International Standard

ISO/IEC 14888-3

IT Security techniques — Digital signatures with appendix —

Part 3: Discrete logarithm based mechanisms

AMENDMENT 1

Techniques de sécurité IT — Signatures numériques avec appendice —

Partie 3: Mécanismes basés sur un logarithme discret

AMENDEMENT 1

Fourth edition
2018-11

AMENDMENT 1
2026-11

Sample Document
get full document from standards.iteh.ai

Reference number
ISO/IEC 14888-3:2018/Amd. 1:2026(en)

© ISO/IEC 2026

ISO/IEC 14888-3:2018/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/40476252-ec08-4efb-b2c4-b5afd96ad4b0/iso-iec-14888-3-2018-amd-1-2026

Sample Document

get full document from standards.iteh.ai



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

ISO/IEC 14888-3:2018/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/40476252-ec08-4efb-b2c4-b5afd96ad4b0/iso-iec-14888-3-2018-amd-1-2026

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

Sample Document

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cyber security, and privacy protection*.

get full document from standards.iteh.ai

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

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 and www.iec.ch/national-committees.

© ISO/IEC 2026 – All rights reserved

ISO/IEC 14888-3:2018/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/40476252-ec08-4efb-b2c4-b5afd96ad4b0/iso-iec-14888-3-2018-amd-1-2026

Sample Document

get full document from standards.iteh.ai

IT Security techniques — Digital signatures with appendix —

Part 3:
Discrete logarithm based mechanisms

AMENDMENT 1

Introduction

After Note 4, replace the paragraph with the following text:

This document includes 15 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, three of which (KCDSA, IBS-1 and IBS-2) were added in ISO/IEC 14888-3:2006, four of which (SDSA, EC-RDSA, EC-SDSA and EC-FSDSA) were added in ISO/IEC 14888-3:2006/Amd 1:2010, two of which (SM2 and Chinese IBS) were added in ISO/IEC 14888-3:2018 and one of which (EdDSA) is added in this document.

Reword Note 5 as follows:

The mechanisms of EC-DSA, EC-GDSA, EC-RDSA and EC-FSDSA can 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 to 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. EdDSA includes this protection in its design.

Sample Document
get full document from standards.iteh.ai

Clause 2, Normative references

Add the following:

ISO/IEC 29192-5, *Information technology — Security techniques — Lightweight cryptography — Part 5: Hash-functions*

Clause 3, Terms and definitions

Insert the following definition after 3.6:

3.7

complete twisted Edwards curve group

cyclic group (3.2) defined on the points of a complete twisted Edwards curve over a finite field

Note 1 to entry Let $F = \mathrm{GF}(r)$ be a finite field where r is an odd prime. Let a and d be distinct non-zero elements of F such that a is a square in F and d is a non-square in F. Then the affine curve $ax^2 + y^2 = 1 + dx^2y^2$ is a complete twisted Edwards curve defined over F. The set E of points of this curve consists of a collection of certain affine points from $F \times F$, namely those that satisfy the curve equation. Let "+" denote the binary operation known as "Edwards-curve addition", defined for all affine points of E by

© ISO/IEC 2026 – All rights reserved

ISO/IEC 14888-3:2018/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/40476252-ec08-4efb-b2c4-b5afd96ad4b0/iso-iec-14888-3-2018-amd-1-2026

$$(x_1, y_1)+(x_2, y_2)=((x_1y_2+x_2y_1)/(1+dx_1x_2y_1y_2),(y_1y_2-ax_1x_2)/(1-dx_1x_2y_1y_2)).$$

The identity element for "+" is $(0,1)$. The set E together with the binary operation "+" forms a finite commutative group E that is the complete twisted Edwards curve group for this curve.

Clause 4, Symbols and abbreviated terms

Add the following symbols/abbreviated terms:

a, d twisted Edwards curve coefficients

EdDSA Edwards curve Digital Signature Algorithm

Replace the definition of E with the following*:*

E an elliptic curve defined by two elliptic curve coefficients, a_1 and a_2, or a twisted Edwards curve defined by two curve coefficients a and d

Replace the definition of $_E$ with the following:

$_E$ a finite commutative group; for the mechanisms based on a multiplicative group, the elements of $_E$ are in Z_p^*; for the mechanisms based on an additive group of elliptic curve points, the elements of $_E$ are the points on an elliptic curve E over $GF(r)$ or the points on the twisted Edwards curve E over $GF(r)$

Sample Document
get full document from standards.iteh.ai

Replace the definition of #$_E$ with the following:

#$_E$ the cardinality of $_E$; for the mechanisms based on a multiplicative group Z_p*, #$_E$ is p – 1; for the mechanisms based on an additive group of elliptic curve points, #$_E$ is one more than the number of points on the elliptic curve E over $GF(r)$ [including 0_E (the point at infinity)]; for the mechanisms based on twisted Edwards curve points, #$_E$ is the number of points on the twisted Edwards curve E over $GF(r)$

5.2.2

At the end of Note 2, add the text:

Mechanisms can also permit a larger range for K or specify some algebraic format of K.

5.3.5

Add the following text at the end of the subclause:

For EdDSA the verification mechanism is specified in 6.13.

6.1

Replace the first paragraph with the following:

© ISO/IEC 2026 – All rights reserved

ISO/IEC 14888-3:2018/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/40476252-ec08-4efb-b2c4-b5afd96ad4b0/iso-iec-14888-3-2018-amd-1-2026

Clause 6 specifies twelve certificate-based mechanisms. These make use of arithmetic in the multiplicative group Z_p*, the additive group of elliptic curve points, or the additive group of points on twisted Edwards curves. The mechanisms using arithmetic in the multiplicative group Z_p*, are the Digital Signature Algorithm (DSA), the Korean Certificate-based Digital Signature Algorithm (KCDSA), the Pointcheval/Vaudenay algorithm, and the Schnorr Digital Signature Algorithm (SDSA). The mechanisms using arithmetic in the additive group of elliptic curve points are the Elliptic Curve DSA (EC-DSA), the Elliptic Curve KCDSA (EC-KCDSA), the Elliptic Curve German Digital Signature Algorithm (EC-GDSA), the Elliptic Curve Russian Digital Signature Algorithm (EC-RDSA), the Elliptic Curve Schnorr Digital Signature Algorithm (EC-SDSA), the Elliptic Curve Full Schnorr Digital Signature Algorithm (EC-FSDSA), the SM2 algorithm, and the Edwards-curve Digital Signature Algorithm (EdDSA).

At the end of the second paragraph insert the text:

The curves Ed25519 and Ed448 for EdDSA are specified in 6.13.

6.3.2

Replace the penultimate paragraph (starting "Three choices") with the following:

The pair (α,β) for KCDSA shall be chosen in accordance with the chosen security level, as shown in Table 1 in 5.1.3.1. Typical examples are (2 048, 224) and (3 072, 256).

The hash-function h shall be one of the approved hash-functions from ISO/IEC 10118-3 and ISO/IEC 29192-5. The security strength γ of the hash-function h shall meet or exceed the security strength associated with the pair (α,β).

Sample Document

6.5.2

get full document from standards.iteh.ai

Replace the paragraph under the listing (starting "Four choices") with the following:

Three choices for α are permitted in SDSA, namely 1 024, 2 048, and 3 072. The values of γ and β shall be selected in accordance with the value of α, as specified in Table 1 in 5.1.3.1, such that $\gamma \geq \beta$. The hash-function h shall be one of the approved hash-functions from ISO/IEC 10118-3, and its security strength shall meet or exceed the security strength associated with the pair (α,β).

6.6.1

In the second paragraph, replace the last sentence "The hash-function h ... 10118-3" with the following.

The hash function h shall be one of SHA-224, SHA-512/224, SHA3-224, SHA-256, SHA-512/256, SHA3-256, SHAKE128 (d=256 bits), SHA-384, SHA3-384, SHA-512, SHA3-512, and SHAKE256 (d=512 bits) specified in ISO/IEC 10118-3. The security level γ shall meet or exceed the level associated with the parameter α (see Table 1 in 5.1.3.1).

6.12.5.7

Add the following text after 6.12.5.7:

6.13 EdDSA

6.13.1 General

EdDSA (Edwards Curve Digital Signature Algorithm) is a signature mechanism with verification key Y' equal to the encoding of $Y = \lfloor X \rfloor G$, where G is a specified point on a twisted Edwards curve and X is a multiple of

© ISO/IEC 2026 – All rights reserved

ISO/IEC 14888-3:2018/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/40476252-ec08-4efb-b2c4-b5afd96ad4b0/iso-iec-14888-3-2018-amd-1-2026