ISO/IEC JTC 1/SC 27 N15619

Date: 2017-08-10

ISO/IEC 14888-3

ISO/IEC JTC 1/SC 27/WG 2

Secretariat: DIN

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: Méchanismes basés sur un logarithme discréte

Style Definition ... [1]

Field Code Changed ... [2]

Formatted ... [3]

Field Code Changed

Formatted ... [4]

Field Code Changed

Formatted ... [5]

Deleted: 2015-11-11

Formatted: French (Switzerland)

Field Code Changed

Formatted ... [6]

Field Code Changed

Formatted ... [7]

Field Code Changed

Formatted ... [8]

Field Code Changed

Formatted ... [9]

Field Code Changed

Formatted ... [10]

Field Code Changed

Formatted ... [11]

Field Code Changed

Formatted ... [12]

Document type: International Standard

Deleted: 2016

Contents

Page

Deleted: 2016

Deleted: 2016

Deleted: 2016

Deleted: 2016

Deleted: 2016

Deleted: 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.

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.

Deleted: 2016

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: English (U.K.)

Formatted: Default Paragraph Font

Formatted: English (U.K.)

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font, English (U.K.)

Deleted: The committee responsible for this

Deleted: is

Deleted: consists of

Deleted: parts, under

Formatted: List Continue 1, Don't keep with next, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Deleted: general title *Information technology — Security techniques — Digital signatures with appendix*:

Deleted: — *Part 1: General*¶
— *Part 2: Integer factorization based mechanisms*¶
— *Part 3: Discrete logarithm based mechanisms*¶

Deleted: 2016

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.

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);

Deleted: 2016

- 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.

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.

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.

Deleted: 2016

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.

Deleted: 2016

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.

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 $a, b \in E$, $a * b = b * a$

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

3.2
cyclic group

finite commutative group (3.1), E, of n elements that contains a group element $a \in E$, 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, E.

Note 2 to entry: The cardinality of the elliptic-curve group, 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*)

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 $a^n{=}a{*}a^{m\text{-}1}$ (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

  $<P_1 + P_2, Q> = <P_1, Q> * <P_2, Q>$,

  $<P, Q_1 + Q_2> = <P, Q_1> * <P, Q_2>$, and