INTERNATIONAL STANDARD

ISO/IEC 14888-3

Third edition
2016-03-15

Corrected version
2017-09

Information technology — Security techniques — Digital signatures with appendix —

Part 3:
Discrete logarithm based mechanisms

Technologies de l'information — Techniques de sécurité — Signatures numériques avec appendice —

Partie 3: Mécanismes basés sur un logarithme discret

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 14888-3:2016
https://standards.iteh.ai/catalog/standards/sist/bef710e2-21d1-4e33-bf4b-fc21a10d7645/iso-iec-14888-3-2016

Reference number
ISO/IEC 14888-3:2016(E)

© ISO/IEC 2016

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 14888-3:2016
https://standards.iteh.ai/catalog/standards/sist/bef710e2-21d1-4e33-bf4b-fc21a10d7645/iso-iec-14888-3-2016

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 14888-3:2016
https://standards.iteh.ai/catalog/standards/sist/bef710e2-21d1-4e33-bf4b-fc21a10d7645/iso-iec-14888-3-2016

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 14888-3:2016
https://standards.iteh.ai/catalog/standards/sist/bef710e2-21d1-4e33-bf4b-fe21a10d7645/iso-iec-14888-3-2016

© ISO/IEC 2016 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 14888-3:2016
https://standards.iteh.ai/catalog/standards/sist/bef710e2-21d1-4e33-bf4b-fc21a10d7645/iso-iec-14888-3-2016

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 14888-3:2016
https://standards.iteh.ai/catalog/standards/sist/bef710e2-21d1-4e33-bf4b-fc21a10d7645/iso-iec-14888-3-2016

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

This third edition cancels and replaces the second edition (ISO/IEC 14888-3:2006), which has been technically revised. It also incorporates the Amendments ISO/IEC 14888-3:2006/Amd 1:2010 and ISO/IEC 14888-3:2006/Amd 2:2012 and the Technical Corrigenda ISO/IEC 14888-3:2006/Cor 1:2007 and ISO/IEC 14888-3:2006/Cor 2:2009.

This corrected version of ISO/IEC 14888-3:2016 incorporates the following corrections:

— the formula has been changed in 5.1.1.2;

— “G^{x-1}” has been changed to “ $G^{x^{-1}}$ ” in 6.3.1 and 6.3.3;

— “β” has been changed to “ β' ” in 6.7.1, 6.7.4.4 and 6.7.4.5;

— the reference has been changed in 6.9.1;

— the code for K has been changed in F.9.2.4.

A list of all parts in the ISO/IEC 14888 series can be found on the ISO website.

Introduction

Digital signature mechanisms can be used to provide services such as entity authentication, data origin authentication, non-repudiation and data integrity. A digital signature mechanism satisfies the following requirements.

- Given either or both of the following two things:
  - the verification key, but not the signature key;
  - a set of signatures on a sequence of messages that an attacker has adaptively chosen;

  it should be computationally infeasible for the attacker
  - to produce a valid signature on a new message,
  - in some circumstances, to produce a new signature on a previously signed message, or
  - to recover the signature key;
- it should be computationally infeasible, even for the signer, to find two different messages with the same signature.

NOTE 1 Computational feasibility depends on the specific security requirements and environment.

NOTE 2 In some applications, producing a new signature on a previously signed message without knowing the signature key is allowed. One example of such applications is a membership credential in an anonymous digital signature mechanism as specified in ISO/IEC 20008.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 14888-3:2016
https://standards.iteh.ai/catalog/standards/sist/bef710e2-21d1-4e33-bf4b-fc21a10d7645/iso-iec-14888-3-2016

Digital signature mechanisms are based on asymmetric cryptographic techniques and involve the following three basic operations:

- a process for generating pairs of keys, where each pair consists of a private signature key and the corresponding public verification key;
- a process that uses the signature key, called the signature process;
- a process that uses the verification key, called the verification process.

The following are the two types of digital signature mechanisms:

- when, for a given signature key, any two signatures produced for the same message are always identical, the mechanism is said to be deterministic (or non-randomized) (see ISO/IEC 14888-1 for further details);
- when, for a given message and signature key, any two applications of the signature process produce (with high probability) two distinct signatures, the mechanism is said to be randomized (or non-deterministic).

The mechanisms specified in this part of ISO/IEC 14888 are all randomized.

Digital signature mechanisms can also be divided into the following two categories:

- when the whole message has to be stored and/or transmitted along with the signature, the mechanism is termed a "signature mechanism with appendix" (such mechanisms are the subject of ISO/IEC 14888);
- when the whole message, or part of it, can be recovered from the signature, the mechanism is termed a "signature mechanism giving message recovery" (ISO/IEC 9796 specifies mechanisms in this category).

The verification of a digital signature requires access to the signing entity’s verification key. It is, thus, essential for a verifier to be able to associate the correct verification key with the signing entity, or more precisely, with (parts of) the signing entity's identification data. This association between the signer's identification data and the signer's public verification key can either be guaranteed by an outside entity or mechanism, or the association can be somehow inherent in the verification key itself. In the former case, the scheme is said to be "certificate-based." In the latter case, the scheme is said to be "identity based." Typically, in an identity-based scheme, the verifier can calculate the signer's public verification key from the signer's identification data. The digital signature mechanisms specified in this part of ISO/IEC 14888 are classified into certificate-based and identity-based mechanisms.

NOTE 3 For certificate-based mechanisms, various PKI standards can be used as the basis of key management. For further information, see ISO/IEC 9594-8 (also known as X.509), ISO/IEC 11770-3 and ISO/IEC 15945.

The security of a signature mechanism is based on an intractable computational problem, i.e. a problem for which, given current knowledge, finding a solution is computationally infeasible, such as the factorization problem and the discrete logarithm problem. This part of ISO/IEC 14888 specifies digital signature mechanisms with appendix based on the discrete logarithm problem, and ISO/IEC 14888-2 specifies digital signature mechanisms with appendix based on the factorization problem.

NOTE 4 The first edition of ISO/IEC 14888 grouped identity-based mechanisms into ISO/IEC 14888-2 and certificate-based mechanisms into ISO/IEC 14888-3, with both parts covering mechanisms based on both the discrete logarithm and the factorization problems. Since the second edition was published, the mechanisms have been reorganized. ISO/IEC 14888-2 now contains integer factoring-based mechanisms, and this part of ISO/IEC 14888 now contains discrete logarithm based mechanisms.

This part of ISO/IEC 14888 includes 12 mechanisms, two of which were in ISO/IEC 14888-3:1998, three of which were from ISO/IEC 15946-2:2002 and three of which were added in ISO/IEC 14888-3:2006. The Elliptic Curve Russian Digital Signature Algorithm (EC-RDSA) and three mechanisms based on Schnorr digital signature are added in ISO/IEC 14888-3:2006/Amd.1:2010.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The mechanisms specified in this part of ISO/IEC 14888 use a collision resistant hash-function to hash the message being signed (possibly in more than one part). ISO/IEC 10118 specifies hash-functions.

ISO/IEC 14888-3:2016
https://standards.iteh.ai/catalog/standards/sist/057182-2181-4e53-9f48-fe21af0d7643/iso-iec-14888-3-2016

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this part of ISO/IEC 14888 may involve the use of patents.

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

The holder of these patent rights has assured the ISO and IEC that he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with the ISO and IEC. Information regarding relevant patents is given in the following:

Certicom Corp.

4701 Tahoe Blvd., Building A, Mississauga, ON L4W0B5 Canada.

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 14888 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.

ISO (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up to date information concerning patents.

NOTE 5 The mechanisms of EC-DSA, EC-GDSA. EC-RDSA and EC-FSDSA may be vulnerable to a key substitution attack.[10] The attack is realized if an adversary can find two distinct public keys and one signature such that the signature is valid for both public keys. There are several approaches of avoiding this attack and its possible impact on the security of a cryptographic system. For example, the public key corresponding to the private signing key can be added into the message to be signed.

© ISO/IEC 2016 – All rights reserved

INTERNATIONAL STANDARD **ISO/IEC 14888-3:2016(E)**

Information technology — Security techniques — Digital signatures with appendix —

Part 3:
Discrete logarithm based mechanisms

1 Scope

This part of ISO/IEC 14888 specifies digital signature mechanisms with appendix whose security is based on the discrete logarithm problem.

This part of ISO/IEC 14888 provides

- a general description of a digital signature with appendix mechanism, and
- a variety of mechanisms that provide digital signatures with appendix.

For each mechanism, this part of ISO/IEC 14888 specifies

- the process of generating a pair of keys,
- the process of producing signatures, and
- the process of verifying signatures.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 14888-3:2016
https://standards.iteh.ai/catalog/standards/sist/bef710e2-21d1-4e33-bf4b-fc21a10d7645/iso-iec-14888-3-2016

2 Normative references

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

ISO/IEC 10118-3, *Information technology — Security techniques — Hash-functions*

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 14888-1 and the following apply.

3.1
finite commutative group
finite set E with the binary operation "*" such that

- for all group elements $a, b \in E$, $a * b \in E$;
- for all group elements $a, b, c \in E$, $(a * b) * c = a * (b * c)$;
- there exists a group element $e \in E$ with $e * a = a$ for all $a \in E$, where e is called the identity element of the group;
- for all group elements $a \in E$, there exists a group element $b \in E$ with $b * a = e$;

— for all group elements $a, b \in \mathbb{E}$, $a * b = b * a$

Note 1 to entry: In some cases, such as when $\mathbb{E}$ is the set of points on an elliptic curve, arithmetic in the finite set $\mathbb{E}$ is described with additive notation.

3.2

cyclic group

finite commutative group (3.1), $\mathbb{E}$, of n elements that contains a group element $a \in \mathbb{E}$, called the generator, of order n

3.3

elliptic curve group

cyclic group (3.2) defined on the points of an elliptic curve over a finite field

Note 1 to entry: Let $\boldsymbol{F} = GF(r)$ denote the Galois field with cardinality, r, where either r is an odd prime, p, or r is equal to 2^m, for some positive integer, m. An elliptic curve defined over $\boldsymbol{F}$ can be determined by an affine curve formula, either of the form $y^2 = x^3 + a_1x + a_2$ (when $r = p$ for some odd prime p) or of the form $y^2 + xy = x^3 + a_1x^2 + a_2$ (when $r = 2^m$ for some positive integer m), where the coefficients a_1 and a_2 are (appropriately chosen) elements of $\boldsymbol{F}$. The corresponding elliptic curve E consists of a collection of certain affine points from $\boldsymbol{F} \times \boldsymbol{F}$ together with a special (non-affine) point “at infinity”. An affine point P of E is one that can be represented as an ordered pair $(P_x, P_y) \in \boldsymbol{F} \times \boldsymbol{F}$, such that the selection of $x = P_x$ and $y = P_y$ satisfies the given affine curve formula when the indicated arithmetic is performed in the field, $\boldsymbol{F}$. Let “**+**” denote the binary operation known as “elliptic-curve addition”, defined for (most) affine points of E by the well-known secant-and-tangent rules. Once the collection of affine points of E is augmented by 0_E, a special point of E “at infinity” that serves as the identity element for “**+**” (but is not represented as an ordered pair), the set E together with the binary operation “**+**” forms a finite, commutative, elliptic-curve group, $\mathbb{E}$.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Note 2 to entry: The cardinality of the elliptic-curve group, $\mathbb{E}$, is one more than the number of ordered pairs in $\boldsymbol{F} \times \boldsymbol{F}$ that satisfy the affine curve formula for E.

3.4

order (of a group element *a*)

ISO/IEC 14888-3:2016
https://standards.iteh.ai/catalog/standards/sist/bcef710e2-21d1-4c23-bf4b-fc21a10d7645/iso-iec-14888-3-2016

least positive integer n such that $a^n = e$, where e is the identity element of the group, a^n is defined recursively such that $a^0 = e$ and $a^n = a * a^{m-1}$ ($m > 0$), and * is the group operation

3.5

pairing

function which takes two elements, P and Q, from an *elliptic curve group* (3.3) over a finite field, G_1, as input, and produces an element from another *cyclic group* (3.2) over a finite field, G_2, as output, and which has the following two properties (where it is assumed that the cyclic groups, G_1 and G_2 have order q, for some prime q, and for any two elements P, Q, the output of the pairing function is written as $<P, Q>$)

— Bilinearity: If P, P_1, P_2, Q, Q_1, Q_2 are elements of G_1, and a is an integer satisfying $1 \le a \le q - 1$, then

$$<P_1 + P_2, Q> = <P_1, Q> * <P_2, Q>, <P, Q_1 + Q_2> = <P, Q_1> * <P, Q_2>, \text{ and } <[a]P, Q> = <P, [a]Q> = <P, Q>^a$$

— Non-degeneracy: If P is a non-identity element of G_1, $<P, P> \neq 1$

3.6

trusted key generation centre

KGC

trusted third party, which, in an identity-based signature mechanism, generates a private signature key for each signing entity

© ISO/IEC 2016 – All rights reserved

4 Symbols and abbreviated terms

$a \oplus b$	bitwise exclusive OR of a and b, where a and b are either bits or strings of bits of the same length, and in the latter case, the XOR operation is performed bit-wise
a_1, a_2	elliptic curve coefficients
$a \bmod n$	for an arbitrary integer a and a positive integer n, the unique integer remainder r, $0 \leq r \leq (n - 1)$, satisfying $r = a - bn$, for some integer b.
(A, B, C)	the coefficients of the signature formula, which, for the mechanisms specified in Clause 6, defines how the signature is computed NOTE 1 The signature formula is specified in 5.2.1.
	a parameter which specifies the relationship between the signature key and the verification key
E	an elliptic curve defined by two elliptic curve coefficients, a_1 and a_2
$\mathbb{E}$	a finite commutative group; for the mechanisms based on a multiplicative group, the elements of $\mathbb{E}$ are in $\boldsymbol{Z}_p{}^*$; for the mechanisms based on an additive group of elliptic curve points, the elements of $\mathbb{E}$ are the points on an elliptic curve E over $GF(r)$
$\#\mathbb{E}$	the cardinality of $\mathbb{E}$; for the mechanisms based on a multiplicative group $\boldsymbol{Z}_p{}^*$, $\#\mathbb{E}$ is p - 1; for the mechanisms based on an additive group of elliptic curve points, $\#\mathbb{E}$ is one more than the number of points on the elliptic curve E over $GF(r)$ [including 0_E (the point at infinity)]
$\boldsymbol{F}$	a finite field
$\boldsymbol{F}_p$	a finite field of order p
$gcd(N_1, N_2)$	the greatest common divisor of integers N_1 and N_2
G	an element of order q in $\mathbb{E}$
$GF(r)$	the finite field of cardinality r, where r is a prime power
G_1	a cyclic group of prime order q; elements of G_1 are points on an elliptic curve over $GF(r)$
G_2	a cyclic group of prime order q; elements of G_2 are elements of a finite field $GF(r)$
H_1	a hash-function that converts a data string into an element in G_1 NOTE 2 The input data string is converted to an integer first, then the integer is converted to a point on E over $GF(r)$ by using the $I2P$ function, specified in Annex C.
h, H_2	hash-functions, i.e. one of the mechanisms specified in ISO/IEC 10118
ID	a data string containing an identifier of the signer, used in Mechanisms IBS-1 and IBS-2
m	an embedding degree (or extension degree)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 14888-3:2016
https://standards.iteh.ai/catalog/standards/sist/bef710e2-21d1-4e33-bf4b-fc21a10d7645/iso-iec-14888-3-2016

$[n]P$	multiplication operation that takes a positive integer n and a point P on the curve E as input and produces as output another point Q on the curve E, where $Q = [n]P = P + P + \ldots + P$ added n -1 times. The operation satisfies $[0]P = 0_{\mathrm{E}}$ (the point at infinity), and $[-n]P = [n](-P)$
P	a generator of G_1 which is used in Mechanisms IBS-1 and IBS-2
p	a prime number or a power of a prime number
q	a prime number that is a divisor of $\#E$ and the order of G_1 and G_2
r	the size of $GF(r)$; in the mechanisms based on an additive group of elliptic curve points, r is a prime power, p^m, for some prime $p \geq 2$ and integer $m \geq 1$.
T	the assignment
T_1	the first part of the assignment T
T_2	the second part of the assignment T
U	the KGC's master private key, generated as a randomly chosen integer, which is used in mechanisms IBS-1 and IBS-2
V	the KGC's master public key, an element G_1, of which is used in mechanisms IBS-1 and IBS-2
$\mathbf{Z}_N{}^*$	the set of integers i with $0 < i < N$ and $gcd\ (i, N) = 1$, with arithmetic defined modulo N
$\mathbf{Z}_p{}^*$	the set of integers i with $0 < i < p$ and p a prime number, which is a multiplicative group
α	the bit-length of the prime number (or prime power) p
β	the bit-length of the prime number q
γ	the output bit-length of hash-functions h and H_2
Π	pre-signature
Π_X	x-coordinate of Π in which $\Pi = (\Pi_X, \Pi_Y)$ is an elliptic curve point
Π_Y	y-coordinate of Π in which $\Pi = (\Pi_X, \Pi_Y)$ is an elliptic curve point
Π_a	first element of Π in which $\Pi = (\Pi_a, \Pi_b)$ is an element of an extension field of degree 2
Π_b	second element of Π in which $\Pi = (\Pi_a, \Pi_b)$ is an element of an extension field of degree 2
0_E	the point at infinity on the elliptic curve E
< >	a bilinear and non-degenerate pairing
$\|$	$X \| Y$ is used to mean the result of the concatenation of data items X and Y in the order specified.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 14888-3:2016
https://standards.iteh.ai/catalog/standards/sist/bef710e2-21d1-4e33-bf4b-f21a10d7645/iso-iec-14888-3-2016

© ISO/IEC 2016 – All rights reserved

5 General model

5.1 Parameter generation process

5.1.1 Certificate-based mechanisms

5.1.1.1 Generation of domain parameters

For digital signature mechanisms based on discrete logarithms, the set of domain parameters includes the following parameters:

- E, a finite commutative group;
- q, a prime divisor of $\#E$;
- G, an element of order q in E.

In the group E, multiplicative notation is used. It is worthwhile to note that the particular signature mechanism chosen may place additional constraints on the choice of E, q, and G.

5.1.1.2 Generation of signature key and verification key

A signature key of a signing entity is a secretly generated random or pseudo-random integer X such that $0 < X < q$. The corresponding public verification key Y is an element of E and is computed as

$$Y = G^{x^D}$$

where D is a parameter defined by the mechanism to be used. The value of D is one of two values, -1 and 1.

NOTE An implementation is still considered compliant if it excludes a few integers from consideration as possible X values. For example, the value 1 can be excluded because this value results in the user's verification key being the generator, G, which is easily detectable.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 14888-3:2016
https://standards.iteh.ai/catalog/standards/sist/bef710e2-21d1-4e33-bf4b-f621a10d7645/iso-iec-14888-3-2016

5.1.2 Identity-based mechanisms

5.1.2.1 Notation

The two identity-based mechanisms specified in Clause 7 are both based on the use of pairings over elliptic curve groups. To specify identity-based mechanisms, the additive group notation is used.

5.1.2.2 Generation of domain parameters

The set of domain parameters includes the following parameters:

- E, a finite commutative group;
- $GF(r)$, the Galois field of cardinality r;
- G_1, a cyclic group of prime order q;
- G_2, a cyclic group of prime order q;
- P, a generator of G_1;
- q, a prime number — the cardinality of G_1 and G_2;
- $< >$, a bilinear and non-degenerate pairing

5.1.2.3 Generation of master key

A master private key of a KGC is a secretly generated random or pseudo-random integer U such that $0 < U < q$. The corresponding master public key V is an element of G_1 and is computed as

$$V = [U]P.$$

5.1.2.4 Generation of signature key and verification key

A signature key of a signing entity is an element of G_1 and is computed by the KGC as

$$X = [U]Y$$

where U is the KGC's master private key and $Y = H_1(ID)$ is the public verification key, where ID is an identity string for the KGC and H_1 is a hash-function.

5.1.3 Parameter selection

5.1.3.1 Selecting parameter size

The bit-lengths of parameters for typical security levels are shown in Table 1. The minimum recommended security level is 2^{112}.

NOTE 1 Security level means the number of steps in the best known attack on a cryptographic primitive. If 2^{112} steps are required in the best known attack on a hash-function, the security level of the hash-function is 2^{112}. For a comprehensive analysis of parameter sizes, see References [25] and [34].

It is not necessary to select α, β and γ having the same security level; the security level of an implemented signature scheme is the minimum of the security levels of the parameters.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 14888-3:2016
https://standards.iteh.ai/catalog/standards/sist/bef710e2-21d1-4e33-bf4b-fc21a10d7645/iso-iec-14888-3-2016

Table 1 — Parameter sizes according to the security level

Security level	2^{80}	2^{112}	2^{128}	2^{192}	2^{256}
α	1024	2048	3072	7680	15360
β	160	224	256	384	512
γ	160	224	256	384	512

It is recommended that the security level of 2^{80} should only be used for legacy applications.

NOTE 2 Not every mechanism specified in this part of ISO/IEC 14888 provides all of the levels of security specified in this table. For example, DSA in 6.1 only supports the security levels up to 2^{128}.

5.1.3.2 Selecting a hash-function

Selection of hash-functions should be based on those standardized in ISO/IEC 10118-3. That is, h and H_2 shall be one of the mechanisms specified in ISO/IEC 10118-3, and H_1 converts a data string obtained by using one of the mechanisms specified in ISO/IEC 10118-3 into an element in G_1.

The hash-functions used in this part of ISO/IEC 14888 should be collision-resistant.

The security strength for the selected hash-function should meet or exceed the security strength of the parameters used in key generation. The relationship between the security levels of a hash-function and the key generation parameters is shown in 5.1.3.1.

Furthermore, implementations that verify digital signatures shall have a way of securely determining which hash-function was used by the signer. Otherwise, an attacker might be able to convince a verifier to use a different weaker, hash-function and thus, bypass the intended security level.

5.1.4 Validity of domain parameters and verification key

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

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

- selection of valid domain parameters from a trusted published source, such as a standard;
- generation of valid domain parameters by a trusted third party, such as a CA or a KGC;
- validation of candidate domain parameters by a trusted third party, such as a CA or a KGC;
- 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 verification key can be provided by one of the following:

- for the signer, generation of the public verification/private signature key pair using a trusted system;
- for the signer or verifier, validation of the public verification key by a trusted third party, such as a CA or a KGC;
- validation of the public verification key by the user (i.e. the signer or verifier).

NOTE 1 Validation of domain parameters and keys is required. However, how to achieve this is outside the scope of this part of ISO/IEC 14888.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

NOTE 2 The method of authenticating the signer is dependent on the real applications, which is out of the scope of this part of ISO/IEC 14888.

ISO/IEC 14888-3:2016
https://standards.iteh.ai/catalog/standards/sist/bef710e2-21d1-4e33-bf4b-fc21a10d7645/iso-iec-14888-3-2016

5.2 Signature process

5.2.1 General

All of the signature mechanisms in this part of ISO/IEC 14888 make use of a randomizing value K, which is used (along with the message) to produce a witness R (the first part of the signature) and an assignment (T_1, T_2). The signature for the message is the pair (R, S) where S (the second part of the signature) is computed as the solution of a signature formula.

In the certificate-based mechanisms, specified in Clause 6, the signature formula is

$$AK + BX^D + C \equiv 0 \pmod{q},$$

given that (A, B, C) is a permutation of (S, T_1, T_2), X is the private signature key and D is a parameter depending on the particular mechanism.

In the identity-based mechanisms specified in Clause 7, the signature formula is

$$[K]A + [U^D]B + C \equiv 0_E \text{ (in } G_1\text{)}.$$

Given that (A, B, C) is a permutation of (S, T_1, T_2), U is the master private key and D is a parameter depending on the particular mechanism.

The permutation will be specified or agreed upon when setting up the signature system.