F.4.2.3 Per message data
F.4.2.4 Signature
F.4.2.5 Verification
F.5 SDSA mechanism
F.5.1 Example 1: 2 048-bit Prime p, SHA-224
F.5.1.1 General
F.5.1.2 Parameters
F.5.1.3 Signature key and verification key
F.5.1.4 Per message data
F.5.1.5 Signature
F.5.1.6 Verification
F.5.2 Example 2: 2 048-bit Prime p, SHA-256
F.5.2.1 General
F.5.2.2 Parameters
F.5.2.3 Signature key and verification key
F.5.2.4 Per message data

F.5.2.5 Signature
F.5.2.6 Verification
F.6 EC-DSA mechanism
F.6.1 General
F.6.2 Example 1: Field F2m, m =191, SHA-1
F.6.2.1 Parameters
F.6.2.2 Signature key and verification key
F.6.2.3 Per message data
F.6.2.4 Signature
F.6.2.5 Verification
F.6.3 Example 2: Field Fp, 192-bit Prime p, SHA-1
F.6.3.1 Parameters
F.6.3.2 Signature key and verification key
F.6.3.3 Per message data
F.6.3.4 Signature
F.6.3.5 Verification
F.6.4 Example 3: Field F2m, m =283, SHA-256
F.6.4.1 Parameters
F.6.4.2 Signature key and verification key
F.6.4.3 Per message data
F.6.4.4 Signature
F.6.4.5 Verification
F.6.5 Example 4: Field Fp, 256-bit Prime p, SHA-256
F.6.5.1 Parameters
F.6.5.2 Signature key and verification key
F.6.5.3 Per message data
F.6.5.4 Signature
F.6.5.5 Verification
F.6.6 Example 5: Field Fp, 192-bit Prime p, SHA-224
F.6.6.1 Parameters
F.6.6.2 Signature key and verification key
F.6.6.3 Per message data
F.6.6.4 Signature
F.6.6.5 Verification
F.6.7 Example 6: Field F2m , m = 233, SHA-256
F.6.7.1 Parameters
F.6.7.2 Signature key and verification key
F.6.7.3 Per message data
F.6.7.4 Signature
F.6.7.5 Verification
F.6.8 Example 7: Field F2m, m=283, SHA-384
F.6.8.1 Parameters
F.6.8.2 Signature key and verification key
F.6.8.3 Per message data
F.6.8.4 Signature
F.6.8.5 Verification
F.7 EC-KCDSA mechanism
F.7.1 Example 1: Field Fp, 224-bit Prime p, SHA-224
F.7.1.1 General
F.7.1.2 Parameters
F.7.1.3 Signature key and verification key
F.7.1.4 Per message data
F.7.1.5 Signature
F.7.1.6 Verification
F.7.2 Example 2: Field Fp, 256-bit Prime p, SHA-256
F.7.2.1 General
F.7.2.2 Parameters
F.7.2.3 Signature key and verification key
F.7.2.4 Per message data
F.7.2.5 Signature
F.7.2.6 Verification
F.7.3 Example 3: Field F2m, m = 233, SHA-224
F.7.3.1 General
F.7.3.2 Parameters

F.7.3.3 Signature key and verification key
F.7.3.4 Per message data
F.7.3.5 Signature
F.7.3.6 Verification
F.7.4 Example 4: Field F2m, m = 233 (Koblitz Curve), SHA-224
F.7.4.1 General
F.7.4.2 Parameters
F.7.4.3 Signature key and verification key
F.7.4.4 Per message data
F.7.4.5 Signature
F.7.4.6 Verification
F.7.5 Example 5: Field F2m, m=283, SHA-256
F.7.5.1 General
F.7.5.2 Parameters
F.7.5.3 Signature key and verification key
F.7.5.4 Per message data
F.7.5.5 Signature
F.7.5.6 Verification
F.7.6 Example 6: Field F2m, m = 283 (Koblitz Curve), SHA-256
F.7.6.1 General
F.7.6.2 Parameters
F.7.6.3 Signature key and verification key
F.7.6.4 Per message data
F.7.6.5 Signature
F.7.6.6 Verification
F.7.7 Example 7: Field Fp, 224-bit Prime p, SHA-256
F.7.7.1 General
F.7.7.2 Parameters
F.7.7.3 Signature key and verification key
F.7.7.4 Per message data
F.7.7.5 Signature
F.7.7.6 Verification
F.7.8 Example 8: Field F2m, m = 233, SHA-256
F.7.8.1 General
F.7.8.2 Parameters
F.7.8.3 Signature key and verification key
F.7.8.4 Per message data
F.7.8.5 Signature
F.7.8.6 Verification
F.7.9 Example 9: Field F2m, m = 233 (Koblitz curve), SHA-256
F.7.9.1 General
F.7.9.2 Parameters
F.7.9.3 Signature key and verification key
F.7.9.4 Per message data
F.7.9.5 Signature
F.7.9.6 Verification
F.8 EC-GDSA mechanism
F.8.1 General
F.8.2 Example 1: Field Fp, 192-bit Prime p, SHA-256
F.8.2.1 Parameters
F.8.2.2 Signature key and verification key
F.8.2.3 Per message data
F.8.2.4 Signature
F.8.2.5 Verification
F.8.3 Example 2: Field Fp, 224-bit Prime p, SHA-224
F.8.3.1 Parameters
F.8.3.2 Signature key and verification key
F.8.3.3 Per message data
F.8.3.4 Signature
F.8.3.5 Verification
F.8.4 Example 3: Field Fp, 256-bit Prime p, SHA-256
F.8.4.1 Parameters
F.8.4.2 Signature key and verification key
F.8.4.3 Per message data

F.8.4.4 Signature
F.8.4.5 Verification
F.9 EC-RDSA mechanism
F.9.1 Example 1: Field Fp, 256-bit Prime p, SHA-256
F.9.1.1 General
F.9.1.2 Parameters
F.9.1.3 Signature key and verification key
F.9.1.4 Per message data
F.9.1.5 Signature
F.9.1.6 Verification
F.9.2 Example 2: Field Fp, 512-bit Prime p, SHA-512
F.9.2.1 General
F.9.2.2 Parameters
F.9.2.3 Signature key and verification key
F.9.2.4 Per message data
F.9.2.5 Signature
F.9.2.6 Verification
F.10 EC-SDSA mechanism
F.10.1 Example 1: Field Fp, 256-bit Prime p, SHA-256
F.10.1.1 General
F.10.1.2 Parameters
F.10.1.3 Signature key and verification key
F.10.1.4 Per message data
F.10.1.5 Signature
F.10.1.6 Verification
F.10.2 Example 2: Field Fp, 384-bit Prime p, SHA-384
F.10.2.1 General
F.10.2.2 Parameters
F.10.2.3 Signature key and verification key
F.10.2.4 Per message data
F.10.2.5 Signature
F.10.2.6 Verification
F.11 EC-FSDSA mechanism
F.11.1 Example 1: Field Fp, 256-bit Prime p, SHA-256
F.11.1.1 General
F.11.1.2 Parameters
F.11.1.3 Signature key and verification key
F.11.1.4 Per message data
F.11.1.5 Signature
F.11.1.6 Verification
F.11.2 Example 2: Field Fp, 384-bit Prime p, SHA-384
F.11.2.1 General
F.11.2.2 Parameters
F.11.2.3 Signature key and verification key
F.11.2.4 Per message data
F.11.2.5 Signature
F.11.2.6 Verification
F.12 IBS-1 mechanism
F.12.1 Example 1: Field Fp, 512-bit Prime p, SHA-1
F.12.1.1 General
F.12.1.2 Parameters
F.12.1.3 Signature key and verification
F.12.1.4 Per message data
F.12.1.5 Signature
F.12.1.6 Verification
F.12.2 Example 2: Field Fp, 512-bit Prime p, SHA-1
F.12.2.1 General
F.12.2.2 Parameters
F.12.2.3 Signature key and verification key
F.12.2.4 Per message data
F.12.2.5 Signature
F.12.2.6 Verification
F.13 IBS-2 mechanism
F.13.1 General

F.13.2 Example 1: Field Fp, 512-bit Prime p, SHA-1
F.13.2.1 Parameters
F.13.2.2 Signature key and verification key
F.13.2.3 Per message data
F.13.2.4 Signature
F.13.2.5 Verification
F.14 SM2 mechanism
F.14.1 Example 1: Field Fp, 256-bit Prime p, SM3
F.14.1.1 General
F.14.1.2 Parameters
F.14.1.3 Signature key and verification key
F.14.1.4 Per message data
F.14.1.5 Signature
F.14.1.6 Verification
F.14.2 Example 2: Field F2m, m=257, SM3
F.14.2.1 General
F.14.2.2 Parameters
F.14.2.3 Signature key and verification key
F.14.2.4 Per message data
F.14.2.5 Signature
F.14.2.6 Verification
F.15 Chinese IBS mechanism
F.15.1 General
F.15.2 Example 1: Field Fp, 256-bit Prime p, SM3
F.15.2.1 Parameters
F.15.2.2 Signature key and verification key
F.15.2.3 Per message data
F.15.2.4 Signature
F.15.2.5 Verification

Annex G (informative) Comparison of the signature schemes

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

Annex H (informative) Claimed features for choosing a mechanism

Page count: 155