INTERNATIONAL STANDARD

ISO/IEC 15946-3

First edition
2002-12-01

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

Part 3: Key establishment

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

Partie 3: Établissement de clé

Reference number
ISO/IEC 15946-3:2002(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 15946-3 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 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. In general, only algorithms that take exponential time are known to determine elliptic curve discrete logarithms. 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.

This part of ISO/IEC 15946 describes schemes that can be used for key agreement and schemes that can be used for key transport. Where possible, the schemes are analogous to methods included in ISO/IEC 11770-3. Schemes that are not included in ISO/IEC 11770-3 are noted as such.

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 3: Key establishment

1 Scope

International Standard ISO/IEC 15946 specifies public key cryptographic techniques based on elliptic curves. The standard is split into four parts and includes the establishment of keys for secret key systems and digital signature mechanisms.

This part of ISO/IEC 15946 specifies techniques for key establishment, which includes key agreement and key transport, that use elliptic curves.

The scope of this standard is restricted to cryptographic techniques based on elliptic curves defined over finite fields of prime power order (including the special cases of prime order or characteristic two). The representation of elements of the underlying finite field is outside the scope of this standard. This standard does not fully specify the implementation of the techniques it defines. There may be different products that comply with this International Standard and yet are not compatible.

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 9796 (parts 2 and 3), *Information technology — Security techniques — Digital signature schemes giving message recovery*

ISO/IEC 9797 (all parts), *Information technology — Security techniques — Message Authentication Codes (MACs)*

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

ISO/IEC 11770-3:1999, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

ISO/IEC 14888 (all parts), *Information technology — Security techniques — Digital signatures with appendix*

ISO/IEC 15946-1:2001, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General*

ISO/IEC 15946-2:2001, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 2: Digital signatures*

3 Terms and definitions

For the purposes of this part of ISO/IEC 15946, the definitions of Part 1 apply. In addition, the following definitions from ISO/IEC 11770-3 apply.

3.1 Asymmetric cryptographic technique: a cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation.

3.2 Asymmetric encipherment system: a system based on asymmetric cryptographic techniques whose public transformation is used for encipherment and whose private transformation is used for decipherment.

3.3 Asymmetric key pair: a pair of related keys where the private key defines the private transformation and the public key defines the public transformation.

3.4 Signature system: a system based on asymmetric cryptographic techniques whose private transformation is used for signing and whose public transformation is used for verification.

3.5 Cryptographic check function: a cryptographic transformation which takes as input a secret key and an arbitrary string, and which gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key shall be infeasible [ISO/IEC 9798-1:1997].

3.6 Cryptographic check value: information which is derived by performing a cryptographic transformation on the data unit [ISO/IEC 9798-4:1995].

NOTE The cryptographic check value is the output of the cryptographic check function.

3.7 Decipherment: the reversal of a corresponding encipherment [ISO/IEC 11770-1:1996].

3.8 Digital signature: data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the origin and integrity of the data unit and protect against forgery, e.g. by the recipient [ISO/IEC 11770-1:1996].

3.9 Distinguishing identifier: information which unambiguously distinguishes an entity [ISO/IEC 11770-1:1996].

3.10 Encipherment: the (reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e. to hide the information content of the data [ISO/IEC 9798-1:1997].

3.11 Entity authentication: the corroboration that an entity is the one claimed [ISO/IEC 9798-1:1997].

3.12 Entity authentication of A to B: the assurance of the identity of entity A for entity B.

3.13 Explicit key authentication from A to B: the assurance for entity B that A is the only other entity that is in possession of the correct key.

NOTE Implicit key authentication from A to B and key confirmation from A to B together imply explicit key authentication from A to B.

3.14 Implicit key authentication from A to B: the assurance for entity B that A is the only other entity that can possibly be in possession of the correct key.

3.15 Key: a sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature generation, signature verification, or key agreement) [ISO/IEC 11770-1:1996].

3.16 Key agreement: the process of establishing a shared secret between entities in such a way that neither of them can predetermine the value of that key.

3.17 Key confirmation from A to B: the assurance for entity B that entity A is in possession of the correct key.

3.18 Key control: the ability to choose the key or the parameters used in the key computation.

3.19 Key establishment: the process of making available a shared secret to one or more entities. Key establishment includes key agreement and key transport.

3.20 Key token: key management message sent from one entity to another entity during the execution of a key management mechanism.

3.21 Key transport: the process of transferring a key from one entity to another entity, suitably protected.

3.22 Mutual entity authentication: entity authentication which provides both entities with assurance of each other's identity.

3.23 One-way function: a function with the property that it is easy to compute the output for a given input but it is computationally infeasible to find for a given output an input which maps to this output.

3.24 Private key: that key of an entity's asymmetric key pair which should only be used by that entity.

NOTE In the case of an asymmetric signature system the private key defines the signature transformation. In the case of an asymmetric encipherment system the private key defines the decipherment transformation.

3.25 Public key: that key of an entity's asymmetric key pair which can be made public

NOTE In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group.

3.26 Secret key: a key used with symmetric cryptographic techniques by a set of specified entities.

3.27 Sequence number: a time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period [ISO/IEC 11770-1:1996].

3.28 Time stamp: a data item which denotes a point in time with respect to a common reference [ISO/IEC 11770-1:1996].

The following definition from ISO/IEC 10118-1 applies.

3.29 hash-function: a function which maps strings of bits to fixed-length strings of bits, satisfying two properties.

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

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

NOTES

1 – The literature on this subject contains a variety of terms which have the same or similar meaning as hash-function. Compressed encoding and condensing function are some examples.

2 – Computational feasibility depends on the user's specific security requirements and environment.

Additional definitions which are required are as follows.

3.30 Forward secrecy with respect to *A*: the property that knowledge of A's long-term private key subsequent to a key agreement operation does not enable an opponent to recompute previously derived keys.

3.31 Forward secrecy with respect to both A and B individually: the property that knowledge of A's long-term private key or knowledge of B's long-term private key subsequent to a key agreement operation does not enable an opponent to recompute previously derived keys.

NOTE This differs from mutual forward secrecy in which knowledge of both A's and B's long-term private keys does not enable recomputation of previously derived keys.

3.32 Key derivation function: a key derivation function outputs one or more shared secrets, used as keys, given shared secrets and other mutually known parameters as input.

3.33 Mutual forward secrecy: the property that knowledge of both A's and B's long-term private keys subsequent to a key agreement operation does not enable an opponent to recompute previously derived keys.

3.34 Prefix free representation: a representation of a data element for which concatenation with any other data does not produce a valid representation.

4 Symbols and abbreviated terms

Throughout this part of ISO/IEC 15946, the following symbols and notations are used in addition to those given in ISO/IEC 15946-1.

E_K	Symmetric encryption function using secret key K.
f	A cryptographic check function.
$f_K(Z)$	A cryptographic check value which is the result of applying the cryptographic check function f using as input a secret key K and an arbitrary data string Z.
h	The cofactor used in performing cofactor multiplication.
kdf	A key derivation function.
l	A supplementary value used in performing cofactor multiplication.
MAC	A Message Authentication Code algorithm.
MAC(K,Z)	A Message Authentication Code value which is the result of applying the MAC algorithm using as input the secret key *K* and an arbitrary data string *Z*.
parameters	Parameters used in the key derivation function.
S_X	Entity *X*'s private signature transformation.

NOTE No assumption is made on the nature of the signature transformation. In the case of a signature system with message recovery, $S_A(m)$ denotes the signature itself. In the case of a signature system with appendix, $S_A(m)$ denotes the message *m* together with the signature.

[|| *Text1*], [|| *Text2*]	Optional text, data or other information that may be included in a data block, if desired.
V_X	Entity *X*'s public signature verification transformation.
$\pi^*(\mathrm{Q})$	$(\pi(\mathrm{Q}) \bmod 2^{\lceil \rho/2 \rceil}) + 2^{\lceil \rho/2 \rceil}$ where $\rho = \lceil \log_2 n \rceil$.