INTERNATIONAL STANDARD

ISO/IEC 14888-3

Fourth edition
2018-11

IT Security techniques — Digital signatures with appendix —

Part 3: Discrete logarithm based mechanisms

Techniques de sécurité IT — Signatures numériques avec appendice —

Partie 3: Mécanismes basés sur un logarithme discret

Reference number
ISO/IEC 14888-3:2018(E)

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

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) or the IEC list of patent declarations received (see http://patents.iec. ch).

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

For an explanation of 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 www. iso.org/iso/foreword. html.

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

This fourth edition cancels and replaces the third edition (ISO 14888-3:2016), of which it constitutes a minor revision. The main changes compared to the previous edition are as follows:

— SM2 algorithm has been added to 6.12 and F.14;

— Chinese IBS algorithm has been added to 7.4 and F.15;

— numerical examples of KCDSA, ECDSA and EC-KCDSA have been added to F.3.4, F.6.6, F.6.7, F.6.8, F.7.7, F.7.8 and F.7.9;

— several formulae and symbols have been corrected.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

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, produce a new signature on a previously signed message; or
  - 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 document 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 the ISO/IEC 14888 series);
- when the whole message, or part of it, can be recovered from the signature, the mechanism is termed a "signature mechanism giving message recovery" (the ISO/IEC 9796 series 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 document 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 document 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 the ISO/IEC 14888 series 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 document now contains discrete logarithm based mechanisms.

This document includes 14 mechanisms: two of which (DSA and Pointcheval/Vaudenay algorithm) were in ISO/IEC 14888-3:1998, three of which (EC-DSA, EC-KCDSA, and EC-GDSA) were from ISO/IEC 15946-2:2002 and three of which (KCDSA, IBS-1 and IBS-2) were added in ISO/IEC 14888-3:2006, four of which (SRA, EC-RDSA, EC-SDSA and EC-FSDSA) were added in ISO/IEC 14888-3:2006/Amd 1:2010, and two of which (SM2 and Chinese IBS) are added in this document.

The mechanisms specified in this document 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 document 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 ISO and IEC that he/she 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 may be obtained from:

Certicom Corp.
4701 Tahoe Blvd, Building A
MISSISSAUGA ON L4W 0B5
CANADA

Beijing HuadaInfosec Technology Co., Ltd
4F, Tower B, Yandong Bldg
No. 2 Wanhong West St.
Chaoyang District
100015 BEIJING
P.R. CHINA

Attention is drawn to the possibility that some of the elements of this document 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.

Annexes A, B and D are normative elements; Annexes C, E, F, G and H are for information.

IT Security techniques — Digital signatures with appendix —

Part 3:
Discrete logarithm based mechanisms

1 Scope

This document specifies digital signature mechanisms with appendix whose security is based on the discrete logarithm problem.

This document 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 document specifies

— the process of generating a pair of keys,

— the process of producing signatures, and

— the process of verifying signatures.

Annex A defines object identifiers assigned to the digital signature mechanisms specified in this document, and defines algorithm parameter structures.

Annex B defines conversion functions of FE2I, I2FE, FE2BS, BS2I, I2BS, I2OS and OS2I used in this document.

Annex D defines how to generate DSA domain parameters.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 10118-3, *IT Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

ISO/IEC 14888-1, *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.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/