INTERNATIONAL STANDARD

ISO/IEC 11770-4

Second edition
2017-11-15

AMENDMENT 1
2019-09

Information technology — Security techniques — Key management —

Part 4: Mechanisms based on weak secrets

AMENDMENT 1: Unbalanced Password-Authenticated Key Agreement with Identity-Based Cryptosystems (UPAKA-IBC)

Technologies de l'information — Techniques de sécurité — Gestion de clés —

Partie 4: Mécanismes basés sur des secrets faibles

AMENDEMENT 1: Accord dissymétrique de clé authentifié par mot de passe utilisant un mécanisme de chiffrement basé sur l'identité

Reference number
ISO/IEC 11770-4:2017/Amd.1:2019(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

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, *Information security, cybersecurity and privacy protection*.

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.

Information technology — Security techniques — Key management —

Part 4: Mechanisms based on weak secrets

AMENDMENT 1: Unbalanced Password-Authenticated Key Agreement with Identity-Based Cryptosystems (UPAKA-IBC)

Introduction

Insert the following paragraph after Note 2:

d) **Unbalanced password-authenticated key agreement with identity-based cryptosystems:** Establish one or more secret keys for an entity, *A*, associated with another entity, *B*, where:

1) *A* and *B* share a weak secret and *B* has a strong secret; or

2) *A* has a weak secret and *B* has verification data derived from *A*'s weak secret with a one-way function along with a strong secret.

An example of a strong secret could be a long random key. This strong secret is independent of the weak secret and has been generated for an identity-based cryptosystem.

In an unbalanced password-authenticated key agreement mechanism with an identity-based cryptosystem, the shared secret keys are the result of a data exchange between the two entities. The shared secret keys are established if, and only if, *A* has used the weak secret and *B* has a strong secret corresponding to its identity and neither of the two entities can predetermine the values of the shared secret keys.

NOTE 3 This type of key agreement mechanism runs between entities with unbalanced security requirements such as in the client-server model. It is suitable for the case where a client (*A*) conducts authentication based on both a human-memorable password and a server (*B*)'s identity while enhancing server authentication (thus avoiding an attack on a cryptographic protocol in which an unauthorized party masquerades as a legitimate server, which is often called "a server impersonation attack").

Clause 3

Insert the following terminological entry at the end of the clause:

3.39
master-secret key
secret value used by the private key generator to compute private keys for an identity-based encryption (IBE) or identity-based signature (IBS) scheme

Clause 4

Insert the following abbreviated terms:

CT	ciphertext, an octet string
G_1	point of order r on E over $F(q)$, in the same subgroup as G
IBE	identity-based encryption
IBS	identity-based signature
ID	distinguished identifier that is uniquely assigned to an identity, which is an octet string
κ	security parameter
Msg	plaintext, an octet string
msk	master-secret key of IBE or IBS
$parms$	domain parameters of IBE or IBS
σ	signature, an octet string
sk_{ID}	private key corresponding to an entity with distinguished (octet) identifier ID for an IBE or IBS scheme

Clause 5

Replace the definition of G by the definition of G and G_1 as follows:

— G, G_1 curve points of order r (G and G_1 are called the generators of a subgroup of r points on E). It is assumed that the logarithm of G_1 to the base G is unknown;

Clause 5

Add the following paragraph at the end:

Annex B defines the object identifiers which shall be used to identify the mechanisms specified in this document.

Clause 8

Add new Clause 8 as follows:

8 Unbalanced password-authenticated key agreement with identity-based cryptosystems

8.1 General

This clause specifies two unbalanced password-authenticated key agreement mechanisms using identity-based cryptosystems. In these mechanisms, one entity has a weak secret derived from a password, and the other entity has the password verification data and a strong secret, i.e., a long random key which is used with an identity-based cryptosystem. An identity-based cryptosystem is an

NEN
CONNECT

ALTIJD DE ACTUELE NORM IN UW BEZIT HEBBEN?

Nooit meer zoeken in de systemen en uzelf de vraag stellen: ‘Is ISO/IEC 11770-4:2017/Amd 1:2019 en de laatste versie?’

Via het digitale platform NEN Connect heeft u altijd toegang tot de meest actuele versie van deze norm. Vervallen versies blijven ook beschikbaar. **U en uw collega’s** kunnen de norm via NEN Connect makkelijk raadplagen, online en offline.

Kies voor slimmer werken en bekijk onze mogelijkheden op **www.nenconnect.nl**.

Heeft u vragen?
Onze Klantenservice is bereikbaar maandag tot en met vrijdag, van 8.30 tot 17.00 uur.

Telefoon: 015 2 690 391
E-mail: klantenservice@nen.nl