INTERNATIONAL STANDARD

ISO/IEC 11770-7

First edition
2021-07

Information security — Key management —

Part 7: Cross-domain password-based authenticated key exchange

Sécurité de l'information — Gestion des clés —

Partie 7: Échange de clés authentifié entre mots de passe entre domaines

Reference number
ISO/IEC 11770-7:2021(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

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, *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.

Introduction

In a security domain, two entities can authenticate each other and establish a shared session key to protect their communication. This authentication is typically based on pre-established information, such as a shared password or symmetric key or possession of each other's public key certificates. In a cross-domain communication, two entities assigned to two distinct security domains may not have suitable pre-established authentication information. However, they can still establish a shared session key by using the authentication information that each entity shares with its own domain server and relying on the domain servers themselves to authenticate each other.

Practical cross-domain communication scenarios include email communication, mobile phone communication, and instant messaging. In these cases, communications need to be protected against both passive and active attackers. In these scenarios, each entity is typically registered with a domain-specific server, such as an email exchange server (for email communications) or a home location register (for mobile phone communications). Moreover, the two communicating entities from different domains typically neither share a password or a symmetric key nor possess each other's public key certificate.

An authenticated key exchange (AKE) mechanism enables two entities to establish a shared session key based on their pre-established authentication information. A password-based AKE mechanism is based on two entities pre-sharing a password. Similarly, a symmetric key or an asymmetric key based AKE mechanism is based on two entities pre-sharing a secret key or possessing each other's public key certificate (and a trusted means to verify a certificate). In this document, these three types of mechanisms are referred to as two-party password-based authenticated key exchange (2PAKE) protocols, two-party symmetric key based authenticated key exchange (2SAKE) protocols and two-party asymmetric key based authenticated key exchange (2AAKE) protocols, respectively. 2PAKE protocols are specified in ISO/IEC 11770-4, 2SAKE protocols are specified in ISO/IEC 11770-2 and 2AAKE protocols are specified in ISO/IEC 11770-3. All the mechanisms specified in ISO/IEC 11770-1[6], ISO/IEC 11770-2 and ISO/IEC 11770-3 are appropriate for use in a single security domain. For example, the mechanisms specified in ISO/IEC 11770-4 are used in authenticated key exchange applications, where two players, usually referred to as a server and a client, are in the same security domain.

This document (i.e. ISO/IEC 11770-7) specifies cross-domain password-based authenticated key exchange mechanisms. Such mechanisms enable a user from one domain to establish a session key shared with another user from a different domain through their respective domain servers, and the only pre-established authentication information that each user has is a password shared with their domain server.

More specifically, each mechanism specified in this document involves four parties in two security domains, in which each user and server pair are in the same domain. This type of mechanism is referred to as a four-party password-based authenticated key exchange (4PAKE) protocol. This document contains a framework for designing such 4PAKE protocols using a compositional approach. That is, a 4PAKE protocol can be implemented based on two building blocks:

a) a 2PAKE protocol;

b) a 2SAKE protocol or a 2AAKE protocol.

This document also specifies several mechanisms for such 4PAKE protocols. The 2PAKE, 2SAKE and 2AAKE protocols used to implement such 4PAKE protocols are chosen from ISO/IEC 11770-4, ISO/IEC 11770-2 and ISO/IEC 11770-3 respectively.

The hash functions and key derivation functions used in the mechanisms specified in this document are specified in ISO/IEC 10118-3 and ISO/IEC 11770-6, respectively.

The conversion functions in Annex B used in the mechanisms specified in this document are specified in ISO/IEC JTC 1/SC 27 WG 2 SD 7 [16].

Information security — Key management —

Part 7:
Cross-domain password-based authenticated key exchange

1 Scope

This document specifies mechanisms for cross-domain password-based authenticated key exchange, all of which are four-party password-based authenticated key exchange (4PAKE) protocols. Such protocols let two communicating entities establish a shared session key using just the login passwords that they share with their respective domain authentication servers. The authentication servers, assumed to be part of a standard public key infrastructure (PKI), act as ephemeral certification authorities (CAs) that certify key materials that the users can subsequently use to exchange and agree on as a session key.

This document does not specify the means to be used to establish a shared password between an entity and its corresponding domain server. This document also does not define the implementation of a PKI and the means for two distinct domain servers to exchange or verify their respective public key certificates.

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 11770-2, *IT Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*

ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

ISO/IEC 11770-4, *Information technology — Security techniques — Key management — Part 4: Mechanisms based on weak secrets*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 11770-4 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 https://www.electropedia.org/

3.1
asymmetric key pair
pair of related keys where the private key defines the private transformation and the public key defines the public transformation

[SOURCE: ISO/IEC 11770-3:2015, 3.3]

3.2
asymmetric-key authenticated key exchange
process of establishing one or more shared secret keys between two entities using asymmetric-key techniques and neither of them can predetermine the values of the shared secret keys

3.3
certification authority
entity trusted to create and assign *public key certificates* (3.9)

[SOURCE: ISO/IEC 11770-1:2010, 2.3]

3.4
cross-domain password-based authenticated key exchange
process of establishing one or more shared secret keys between two entities associated with two distinct *security domains* (3.10) using the entity's prior domain-specific password-based information such that neither of the entities can predetermine the values of the shared secret keys

3.5
distinguishing identifier
information which unambiguously distinguishes an entity

[SOURCE: ISO/IEC 11770-1:2010, 2.9]

3.6
key derivation function
function which takes as input a number of parameters, at least one of which is secret, and which gives as output keys appropriate for the intended algorithm(s) and applications

[SOURCE: ISO/IEC 11770-2:2018, 3.6, modified — Note 1 to entry has been removed.]

3.7
key establishment
process of making available a shared key to one or more entities, where the process includes key agreement or key transport

[SOURCE: ISO/IEC 11770-3:2015, 3.23]

3.8
non-interactive key exchange
process of establishing one or more shared secret keys between two entities in a non-interactive manner with mutual implicit key authentication

3.9
public key certificate
public key information of an entity signed by the *certification authority* (3.3)

[SOURCE: ISO/IEC 11770-1:2010, 2.37]

3.10
security domain
set of elements, security policy, security authority and set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain

[SOURCE: ISO/IEC 11770-1:2010, 2.43]

3.11
signature
data unit appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to verify the origin and integrity of the data unit and protect the sender and the recipient of the data unit against forgery by third parties, and the sender against forgery by the recipient

[SOURCE: ISO/IEC 11770-3:2015, 3.7, modified — the word "digital" has been removed from the term.]

3.12
symmetric-key
key used with symmetric cryptographic techniques and usable only by a set of specified entities

3.13
symmetric-key authenticated key exchange
process of establishing one or more shared secret keys between two entities using *symmetric-key* (3.12) techniques such that neither of the entities can predetermine the values of the shared secret keys

4 Symbols and abbreviated terms

4.1 Abbreviated terms

2AAKE	two-party asymmetric-key authenticated key exchange
2NIKE	two-party non-interactive key exchange protocol
2PAKE	two-party password-based authenticated key exchange
2SAKE	two-party symmetric-key authenticated key exchange
4PAKE	four-party password-based authenticated key exchange
BS2I	function that converts a bit string into an integer
BS2OS	function that converts a bit string to an octet string
CA	certification authority
FE2I	function that converts a field element to an integer
FE2OS	function that converts a field element to an octet string
$GE2OS_x$	function that converts a group element with *x*-coordinate to an octet string
I2BS	function that converts an integer to a bit string
I2OS	function that converts an integer to an octet string
KD	key derivation function
MAC	message authentication code
MAX	maximum value function
MIN	minimum value function
PKI	public key infrastructure
$Param_A$	2AAKE prior shared system parameters
$Param_N$	2NIKE prior shared system parameters

Param_S 2SAKE prior shared system parameters

Param_P 2PAKE prior shared system parameters

SIF session identity generation function

4.2 Symbols

A, B distinguishing clients' identities including their respective domain names represented as octet strings

$AK_{X,\,Y}$ symmetric authentication key shared between X and Y

aKG authentication public/private key pair generation function

aKV authentication public key validation function

apk_X entity X's authentication public key

ask_X entity X's authentication private key corresponding to apk_X

c_X ciphertext generated from a symmetric encryption function by entity X

DEC(K, c) symmetric decryption function taking a secret key K and a ciphertext c as input and giving as output a message m or a decryption failure symbol "⊥"

DL discrete logarithm setting

EC elliptic curve setting

ENC(K, m) symmetric encryption function taking a secret key K and a variable-length message m as input and giving a ciphertext c as output, e.g. by using one of the symmetric encryption systems specified in ISO/IEC 18033-3[9] and ISO/IEC 18033-4[10]

$EK_{X,\,Y}$ symmetric encryption key shared between X and Y

eKG ephemeral public/private key pair generation function

eKV ephemeral public key validation function

epk_X entity X's ephemeral public key

esk_X entity X's ephemeral private key corresponding to epk_X

GE group element under either discrete logarithm or elliptic curve setting

H hash-function taking an octet string as input and giving a bit string as output, e.g. one of the dedicated hash-functions specified in ISO/IEC 10118-3[4]

h_X entity X's private key agreement key corresponding to p_X

$K_{X,\,Y}$ symmetric key shared between two entities X and Y

MAC(K, m) MAC function taking a symmetric key K and a variable-length message m as input and giving a fixed-length cryptographic checksum μ_X as output, e.g., by using one of the MAC algorithms specified in ISO/IEC 9797-2[3]

MAX(x, y) maximum value function taking two integers x and y as input and giving the maximum value between x and y as output

MIN(x, y)	minimum value function taking two integers x and y as input and giving the minimum value between x and y as output
MiX	step i performed by entity X in a mechanism
p_X	entity X's public key agreement key
$pwd_{S,\,C}$	password shared between a domain server S and a domain client C
S_A, S_B	distinguishing identities of domain servers of clients A and B, respectively, represented as octet strings
SI	group setting index
sid	session identity which is uniquely indicating to the session
SK_X	entity X's private signature key corresponding to VK_X
sn_A	session id contribution from entity A
TK	2SAKE symmetric authentication key
ts	timestamp specifying a start time and an end time
VK_X	entity X's public verification key
μ_X	cryptographic checksum generated from a MAC function by entity X
Σ	digital signature system
σ_X	digital signature generated from Σ.SIG by entity X
Σ.SIG(SK_X, m)	private signature transformation function taking entity X's private signature key SK_X and a variable-length message m as input and giving a digital signature σ_X as output, e.g. by using one of the digital signature systems specified in ISO/IEC 9796 (all parts)[2] and ISO/IEC 14888 (all parts)[8]
Σ.VER(VK_X, m, σ_X)	public signature verification function taking entity X's public verification key VK_X, a variable-length message m and a digital signature σ_X as input, and giving a single bit output: 0 (invalid) or 1 (valid)
||	X||Y denotes the result of the concatenation of octet strings X and Y in the order specified. In cases where the result of concatenating two or more octet strings is input to a cryptographic function as part of one of the mechanisms specified in this document, this result shall be composed so that it can be uniquely resolved into its constituent octet strings, i.e. so that there is no possibility of ambiguity in interpretation. This latter property can be achieved in a variety of different ways, depending on the application. For example, it can be guaranteed by a) fixing the length of each of the octet strings throughout the domain of use of the mechanism, or b) encoding the sequence of concatenated octet strings using a method that guarantees unique decoding, e.g. using the distinguished encoding rules defined in ISO/IEC 8825-1[1].
|y|	bit length of a binary string y