INTERNATIONAL STANDARD

ISO/IEC 29150

First edition
2011-12-15

Information technology — Security techniques — Signcryption

Technologies de l'information — Techniques de sécurité — Signcryptage

Reference number
ISO/IEC 29150:2011(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

Page

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. 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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29150 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

When data is sent from one place to another, it is often necessary to protect it in some way whilst it is in transit, e.g. against eavesdropping or unauthorized modification. Similarly, when data is stored in an environment to which unauthorized parties can have access, it is important to protect it against unauthorized access.

If the confidentiality of the data needs to be protected, e.g. against eavesdropping, then one solution is to use public key encryption, as specified in ISO/IEC 18033. Alternatively, if it is necessary to protect the data against unauthorized modification or forgery, then digital signatures, as specified in ISO/IEC 9796 and ISO/IEC 14888, can be used. If both confidentiality and unforgeability are required, then one possibility is to use both public key encryption and digital signature. Whilst these operations can be combined in many ways, not all combinations of such mechanisms provide the same security guarantees. As a result it is desirable to define in detail exactly how confidentiality and unforgeability mechanisms should be combined to provide the optimum level of security. Moreover, in some cases significant efficiency gains can be obtained by defining a single method of processing the data with the objective of providing both confidentiality and unforgeability.

In this International Standard, *signcryption mechanisms* are defined. These are methods for processing data to provide both confidentiality and unforgeability. These data processing methods typically involve either the use of an asymmetric encryption scheme and a digital signature scheme combined in a specific way or the use of a specially developed algorithm which fulfils both functions simultaneously.

The methods specified in this International Standard have been designed to maximise the level of security and provide efficient processing of data. All the mechanisms defined here have mathematical “proofs of security”, i.e. rigorous arguments supporting their security claims.

Information technology — Security techniques — Signcryption

1 Scope

This International Standard specifies four mechanisms for signcryption that employ public key cryptographic techniques requiring both the originator and the recipient of protected data to have their own public and private key pairs.

This International Standard is not applicable to infrastructures for management of public keys which are defined in ISO/IEC 11770-1 and ISO/IEC 9594.

NOTE 1 Signcryption mechanisms are defined ways of processing a data string with the following security objectives:

— **data confidentiality**, i.e. protection against unauthorized disclosure of data;

— **data integrity**, i.e. protection that enables the recipient of data to verify that it has not been modified;

— **data origin authentication**, i.e. protection that enables the recipient of data to verify the identity of the data originator;

— **data unforgeability**, i.e. protection against unauthorized modification of data, even by a recipient of the data.

These four security objectives are not necessarily mutually exclusive. The fourth objective, data unforgeability, in particular is a stronger notion of security that implies both data integrity and data origin authentication.

NOTE 2 Two of the mechanisms specified in this International Standard, namely mechanisms DLSC and ECDLSC, require the employment of system wide public key parameters for both the sender and the recipient of data. In a system where a multiple number of pairs of senders and recipients exist, the same system wide parameters are required to be used by all these users. The two remaining specified mechanisms, namely IFSC and EtS, do not require the use of such system wide public key parameters.

NOTE 3 In selecting the four signcryption mechanisms for inclusion in this International Standard from the large variety of such techniques published and in use, the same seven criteria as those stated in ISO/IEC 18033-1:2005, Annex A, have been followed. The exclusion of particular methods does not imply that those methods are insecure.

NOTE 4 This International Standard bears a conceptual similarity to ISO/IEC 19772[14] which specifies a number of mechanisms for authenticated encryption, that is, simultaneously achieving message integrity and confidentiality. Major differences between ISO/IEC 19772 and this International Standard include (1) mechanisms specified in ISO/IEC 19772 fall into the category of symmetric cryptographic techniques, whereas those specified in this International Standard are representatives of asymmetric cryptographic techniques; (2) while all mechanisms specified in ISO/IEC 19772 and this International Standard offer the capability of data integrity and origin authentication, mechanisms specified in this International Standard further offer the capability of data unforgeability, even by a recipient of the data.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9796-2:2010, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

ISO/IEC 9796-3:2006, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms*

ISO/IEC 14888-1:2008, *Information technology — Security techniques — Digital signatures with appendix — Part 1: General*

ISO/IEC 14888-2:2008, *Information technology — Security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms*

ISO/IEC 14888-3:2006, *Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*

ISO/IEC 18033-1:2005, *Information technology — Security techniques — Encryption algorithms — Part 1: General*

ISO/IEC 18033-2:2006, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
asymmetric cipher
alternative term for asymmetric encryption system

[ISO/IEC 18033-1:2005]

3.2
asymmetric cryptographic technique
cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key)

[ISO/IEC 11770-1:2010]

3.3
asymmetric encryption system
system based on asymmetric cryptographic techniques whose public transformation is used for encryption and whose private transformation is used for decryption

[ISO/IEC 9798-1:2010]

3.4
asymmetric key pair
pair of related keys where the private key defines the private transformation and the public key defines the public transformation

[ISO/IEC 9798-1:2010]

3.5
block
string of bits of a defined length

3.6
block cipher
symmetric encryption system with the property that encryption operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext, and decryption operates on the ciphertext to yield the original plaintext

[ISO/IEC 18033-1:2005]

3.7
cipher
alternative term for encryption system

[ISO/IEC 18033-1:2005]

3.8
ciphertext
data which has been transformed to hide its information content

[ISO/IEC 10116:2006]

3.9
cleartext
alternative term for plaintext

3.10
collision-resistant hash-function
hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output

[ISO/IEC 10118-1:2000]

3.11
data element
integer or bit string or set of integers or set of bit strings

3.12
decryption
reversal of encryption by a cryptographic algorithm to produce a plaintext

3.13
decryption algorithm
process which transforms a ciphertext into a plaintext

[ISO/IEC 18033-1:2005]

3.14
domain
set of entities operating under a single security policy

[ISO/IEC 14888-1:2008]

3.15
domain parameter
data element which is common to and known by or accessible to all entities within the domain

[ISO/IEC 14888-1:2008]

3.16
encryption
(reversible) transformation of data by a cryptographic algorithm to produce a ciphertext, i.e. to hide the information content of the data

NOTE Adapted from ISO/IEC 9797-1:2011.

3.17
encryption algorithm
process which transforms a plaintext into a ciphertext

[ISO/IEC 18033-1:2005]

3.18
encryption system
cryptographic technique used to protect the confidentiality of data, and which consists of three component processes: a method for generating keys, an encryption algorithm and a decryption algorithm

3.19
full domain cryptographic hash function
function that maps strings of bits to integers in a fixed range, satisfying the properties of (1) for a given output, it is computationally infeasible to find an input which maps to this output, and (2) for a given input, it is computationally infeasible to find a second input which maps to the same output

NOTE A full domain cryptographic hash function is similar to a standard cryptographic hash function with the exception that the former outputs an integer rather than a bit string; see 7.2.2.

3.20
identification data
sequence of data elements, including the distinguishing identifier for an entity, assigned to an entity and used to identify it

NOTE The identification data can additionally contain data elements such as identifier of the signature process, identifier of the signature key, validity period of the signature key, restrictions on key usage, associated security policy parameters, key serial number, or domain parameters.

[ISO/IEC 14888-1:2008]

3.21
key
sequence of symbols that controls the operation of a cryptographic transformation (e.g. encryption, decryption)

[ISO/IEC 11770-1:2010]

3.22
key pair
pair consisting of a public key and a private key associated with an asymmetric cipher

3.23
keystream
pseudorandom sequence of symbols, intended to be secret, used by the encryption and decryption algorithms of a stream cipher

NOTE If a portion of the keystream is known by an attacker, then it is computationally infeasible for the attacker to deduce any information about the remainder of the keystream.

3.24
message
string of bits of any length

3.25
***n*-bit block cipher**
block cipher with the property that plaintext blocks and ciphertext blocks are *n* bits in length

[ISO/IEC 10116:2006]

3.26
one-way hash function
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;
- for a given input, it is computationally infeasible to find a second input which maps to the same output

[ISO/IEC 10118-1:2000]

3.27
parameter
integer or bit string or function

3.28
plaintext
unencrypted information

[ISO/IEC 10116:2006]

3.29
private key
that key of a key pair associated with an entity's asymmetric cipher which is kept secret and used by that entity only

[ISO/IEC 11770-1:2010]

3.30
public key
that key of a key pair associated with an entity's asymmetric cipher which can be made public and used by any entity

[ISO/IEC 11770-1:2010]

3.31
secret key
key used with symmetric cryptographic techniques by a specified set of entities

[ISO/IEC 11770-3:2008]

3.32
signature
one or more data elements resulting from the signature process

3.33
signature key
set of private data elements specific to an entity and usable only by this entity in the signature process

[ISO/IEC 14888-1:2008]

3.34
signature process
process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature

3.35
signcrypt
to apply signcryption on a plaintext

3.36
signcryption
(reversible) transformation of data by a cryptographic algorithm to produce a ciphertext from which no information about the original data can be recovered (except possibly its length), nor can a new ciphertext be forged by an unauthorized entity without detection, that is, it provides data confidentiality, data integrity, data origin authentication, and non-repudiation

NOTE Unforgeability implies data integrity, data origin authentication, and non-repudiation.

3.37
signcryption algorithm
one of the three component algorithms of a signcryption mechanism which takes as input a plaintext, a sender's public and private key pair, a recipient's public key and other data, outputs a ciphertext after performing a sequence of specified operations on the input

3.38
signcryption mechanism
cryptographic technique used to protect the confidentiality and simultaneously guarantee the origin, integrity and non-repudiation of data, and which consists of three component algorithms: a key generation algorithm, a signcryption algorithm and a unsigncryption algorithm

3.39
signed message
set of data elements consisting of the signature, the part of the message which cannot be recovered from the signature, and an optional text field

[ISO/IEC 14888-1:2008]

3.40
symmetric cipher
cipher based on symmetric cryptographic techniques that uses the same secret key for both the encryption and decryption algorithms

[ISO/IEC 18033-1:2005]

3.41
symmetric cryptographic technique
cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation

NOTE 1 Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation.

NOTE 2 Examples of symmetric cryptographic techniques include symmetric ciphers and Message Authentication Codes (MACs). In a symmetric cipher, the same secret key is used to encrypt and decrypt data. In a MAC, the same secret key is used to generate and verify MACs.

3.42
unsigncrypt
to apply unsigncryption on a ciphertext

3.43
unsigncryption
verification and decryption of a ciphertext by a cryptographic algorithm

3.44
unsigncryption algorithm
one of the three component algorithms of a signcryption mechanism which takes as input a ciphertext, a recipient's public and private key pair, a sender's public key and other data, outputs a pair consisting of either a symbolic value ACCEPT and a plaintext, or a symbolic value REJECT and the null string

3.45
verification key
set of public data elements which is mathematically related to an entity's signature key and which is used by the verifier in the verification process

[ISO/IEC 14888-1:2008]

3.46
verification process
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

[ISO/IEC 14888-1:2008]

4 Symbols and notations

For the purposes of this International Standard, the following symbols and notations apply:

$\lfloor x \rfloor$ the largest integer less than or equal to real number x. For example, $\lfloor 8 \rfloor = 8$, $\lfloor 8.7 \rfloor = 8$ and $\lfloor -10.4 \rfloor = -11$.

$\lceil x \rceil$ the smallest integer greater than or equal to real number x. For example, $\lceil 8 \rceil = 8$, $\lceil 8.2 \rceil = 9$, and $\lceil -9.5 \rceil = -9$.

$[a,...,b]$ the interval of integers from a to b, including both a and b.

$(a,...,b)$ the interval of integers from a to b, but excluding both a and b.

$|X|$ if X is a finite set, then the cardinality of X, namely the number of elements in the set X; if X is a finite abelian group or a finite field, then the cardinality of the underlying set of elements; if X is a real number, then the absolute value of X; if X is a bit string, then the length in bits of the string.

$x \oplus y$ the bit-wise exclusive-or (XOR) of two bit strings x and y, where x and y are of equal length. (See also 6.1.)

$\langle x_1,\ldots,x_l \rangle$ the bit string of length l consisting of l bits $x_1,...,x_l$ in the given order. (See also 6.1.)

$x \| y$ The result of concatenating two data items x and y in the order specified. In cases where the result of concatenating two or more data items is input to a cryptographic algorithm as part of a signcryption mechanism, this result shall be composed so that it can be uniquely resolved into its constituent data strings, i.e. so that there is no possibility of ambiguity in interpretation. This latter property can be achieved in a variety of different ways, depending on the application. For example, it can be guaranteed by (a) fixing the length of each of the substrings throughout the domain of use of the mechanism, or (b) encoding the sequence of concatenated strings using a method that guarantees unique decoding, e.g. using the distinguished encoding rules defined in ISO/IEC 8825-1 [6].

$\gcd(a,b)$ the greatest common divisor of two integers a and b.

$a \mid b$ integer a divides integer b; that is, there exists an integer c such that $b = ca$.

$a \equiv b \pmod{n}$	integer a and integer b are congruent modulo non-zero integer n; that is $n \mid (a-b)$.
$a \mod n$	the unique remainder in $[0,...,n-1]$ when integer a is divided by positive integer n.
$a^{-1} \mod n$	for integer a and positive integer n such that $\gcd(a,n)=1$, the unique integer b in $[1,...,n-1]$ such that $ab \equiv 1 \pmod{n}$.
$L_b(n)$	the length in bits of a non-negative integer n, or the smallest integer l such that $\mathrm{I2BSP}(n,l)$ does not fail; that is, $L_b(n) = \lceil \log_2(n+1) \rceil$, where $\mathrm{I2BSP}(n,l)$, defined in 6.2, converts integer n to a bit string of length l.
AC.Decrypt	decryption algorithm for an asymmetric cipher.
AC.Encrypt	encryption algorithm for an asymmetric cipher.
AC.KeyGen	key generation algorithm for an asymmetric cipher.
ID_X	bit string which uniquely identifies entity X in some context.
pk_d	private decryption key.
pk_s	private signature generation key.
pk_X	private key belonging to the entity X.
$pk_{X,d}$	private decryption key belonging to the entity X.
$pk_{X,s}$	private signature generation key belonging to the entity X.
PK_e	public encryption key.
PK_v	public signature verification key.
PK_X	public key belonging to the entity X.
$PK_{X,e}$	public encryption key belonging to the entity X.
$PK_{X,v}$	public signature verification key belonging to the entity X.
SS.KeyGen	key generation algorithm for a signature scheme.
SS.Sign	signature generation algorithm for a signature scheme.
SS.Verify	signature verification algorithm for a signature scheme.

5 Finite fields and elliptic curves

5.1 Finite fields

This clause describes a very general framework for representing specific finite fields. A finite field specified in this way is called an explicitly given finite field, and it is determined by explicit data.

For a finite field F of cardinality p^e, where p is prime and $e \geq 1$, explicit data for F consists of p and e, along with a "multiplication table" which is a matrix $T = (T_{ij})_{1 \leq i,j \leq e}$, where each T_{ij} is an e-tuple, or an ordered list of e elements, over $[0,..., p-1]$.

The set of elements of F is the set of all e-tuples over $[0,...,p-1]$. The entries of T are themselves viewed as elements of F.

Addition in F is defined element-wise: if $a=(a_1,\ldots,a_e)\in F$ and $b=(b_1,\ldots,b_e)\in F$, then $a+b=c$, where

$$c=(c_1,\ldots,c_e) \text{ and } c_i=(a_i+b_i) \bmod p \ (1\le i\le e).$$

A scalar multiplication operation for F is also defined element-wise: if $a=(a_1,\ldots,a_e)\in F$ and $d\in[0,\ldots,p-1]$, then $d\cdot a=c$, where

$$c=(c_1,\ldots,c_e) \text{ and } c_i=(d\cdot a_i) \bmod p \ (1\le i\le e).$$

Multiplication in F is defined via the multiplication table T, as follows: if $a=(a_1,\ldots,a_e)\in F$ and $b=(b_1,\ldots,b_e)\in F$, then

$$a\cdot b=\sum_{i=1}^{e}\sum_{j=1}^{e}\left[\left(a_i b_j \bmod p\right)T_{ij}\right]$$

where the products $\left(a_i b_j \bmod p\right)T_{ij}$ are defined using the above rule for scalar multiplication, and where these products are summed using the above rule for addition in F. It is assumed that the multiplication table defines an algebraic structure that satisfies the usual axioms of a field; in particular, there exist additive and multiplicative identities, every element has an additive inverse, and every element besides the additive identity has a multiplicative inverse.

Observe that the additive identity of F, denoted 0_F, is the all-zero e-tuple, and that the multiplicative identity of F, denoted 1_F, is a non-zero e-tuple whose precise format depends on T.

NOTE 1 The field F is a vector space of dimension e over the prime field F' of cardinality p, where scalar multiplication is defined as above. The prime p is called the characteristic of F. For $1\le i\le e$, let θ_i denote the e-tuple over F' whose i-th component is 1, and all of whose other components are 0. The elements $\theta_1,...,\theta_e$ form an ordered basis of F as a vector space over F'. Note that for $1\le i,j\le e$, we have $\theta_i\cdot\theta_j=T_{ij}$.

NOTE 2 For $e>1$, two types of standard bases are defined that are commonly used in implementations of finite field arithmetic, namely *polynomial basis* and *normal basis*.

- Polynomial basis: $\theta_1,...,\theta_e$ are called a polynomial basis for F over F' if for some $\theta\in F$, $\theta_i=\theta^{e-i}$ for $1\le i\le e$. Note that in this case, $1_F=\theta_e$.
- Normal basis: $\theta_1,...,\theta_e$ are called a normal basis for F over F' if for some $\theta\in F$, $\theta_i=\theta^{p^{i-1}}$ for $1\le i\le e$. Note that in this case, $1_F=c\sum_{i=1}^{e}\theta_i$ for some $c\in[1,...,p)$; if $p=2$, then the only possible choice for c is 1; moreover, one can always choose a normal basis for which $c=1$.

NOTE 3 The definition given here of an explicitly given finite field comes from ISO/IEC 18033-2.

5.2 Elliptic curves

An elliptic curve V over an explicitly given finite field F is a set of points $P=(x,y)$, where x and y are elements of F that satisfy a certain equation, together with the "point at infinity" which is denoted by O. For the purposes of this International Standard, the curve V is specified by two field elements $a,b\in F$, called the coefficients of V.