INTERNATIONAL STANDARD

ISO/IEC 11770-4

Second edition
2017-11

AMENDMENT 2
2021-02

Information technology — Security techniques — Key management —

Part 4: Mechanisms based on weak secrets

AMENDMENT 2: Leakage-resilient password-authenticated key agreement with additional stored secrets

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

Partie 4: Mécanismes basés sur des secrets faibles

AMENDEMENT 2

Reference number
ISO/IEC 11770-4:2017/Amd.2:2021(E)

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

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 https://patents.iec).

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*, SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 11770 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.

Information technology — Security techniques — Key management —

Part 4: Mechanisms based on weak secrets

AMENDMENT 2: Leakage-resilient password-authenticated key agreement with additional stored secrets

Introduction

Insert new list item e) as follows:

e) **Leakage-resilient password-authenticated key agreement with additional stored secrets:** Establish one or more shared secret keys between two entities *A* and *B*, where *A* has a weak secret and a (possibly, insecure) stored secret that might be revealed to or altered by adversaries and *B* has verification data derived from *A*'s weak secret and stored secret. In a leakage-resilient password-authenticated key agreement with additional stored secrets mechanism, 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, the two entities have used the weak secret, the stored secret and the corresponding verification data; and *A*, *B* and an adversary who has obtained and altered the stored secret are all unable to predetermine the values of the shared secret keys.

NOTE 4 Here, "leakage-resilience" means security against either compromise of stored secrets held by client *A* or compromise of verification data held by server *B*, but not both. This type of key agreement mechanism is able to protect *A*'s weak secret from being discovered by *B*, as well as preventing an adversary from getting *A*'s weak secret from *B*. Also, this type of key agreement mechanism prevents an adversary from performing online dictionary attacks unless the adversary obtains *A*'s stored secret. In other words, an adversary who obtains *A*'s stored secret is restricted to performing online dictionary attacks, and the security level in this case is the same as that of the other mechanisms in this document. A typical application scenario would involve use between a client (*A*) and a server (*B*), where a client user employs a portable device such as a smart phone, USB memory or smart card to save the user's stored secret, or where a client terminal shares a network-attached storage device in an office environment.

Clause 2

Replace Clause 2 with the following:

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 (all parts), *Information technology — Security techniques — Hash-functions*

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

ISO/IEC 9797 (all parts), *Information technology — Security techniques — Message Authentication Codes (MACs)*

ISO/IEC 29192-6, *IT Security techniques — Lightweight cryptography — Part 6: Message Authentication Codes (MACs)*

ISO/IEC 11770-6, *Information technology — Security techniques — Key management — Part 6: Key derivation*

ISO/IEC 18033-2, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*

ISO/IEC 19772, *Information technology — Security techniques — Authenticated encryption*

Clause 3

Insert new term 3.40 as follows:

3.40
Hamming weight
number of non-zero elements in a bit string

Clause 4

Replace definitions as follows:

H	a collision-resistant hash-function taking an octet string as input and giving a bit string as output. One of the hash-functions specified in ISO/IEC 10118 (all parts) or ISO/IEC 29192-5 shall be used
$h(x, L_K)$	a collision-resistant hash-function taking an octet string x and an integer L_K as input and giving a bit string of length L_K (in bits) as output. One of the hash-functions specified in ISO/IEC 10118 (all parts) or ISO/IEC 29192-5 shall be used
$mac(k, m)$	a message authentication code (MAC) function taking a key k and a variable-length message m as input and giving a fixed-length output. One of the MAC algorithms specified in ISO/IEC 9797 (all parts) or ISO/IEC 29192-6 shall be used

G,G_a,G_b	points of order r on E over $F(q)$, where the relative discrete logarithms of G,G_a,G_b are unknown
g, g_1, g_a, g_b	elements of multiplicative order r in $F(q)$, where the relative discrete logarithms of g, g_1, g_a, g_b are unknown

K	a function for deriving a key from a secret value and a key derivation parameter. One of the key derivation functions specified in ISO/IEC 11770-6 shall be used

Add the following definitions:

