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*