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)

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

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 20009-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
abelian group
group (S, $*$) such that $a*b = b*a$ for every a and b in S

[SOURCE: ISO/IEC 15946-1:2016, 3.1]

3.2
authenticated encryption
(reversible) transformation of data by a cryptographic algorithm to produce ciphertext that cannot be altered by an unauthorized entity without detection, i.e. provides data confidentiality, data integrity, and data origin authentication

[SOURCE: ISO/IEC 19772:2009, 3.1]

3.3
authentication credential
credential (3.7) containing information that can be used to help authenticate the entity

3.4
authenticator
data string that is sent to and verified by the other entity as part of the mechanism

3.5
claimant
entity which is or represents a principal for the purposes of authentication

Note 1 to entry: A claimant includes the functions and the private data necessary for engaging in authentication exchanges on behalf of a principal.

[SOURCE: ISO/IEC 9798-1:2010, 3.6]

3.6
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 1 to entry: Computational feasibility depends on the specific security requirements and environment.

[SOURCE: ISO/IEC 10118-1:2016, 3.1]

3.7
credential
representation of an identity

Note 1 to entry: A credential is typically made to facilitate data authentication of the identity information in the identity it represents.

Note 2 to entry: The identity information represented by a credential can be printed on paper or stored within a physical token that typically has been prepared in a manner to assert the information as valid.

EXAMPLE A credential can be a username, a username with a password, a PIN, a smartcard, a token, a fingerprint, a passport, etc.

[SOURCE: ISO/IEC 24760-1:2011, 3.3.5]

3.8
cyclic group
abelian group (3.1) (G, *) such that there exists an element g in G, called the generator of the group, such that for any element a in G, there exists an integer i with $a = g^i$

3.9
distinguishing identifier
information which unambiguously distinguishes an entity

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

3.10
exhaustive search
attack technique, also known as brute-force, involving searching through all possibilities for a secret value

3.11
field
set of elements S and a pair of operations (+, *) defined on S such that: (i) $a*(b + c) = a*b + a*c$ for every a, b and c in S, (ii) S together with + forms an *abelian group* (3.1) (with identity element 0), and (iii) S excluding 0 together with * forms an abelian group

[SOURCE: ISO/IEC 15946-1:2016, 3.4]

3.12
finite field
field containing a finite number of elements

Note 1 to entry: For any positive integer, m, and a prime, p, there exists a finite field containing exactly p^m elements. This field is unique up to isomorphism and is denoted by $F(p^m)$, where p is called the characteristic of $F(p^m)$.

[SOURCE: ISO/IEC 15946-1:2016, 3.5]

3.13
group
set of elements S and an operation * defined on the set of elements such that (i) $a*(b*c) = (a*b)*c$ for every a, b and c in S, (ii) there exists an identity element e in S such that $a*e = e*a = a$ for every a in S, and (iii) for every a in S, there exists an inverse element a^{-1} in S such that $a*a^{-1} = a^{-1}*a = e$

[SOURCE: ISO/IEC 15946-1:2016, 3.6]

3.14
group generator
generator of a cyclic group

3.15
homomorphic encryption
symmetric or asymmetric encryption that allows third parties to perform operations on plaintext data while keeping them in encrypted form

Note 1 to entry: Third parties refer to parties that are neither the encryptor nor the decryptor.

3.16
message authentication code algorithm
MAC algorithm
algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following two properties:

- for any key and any input string, the function can be computed efficiently;
- for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of a set of input strings and corresponding function values, where the value of the ith input string might have been chosen after observing the value of the first i-1 function values (for integers $i > 1$).

Note 1 to entry: A MAC algorithm is sometimes called a cryptographic check function (see for example ISO 7498-2).

Note 2 to entry: Computational feasibility depends on the user's specific security requirements and environment.

[SOURCE: ISO/IEC 9797-1:2011, 3.10]

3.17
offline exhaustive search
exhaustive search or brute-force attack that is performed without interacting with any of the authorized parties

3.18
password
secret word, phrase, number or character sequence used for entity authentication, which is a memorized weak secret

[SOURCE: ISO/IEC 11770-4:2006, 3.25]

3.19
password verification data
data that is used to verify an entity's knowledge of a specific *password* (3.18)

[SOURCE: ISO/IEC 11770-4:2006, 3.29]

3.20
password wrapped credential
authentication credential (3.3) generated as a function of a *password* (3.18) in a protected format that resists *offline exhaustive search* (3.17) of passwords

3.21
prime field
finite field (3.12) containing a prime number of elements

3.22
pseudo distinguishing identifier
information which unambiguously distinguishes an entity, but which is valid for only a limited period of time

3.23
secure prime
prime integer p such that $(p - 1) / 2$ has only large prime factors

3.24
system parameters
choice of parameters that selects a particular cryptographic scheme or function from a family of cryptographic schemes or functions

[SOURCE: ISO/IEC 18033-2:2006, 3.41]

4 Symbols, abbreviated terms and conversion functions

4.1 Symbols and abbreviated terms

For the purposes of this document, the symbols and abbreviated terms given in ISO/IEC 20009-1 and the following apply.

AD_K decryption function for an authenticated encryption scheme using K as the key; that shall be selected from among those standardized in ISO/IEC 19772

AE_K encryption function for an authenticated encryption scheme using K as the key; that shall be selected from among those standardized in ISO/IEC 19772

$a \bmod n$ for an integer a and a positive integer n, the unique integer $r \in [0, n - 1]$ such that $r \equiv a \pmod{n}$

$a \equiv b \pmod{n}$ for a non-zero integer n, a relation between integers a and b that holds if and only if a and b are congruent modulo n, i.e. $n|(a - b)$

$a^{-1} \bmod n$ for an integer a and a positive integer n such that $\gcd(a, n) = 1$, the unique integer $b \in [1, n - 1]$ such that $ab \equiv 1 \pmod{n}$

CRL credential revocation list

DEC_{pw} decryption function for a stream cipher algorithm using a key derived from a password, pw, (and using a random initial value if the algorithm requires it); shall be selected from among those standardized in ISO/IEC 18033-4

ENC_{pw} encryption function for a stream cipher algorithm using a key derived from a password, pw, (and using a random initial value if the algorithm requires it); shall be selected from among those standardized in ISO/IEC 18033-4

$E(F(p))$ a set of $F(p)$-valued points of an elliptic curve and an extra point O_E referred to as the point at infinity (see ISO/IEC 15946-1)

$F(p)$ a finite field containing p elements, where p is a prime or a power of a prime

$\gcd(a, b)$ for integers a and b, the greatest common divisor of a and b, i.e. the largest positive integer that divides both a and b (or 0 if $a = 0$ or $b = 0$)

g^x if g is an element of the finite field $F(p)$, then this denotes g^x computed in $F(p)$ where g is a generator of a cyclic group of prime order, q. If g is an elliptic curve point, then this denotes an elliptic curve scalar multiplication $[x]g$, where x is a scalar and g is a base point of prime order q on the elliptic curve

$g_1{*}g_2$ if g_1 and g_2 are elements of the finite field $F(p)$, then this denotes $g_1{*}g_2$ computed in $F(p)$. If g_1 and g_2 are elliptic curve points, then this denotes $g_1 + g_2$ for the cyclic group operation + defined over the elliptic curve

g_1/g_2 if g_1 and g_2 are elements of the finite field $F(p)$, then this denotes g_1/g_2 computed in $F(p)$. If g_1 and g_2 are elliptic curve points, then this denotes $g_1 - g_2$ for the cyclic group operation − defined over the elliptic curve

H a collision-resistant hash-function taking a bit/octet string as input and giving a bit/octet string as output; shall be selected from among those standardized in ISO/IEC 10118

HD_{sk} decryption function under a private key sk of a homomorphic encryption scheme

HE_{pk} encryption function under a public key pk of a homomorphic encryption scheme

H_g a collision-resistant hash-function taking a bit/octet string as input and giving a generator of a cyclic group of prime order, q, as output, which shall be made up of the composition of a hash-function selected from among those standardized in ISO/IEC 10118-3 and a function $R_{1\mathrm{DL}}$ or $R_{1\mathrm{EC}}$ in ISO/IEC 11770-4 that converts a bit string to a cyclic group element

H_λ a collision-resistant hash-function taking a bit/octet string as input and giving a bit/octet string of bit length, λ, as output; shall be selected from among those standardized in ISO/IEC 10118-3 and whose output is truncated to λ bits

I_S octet string representing the distinguishing identifier of the authentication server S

I_U octet string representing the distinguishing identifier of a user U, a claimant or a group of users

I_{U_i} octet string representing the distinguishing identifier of a user U_i from a group of users U_1, U_2, …, U_n

$\underline{I}_{\mathrm{U}_i}$ octet string representing the pseudo distinguishing identifier for a user U_i