INTERNATIONAL STANDARD

ISO/IEC 15946-2

First edition
2002-12-01

Information technology — Security techniques — Cryptographic techniques based on elliptic curves —

Part 2: Digital signatures

Technologies de l'information — Techniques de sécurité — Techniques cryptographiques basées sur les courbes elliptiques —

Partie 2: Signatures digitales

Reference number
ISO/IEC 15946-2:2002(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 15946-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 15946 consists of the following parts, under the general title *Information technology — Security techniques — Cryptographic techniques based on elliptic curves*:

— *Part 1: General*

— *Part 2: Digital signatures*

— *Part 3: Key establishment*

— *Part 4: Digital signatures giving message recovery*

Annexes A and B of this part of ISO/IEC 15946 are for information only.

Introduction

Some of the most interesting and potentially useful of the public-key cryptosystems that are currently available are cryptosystems based on elliptic curves defined over finite fields. The concept of an elliptic curve based public-key cryptosystem is rather simple:

— Every elliptic curve is endowed with a binary operation "+" under which it forms a finite abelian group.

— The group law on elliptic curves extends in a natural way to a "discrete exponentiation" on the point group of the elliptic curve.

— Based on the discrete exponentiation on an elliptic curve one can easily derive elliptic curve analogues of the well known public-key schemes of Diffie-Hellman and ElGamal type.

The security of such a public-key system depends on the difficulty of determining discrete logarithms in the group of points of an elliptic curve. This problem is - with current knowledge - much harder than the factorization of integers or the computation of discrete logarithms in a finite field. Indeed, since Miller and Koblitz in 1985 independently suggested the use of elliptic curves for public-key cryptographic systems, no substantial progress in tackling the elliptic curve discrete logarithm problem has been reported. The only known general algorithms to determine elliptic curve discrete logarithms take fully exponential time. Thus, it is possible for elliptic curve based public-key systems to use much shorter parameters than the RSA system or the classical discrete logarithm based systems that make use of the multiplicative group of some finite field. This yields significantly shorter digital signatures and system parameters and allows for computations using smaller integers.

It is the purpose of this document to meet the increasing interest in elliptic curve based public key technology and describe the components that are necessary to implement a secure digital signature system based on elliptic curves.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this International Standard may involve the use of patents.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured ISO and IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC. Information may be obtained from:

ISO/IEC JTC 1/SC 27 Standing Document 8 (SD 8)

SD 8 is publicly available at:
http://www.din.de/ni/sc27

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 15946 may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 2: Digital signatures

1 Scope

This part of ISO/IEC 15946 specifies public-key cryptographic techniques based on elliptic curves. They include the establishment of keys for secret-key systems, and digital signature mechanisms.

This part of ISO/IEC 15946 describes mechanisms for digital signatures. The mathematical background and general techniques necessary for implementing the mechanisms are described in part 1 of ISO/IEC 15946.

The scope of this part of ISO/IEC 15946 is restricted to cryptographic techniques based on elliptic curves defined over finite fields of prime power order (including the special cases of prime order and characteristic two). The representation of elements of the underlying finite field (i.e. which basis is used) is outside the scope of this part of ISO/IEC 15946.

This part of ISO/IEC 15946 does not fully specify the implementation of the techniques it defines. Thus, additional specification may be required to ensure the compatibility of products complying with this part of ISO/IEC 15946.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 15946. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/IEC 15946 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 10118 (all parts), *Information technology – Security techniques – Hash-functions*

ISO/IEC 15946-1, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General*

3 Symbols and abbreviated terms

For the purposes of this part of ISO/IEC 15946, the symbols, terms and definitions described in ISO/IEC 15946-1 apply. In addition, the following terms and symbols are used.

3.1 Terms and definitions

3.1.1 domain parameter

[ISO/IEC14888-1] A data item which is common to and known by or accessible to all entities within the domain.

NOTE The set of domain parameters may contain data items such as hash-function identifier, elliptic curve parameters, or other parameters specifying the security policy in the domain.

3.1.2 hash-code
[ISO/IEC 10118-1] The string of bits which is the output of a hash-function.

3.1.3 hash-function
[ISO/IEC 10118-1] A function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:

— for a given output, it is computationally infeasible to find an input which maps to this output; and

— for a given input, it is computationally infeasible to find a second input which maps to the same output.

NOTE Computational feasibility depends on the specific security requirements and environment.

3.1.4 message
[ISO/IEC 9796-1] A string of bits of any length.

3.1.5 randomizer
[ISO/IEC 14888-1] A secret data item produced by the signing entity in the pre-signature production process, and not predictable by other entities.

3.1.6 signature
[ISO/IEC 9796-1] The string of bits resulting from the signature process.

3.1.7 signature key
[ISO/IEC 14888-1] A secret data item specific to an entity and usable only by this entity in the signature process.

3.1.8 signature process
[ISO/IEC 14888-1] A process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature.

3.1.9 verification key
[ISO/IEC 14888-1] A data item which is mathematically related to an entity's signature key and which is used by the verifier in the verification process.

3.1.10 verification process
[ISO/IEC 14888-1] A process which takes as input the signed message, the verification key and the domain parameters, and which gives as output the result of the signature verification: valid or invalid.

3.2 Symbols and notation

In addition to the symbols and notation defined in ISO/IEC 15946-1, the following symbols and notation are used in this part of ISO/IEC 15946:

Cert_Data	certification data
e, e'	hash code and recovered hash code respectively
k	randomizer
m	positive integer
(*r,s*) , (*r',s'*)	signature and received signature respectively
M, *M'*	message and received message respectively
len_x	length in bits of *x*
h()	hash function

4 General Model for Digital Signatures with Appendix

This part of ISO/IEC 15946 describes signature schemes based on the one way property of discrete exponentiation on elliptic curves defined over some finite prime field $\boldsymbol{F}(p)$, some finite field $\boldsymbol{F}(2^m)$ or some finite extension field of $\boldsymbol{F}(p)$.

A digital signature scheme is defined by the specification of the following processes:

— Parameter generation process;

— Signature generation process;

— Signature verification process.

4.1 Parameter Generation Process

The parameters can be divided into domain parameters and user parameters.

4.1.1 Domain Parameters

The domain parameters consist of parameters to define a finite field, parameters to define an elliptic curve over the finite field, and other public information which is common to and known by or accessible to all entities within the domain. As well as the domain parameters for a general cryptographic scheme based on elliptic curves which are specified in ISO/IEC 15946-1, the following parameters are required to be specified:

— An identifier for the digital signature scheme used;

— An identifier for the hash function $\boldsymbol{h}()$ mapping an arbitrary message to a bit string of constant length;

— The user parameter generation procedure.

NOTE One of the domain parameters specified in ISO/IEC 15946-1 is the function $\pi()$ for converting a field element into an integer. It should be noted that operation of this function is trivial when the field is $\boldsymbol{F}(p)$ or $\boldsymbol{F}(2^m)$, but is not trivial when the field is $\boldsymbol{F}(p^m)$.

4.1.2 User Parameters

Each entity has its own public and private parameters. The user parameters of the entity A consist of the following:

— The private key d_A.

— The public key P_A.

— (Optional) Other information, which is specific to the entity A, for the use in the signature generation and/or verification process.

4.1.3 Validity of Parameters

The signature verifier may require assurance that the domain parameters and public key are valid, otherwise there is no assurance of meeting the intended security even if the signature verifies. The signer may also require assurance that the domain parameters and public key are valid, otherwise an adversary may be able to generate signatures that verify.

Assurance of validity of domain parameters can be provided by one of the following:

— Selection of valid domain parameters from a published source, such as a standard.

— Generation of valid domain parameters by a trusted third party, such as a Certification Authority.

— Validation of candidate domain parameters by a trusted third party, such as a Certification Authority.

— For the signer, generation of valid domain parameters by the signer using a trusted system.

— Validation of candidate domain parameters by the user (i.e., the signer or verifier).

Assurance of validity of a public key can be provided by one of the following:

— For the signer, generation of the public/private key pair using a trusted system.

— For the signer or verifier, validation of the public key by a trusted third party, such as a Certification Authority.

— Validation of the public key by the user (i.e., the signer or verifier).

4.2 Signature Generation Process

The following data items are required for the signature generation process:

— the domain parameters;

— the signer A's user parameters including the private key d_A;

— the message *M*.

For all the schemes the signature generation process consists of the following procedures:

— calculation of the message digest;

— elliptic curve computations;

— computations modulo the group order of the base point *G*.

The output of the signature generation process is a pair of integers (r,s) that constitutes A's digital signature of the message *M*.

4.2.1 Randomizer

Prior to each signature computation the signing entity must have a fresh, secret value of randomizer available. The randomizer is an integer *k* such that $0 < k < n$. The implementation of the signature scheme must ensure that the following two requirements are satisfied:

— The used randomizers are never disclosed, since knowledge of a randomizer and the signature generated using this randomizer can be used to compromise the private signature key.

— Randomizers are statistically unique, that is, the probability that the same randomizer is used to produce signatures for two different messages is negligible. If the same value of randomizer is used to produce signatures for two different messages, then the signature key can be deduced from the signatures.

4.3 Signature Verification Process

The following data items are required for the signature verification process:

— the domain parameters;

— the signer A's user parameters including the public key P_A but not the private key d_A;

— the received message, *M'*;

— the received signature of *M*, represented as the two integers, *r'* and *s'*.

For all the schemes the signature verification process consists of some or all of the following procedures:

— signature size verification;

— calculation of the message digest;

— computations modulo the group order of the base point G;

— elliptic curve computations;

— signature checking.

If all procedures are passed, the signature is accepted by the verifier, otherwise it is rejected.

5 EC-GDSA Signature Algorithm

The EC-GDSA signature scheme is an example of a mechanism producing a digital signature with appendix.

5.1 Domain and User Parameters

The bit length of n should be greater than the output bit length of the hash function $\boldsymbol{h}()$.

The private and public keys of entity A, d_A and P_A respectively, should be produced in accordance with the procedure 7.2 defined in ISO/IEC 15946-1.

5.2 Signature Generation Process

The input to the signature process consists of:

— the domain parameters;

— the signer's private key d_A;

— the message M.

The output of the signature generation process is a pair $(r,s) \in \boldsymbol{F}(n)^* \times \boldsymbol{F}(n)^*$ that constitutes A's digital signature of the message M.

To sign a message M, A executes the following steps:

5.2.1 Calculation of the message digest

1. Compute the hash-code $e = \boldsymbol{h}(M)$.

5.2.2 Elliptic Curve Computations (Arithmetic operations in the underlying field)

2. Select a random integer k in the interval $\{1, \ldots, n-1\}$.

3. Compute the elliptic curve point $(x_1, y_1) = kG$.

5.2.3 Computations modulo the group order of G (Arithmetic operations in $\boldsymbol{F}(n)$)

4. Set $r = \pi(kG) \bmod n$.

5. Set $s = (kr - e)d_A \bmod n$.

If the signature generation process yields either $s = 0$ or $r = 0$ then the process must be repeated from step 2 with a new random value k. (But note that the probability that either $r = 0$ or $s = 0$ is negligibly small if k is chosen as described in 5.2.2.)

NOTE Since the computation of r is independent of any message to be signed, r may be precomputed and stored for a later one-time use in a signing operation.

5.3 The Signature

The pair $(r,s) \in \boldsymbol{F}(n)^* \times \boldsymbol{F}(n)^*$ constitutes A's digital signature of the message *M*.

5.4 Signature Verification Process

The signature verification process consists of four steps: signature size verification; calculation of the message digest; elliptic curve computations, and signature checking.

The input to the signature verification process consists of:

— the domain parameters;

— A's public key P_A;

— the received message, *M'*;

— the received signature of *M*, represented as the two integers, *r'* and *s'*.

To verify A's signature of message *M'*, *B* executes the following steps:

5.4.1 Signature Size Verification

1. Verify that $0 < r' < n$ and $0 < s' < n$; if not, then reject the signature.

5.4.2 Calculation of the message digest

2. Compute the hash-code $e' = \boldsymbol{h}(M')$ using the hash function $\boldsymbol{h}()$.

5.4.3 Elliptic Curve Computations

3. Compute $w = (r')^{-1} \bmod n$.

4. Compute $u_1 = e'w \bmod n$ and $u_2 = s'w \bmod n$.

5. Compute the elliptic curve point $(x_1, y_1) = u_1 G + u_2 P_A$.

5.4.4 Signature Checking

6. Compute $v = \pi((x_1, y_1)) \bmod n$.

If $r' = v$, then the signature shall be accepted by the verifier. If $r' \neq v$, then the signature shall be rejected by the verifier.

6 EC-DSA

The signature scheme EC-DSA is the elliptic curve analogue of the DSA signature scheme. It is an example of a mechanism producing a digital signature with appendix.

6.1 Domain and User Parameters

The bit length of *n* should be greater than the output bit length of the hash function $\boldsymbol{h}()$.

The private and public keys of entity A, d_A and P_A respectively, should be produced in accordance with the procedure 7.1 defined in ISO/IEC 15946-1.

6.2 Signature Generation Process

The input to the signature process consists of: