INTERNATIONAL STANDARD

ISO/IEC 20009-4

First edition
2017-08

Information technology — Security techniques — Anonymous entity authentication —

Part 4: Mechanisms based on weak secrets

Technologies de l'information — Techniques de sécurité — Authentification d'entité anonyme —

Partie 4: Mécanismes basés sur des secrets faibles

Reference number
ISO/IEC 20009-4:2017(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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 ISO documents 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 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).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

A list of all parts in the ISO/IEC 20009 series can be found on the ISO website.

Introduction

Inputting a user's "identity (ID)" together with a "password" has almost certainly been the most common method of user authentication since the advent of computers and remains very widely used. Every day, there are probably billions of instances of password-based user authentications in cyberspace. One reason for the wide acceptance of password-based authentication is portability; no dedicated device is required, and a user needs only memorize a password and can then be authenticated anywhere and anytime. ISO/IEC 11770-4 specifies key management mechanisms that are based on passwords (usually passwords are weak secrets). These mechanisms can be used to achieve password-based entity authentication.

Individual privacy in cyberspace is an area of increasing concern. Protection of user privacy during entity authentication is a critical step towards individual privacy protection in cyberspace. ISO/IEC 20009 specifies privacy preserving entity authentication techniques, supporting anonymous entity authentication. This document focuses on anonymous entity authentication mechanisms based on weak secrets. In particular, it specifies password-based anonymous entity authentication (PAEA) mechanisms that enable password authentication with simultaneous protection of user privacy.

PAEA mechanisms need to address the fact that use of a weak secret such as a password with an anonymous authentication mechanism intended to be used with a strong secret cannot protect user privacy because a weak secret reveals information. This document specifies two types of PAEA mechanisms: password-only PAEA mechanisms and storage-extra PAEA mechanisms. In a password-only PAEA mechanism, users register their password verification data at the authentication server and remember their passwords in the same way as when using non-anonymous password authentication mechanisms. In a storage-extra PAEA mechanism, users not only remember their passwords, but also hold password-wrapped credentials that can be revealed to adversaries without compromising user privacy. In mechanisms of the latter type, user password verification data are not saved at the server. Mechanisms of both types have advantages in certain scenarios.

NOTE Annex A gives object identifiers for the PAEA mechanisms specified in this document.

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of patents.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured ISO and IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC. Information may be obtained from:

National Institute of Advanced Industrial Science and Technology
1-1-1 Umezono
Tsukuba
Ibaraki 305-8560
Japan

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and/or IEC shall not be held responsible for identifying any or all such patent rights.

ISO (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up to date information concerning patents.

Information technology — Security techniques — Anonymous entity authentication —

Part 4: Mechanisms based on weak secrets

1 Scope

This document specifies anonymous entity authentication mechanisms based on weak secrets. The precise operation of each mechanism is specified, together with details of all inputs and outputs. This document is applicable to situations in which the server only verifies that the user belongs to a certain user group without obtaining any information that can be used to identify the user later on.

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 9797-2, *Information technology — Security techniques — Message authentication codes (MACs) — Part 2: Mechanisms using a dedicated hash-function*

ISO/IEC 10118-3, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

ISO/IEC 11770-4:2006, *Information technology — Security techniques — Key management — Part 4: Mechanisms based on weak secrets*

ISO/IEC 18033-4, *Information technology — Security techniques — Encryption algorithms — Part 4: Stream ciphers*

ISO/IEC 19772:2009, *Information technology — Security techniques — Authenticated encryption*

ISO/IEC 20009-1, *Information technology — Security techniques — Anonymous entity authentication — Part 1: General*