INTERNATIONAL STANDARD

ISO/IEC 11770-4

First edition
2006-05-01

Information technology — Security techniques — Key management —

Part 4:
Mechanisms based on weak secrets

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

Partie 4: Mécanismes basés sur des secrets faibles

Reference number
ISO/IEC 11770-4:2006(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword iv
1 Scope 1
2 Normative references 2
3 Terms and definitions 2
4 Symbols and notation 6
5 Requirements 8
6 Password-authenticated key agreement 9
6.1 Key Agreement Mechanism 1 10
6.1.1 Prior shared parameters 10
6.1.2 Functions 10
6.1.3 Key agreement operation 12
6.2 Key Agreement Mechanism 2 13
6.2.1 Prior shared parameters 14
6.2.2 Functions 14
6.2.3 Key agreement operation 16
6.3 Key Agreement Mechanism 3 17
6.3.1 Prior shared parameters 17
6.3.2 Functions 17
6.3.3 Key agreement operation 20
7 Password-authenticated key retrieval 21
7.1 Key Retrieval Mechanism 1 22
7.1.1 Prior shared parameters 22
7.1.2 Functions 22
7.1.3 Key retrieval operation 23
Annex A (normative) Functions for Data Type Conversion 24
Annex B (normative) ASN.1 Module 28
Annex C (informative) Guidance on Choice of Parameters 30
Bibliography 32

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 11770-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 11770 consists of the following parts, under the general title *Information technology — Security techniques — Key management*:

— *Part 1: Framework*

— *Part 2: Mechanisms using symmetric techniques*

— *Part 3: Mechanisms using asymmetric techniques*

— *Part 4: Mechanisms based on weak secrets*

Further parts may follow.

Information technology — Security techniques — Key management —

Part 4:
Mechanisms based on weak secrets

1 Scope

This part of ISO/IEC 11770 defines key establishment mechanisms based on weak secrets, i.e., secrets that can be readily memorized by a human, and hence secrets that will be chosen from a relatively small set of possibilities. It specifies cryptographic techniques specifically designed to establish one or more secret keys based on a weak secret derived from a memorized password, while preventing off-line brute-force attacks associated with the weak secret. More specifically, these mechanisms are designed to achieve one of the following three goals.

1) **Balanced password-authenticated key agreement:** Establish one or more shared secret keys between two entities that share a common weak secret. In a balanced password-authenticated key agreement 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 same weak secret, and neither of the two entities can predetermine the values of the shared secret keys.

2) **Augmented password-authenticated key agreement:** Establish one or more shared secret keys between two entities *A* and *B*, where *A* has a weak secret and *B* has verification data derived from a one-way function of *A*’s weak secret. In an augmented password-authenticated key agreement 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 and the corresponding verification data, and neither of the two entities can predetermine the values of the shared secret keys.

   NOTE – This type of key agreement mechanism is unable to protect *A*’s weak secret being discovered by *B*, but only increases the cost for an adversary to get *A*'s weak secret from *B*. Therefore it is normally used between a client (*A*) and a server (*B*).

3) **Password-authenticated key retrieval:** Establish one or more secret keys for an entity, *A*, associated with another entity, *B*, where *A* has a weak secret and *B* has a strong secret associated with *A*'s weak secret. In an authenticated key retrieval mechanism, the secret keys, retrievable by *A* (not necessarily derivable by *B*), are the result of a data exchange between the two entities, and the secret keys are established if and only if the two entities have used the weak secret and the associated strong secret. However, although *B*’s strong secret is associated with *A*'s weak secret, the strong secret does not (in itself) contain sufficient information to permit either the weak secret or the secret keys established in the mechanism to be determined.

   NOTE – This type of key retrieval mechanism is used in those applications where *A* does not have secure storage for a strong secret, and requires *B*’s assistance to retrieve the strong secret for her. It is normally used between a client (*A*) and a server (*B*).

This part of ISO/IEC 11770 does not cover aspects of key management such as

- lifecycle management of weak secrets, strong secrets and established secret keys;
- mechanisms to store, archive, delete, destroy, etc. weak secrets, strong secrets, and established secret keys.

NOTE – The keys generated or retrieved through the use of weak secrets cannot be more secure against exhaustion than the sum of the weak secrets themselves. With this proviso, the mechanisms specified in this part of ISO/IEC 11770 are recommended for practical use in low-security environments.

2 Normative references

The following referenced documents are indispensable for the application 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 10118-3:2004, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

ISO/IEC 11770-1:1996, *Information technology — Security techniques — Key management — Part 1: Framework*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1

augmented password-authenticated key agreement

password-authenticated key agreement where entity *A* uses a password-based weak secret and entity *B* uses verification data derived from a one-way function of *A*'s weak secret to negotiate and authenticate one or more shared secret keys

3.2

balanced password-authenticated key agreement

password-authenticated key agreement where two entities *A* and *B* use a shared common password-based weak secret to negotiate and authenticate one or more shared secret keys

3.3

brute-force attack

attack on a cryptosystem that employs an exhaustive search of a set of keys, passwords or other data

3.4

collision-resistant hash-function

hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output

NOTE – Computational feasibility depends on the specific security requirements and environment.

[ISO/IEC 10118-1:2000]

3.5

dictionary attack (on a password-based system)

attack on a cryptosystem that employs a search of a given list of passwords

NOTE – A dictionary attack on a password-based system can use a stored list of specific password values or a stored list of words from a natural language dictionary.

3.6

domain parameter

data item which is common to and known by or accessible to all entities within the domain

NOTE – The set of domain parameters may contain data items such as hash-function identifier, length of the hash-token, length of the recoverable part of the message, finite field parameters, elliptic curve parameters, or other parameters specifying the security policy in the domain.

[ISO/IEC 9796-3:2000]