INTERNATIONAL STANDARD

ISO/IEC 9798-1

Third edition
2010-07-01

Information technology — Security techniques — Entity authentication —

Part 1:
General

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

Partie 1: Généralités

Reference number
ISO/IEC 9798-1:2010(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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

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 9798-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC 9798-1:1997), which has been technically revised.

ISO/IEC 9798 consists of the following parts, under the general title *Information technology — Security techniques — Entity authentication*:

- *Part 1: General*
- *Part 2: Mechanisms using symmetric encipherment algorithms*
- *Part 3: Mechanisms using digital signature techniques*
- *Part 4: Mechanisms using a cryptographic check function*
- *Part 5: Mechanisms using zero-knowledge techniques*
- *Part 6: Mechanisms using manual data transfer*

Introduction

In systems involving real-time communication, entity authentication is a fundamentally important security service. Depending on the specific application and security goals, entity authentication can involve the use of a simple one-pass protocol providing unilateral authentication, or a multi-pass protocol providing unilateral or mutual authentication between the communicating parties.

The goal of entity authentication is to establish whether the claimant of a certain identity is in fact who it claims to be. In order to achieve this goal, there should be a pre-existing infrastructure which links the entity to a cryptographic secret (for instance a Public Key Infrastructure). The establishment of such an infrastructure is beyond the scope of ISO/IEC 9798.

A variety of entity authentication protocols are specified in ISO/IEC 9798 in order to cater for different security systems and security goals. For instance, when replay attacks are not practical or not an issue for a specific system, simple protocols with fewer passes between claimant and verifier may suffice. However, in more complex communication systems, man-in-the-middle attacks and replay attacks are a real threat. In such cases one of the more involved protocols of ISO/IEC 9798 will be necessary to achieve the security goals of the system.

There are two main models for authentication protocols. In one model, the claimant and verifier communicate directly in order to establish the authenticity of the claimant identity. In the other model, entities establish authenticity of identities using a common trusted third party.

The security properties of a scheme that must be considered before choosing an authentication protocol include the following:

- replay attack prevention;
- reflection attack prevention;
- forced delay prevention;
- mutual/unilateral authentication;
- whether a pre-established secret can be used, or a trusted third party needs to be involved to help establish such a shared secret.

Information technology — Security techniques — Entity authentication —

Part 1: General

1 Scope

This part of ISO/IEC 9798 specifies an authentication model and general requirements and constraints for entity authentication mechanisms which use security techniques. These mechanisms are used to corroborate that an entity is the one that is claimed. An entity to be authenticated proves its identity by showing its knowledge of a secret. The mechanisms are defined as exchanges of information between entities and, where required, exchanges with a trusted third party.

The details of the mechanisms and the contents of the authentication exchanges are given in subsequent parts of ISO/IEC 9798.

2 Normative references

There are no normative references for this part of ISO/IEC 9798.

3 Terms and definitions

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

3.1
asymmetric cryptographic technique
cryptographic technique that uses two related transformations: a public transformation (defined by the public key) and a private transformation (defined by the private key)

NOTE The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation.

3.2
asymmetric encryption system
system based on asymmetric cryptographic techniques whose public operation is used for encryption and whose private operation is used for decryption

3.3
asymmetric key pair
pair of related keys where the private key defines the private transformation and the public key defines the public transformation

3.4
asymmetric signature system
system based on asymmetric cryptographic techniques whose private transformation is used for signing and whose public transformation is used for verification

3.5
challenge
data item chosen at random and sent by the verifier to the claimant, which is used by the claimant, in conjunction with secret information held by the claimant, to generate a response which is sent to the verifier

3.6
claimant
entity which is or represents a principal for the purposes of authentication

NOTE A claimant includes the functions and the private data necessary for engaging in authentication exchanges on behalf of a principal.

3.7
ciphertext
data which has been transformed to hide its information content

3.8
cryptographic check function
cryptographic transformation which takes as input a secret key and an arbitrary string, and which gives a cryptographic check value as output

NOTE The computation of a correct check value without knowledge of the secret key shall be infeasible.

3.9
cryptographic check value
information which is derived by performing a cryptographic transformation on the data unit

3.10
decryption
reversal of a corresponding encryption

3.11
digital signature (signature)
data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient

3.12
distinguishing identifier
information which unambiguously distinguishes an entity in the context of an authentication exchange

3.13
encryption
reversible operation by a cryptographic algorithm converting data into ciphertext so as to hide the information content of the data

3.14
entity authentication
corroboration that an entity is the one claimed

3.15
interleaving attack
masquerade which involves use of information derived from one or more ongoing or previous authentication exchanges

3.16
key
sequence of symbols that controls the operation of a cryptographic transformation

NOTE Examples are encryption, decryption, cryptographic check function computation, signature generation, or signature verification.

3.17
masquerade
pretence by an entity to be a different entity

3.18
mutual authentication
entity authentication which provides both entities with assurance of each other's identity

3.19
plaintext
unenciphered information

3.20
principal
entity whose identity can be authenticated

3.21
private decryption key
private key which defines the private decryption transformation

3.22
private key
key of an entity's asymmetric key pair that is kept secret and which should only be used by that entity

3.23
private signature key
private key which defines the private signature transformation

NOTE This is sometimes referred to as a secret signature key.

3.24
public encryption key
public key which defines the public encryption transformation

3.25
public key
key of an entity's asymmetric key pair which can be made public

3.26
public key certificate (certificate)
public key information of an entity signed by the certification authority and thereby rendered unforgeable

NOTE See also Annex C.

3.27
public key information
information specific to a single entity and which contains at least the entity's distinguishing identifier and a public key for this entity

NOTE Other information regarding the certification authority, the entity, and the public key may be included in the public key certificate, such as the validity period of the public key, the validity period of the associated private key, or the identifier of the involved algorithms (see also Annex C).

3.28
public verification key
public key which defines the public verification transformation

3.29
random number
time variant parameter whose value is unpredictable (see also Annex B)

3.30
reflection attack
masquerade which involves sending a previously transmitted message back to its originator

3.31
replay attack
masquerade which involves use of previously transmitted messages

3.32
sequence number
time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period

NOTE See also Annex B.

3.33
symmetric cryptographic technique
cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation

NOTE Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation.

3.34
symmetric encryption algorithm
encryption algorithm that uses the same secret key for both the originator's and the recipient's transformation

3.35
time stamp
time variant parameter which denotes a point in time with respect to a common reference

NOTE See also Annex B.

3.36
time variant parameter
data item used to verify that a message is not a replay, such as a random number, a time stamp or a sequence number

NOTE See also Annex B.

3.37
token
message consisting of data fields relevant to a particular communication and which contains information that has been transformed using a cryptographic technique

3.38
trusted third party
security authority or its agent, trusted by other entities with respect to security related activities

NOTE In the context of ISO/IEC 9798, a trusted third party is trusted by a claimant and/or a verifier for the purposes of authentication.

3.39
unilateral authentication
entity authentication which provides one entity with assurance of the other's identity but not vice versa

3.40
verifier
entity which is or represents the entity requiring an authenticated identity

NOTE A verifier includes the functions necessary for engaging in authentication exchanges.

4 Symbols and abbreviated terms

A the distinguishing identifier of entity A

B the distinguishing identifier of entity B

TP the distinguishing identifier of the trusted third party

TTP the trusted third party

K_{XY} a secret key shared between entities X and Y, used in symmetric cryptographic techniques

P_X a public verification key associated with entity X, used in asymmetric cryptographic techniques

S_X a private signature key associated with entity X, used in asymmetric cryptographic techniques

N_X a sequence number issued by entity X

R_X a random number issued by entity X

T_X a time stamp issued by entity X

T_X/N_X a time variant parameter originated by entity X which is either a time stamp T_X or a sequence number N_X

$Y||Z$ The result of the concatenation of data items Y and Z in the order specified. In cases where the result of concatenating two or more data items is input to a cryptographic algorithm as part of an authentication mechanism, this result shall be composed so that it can be uniquely resolved into its constituent data strings, i.e. so that there is no possibility of ambiguity in interpretation. This latter property could be achieved in a variety of different ways, depending on the application. For example, it could be guaranteed by (a) fixing the length of each of the substrings throughout the domain of use of the mechanism, or (b) encoding the sequence of concatenated strings using a method that guarantees unique decoding, e.g. using the distinguished encoding rules defined in ISO/IEC 8825-1 [3].

$e_K(Z)$ the result of the encryption of data Z with a symmetric encryption algorithm using key K

$d_K(Z)$ the result of the decryption of data Z with a symmetric encryption algorithm using key K

$f_K(Z)$ a cryptographic check value which is the result of applying the cryptographic check function f using as input a secret key K and an arbitrary data string Z

CertX a trusted third party's certificate for entity X

TokenXY a token sent from entity X to entity Y

TVP a time variant parameter

$sS_X(Z)$ the signature resulting from applying the private signature transformation to data Z using the private signature key S_X

5 Authentication model

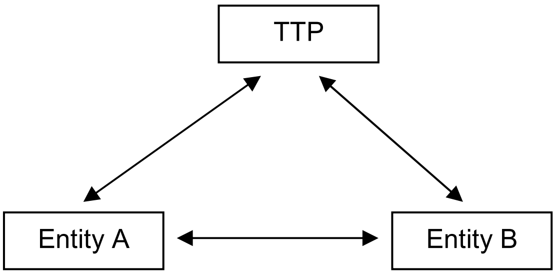

Figure 1 — Authentication model

The general model for entity authentication mechanisms is shown in Figure 1. It is not essential that all the entities and exchanges are present in every authentication mechanism.

For the authentication mechanisms specified in the other parts of ISO/IEC 9798, for unilateral authentication, entity A is considered the claimant, and entity B is considered the verifier. For mutual authentication, A and B each take the roles of both claimant and verifier.

For authentication purposes, the entities generate and exchange standardised messages, called tokens. It takes the exchange of at least one token for unilateral authentication and the exchange of at least two tokens for mutual authentication. An additional pass may be needed if a challenge has to be sent to initiate the authentication exchange. Additional passes may be needed if a trusted third party is involved.

In Figure 1 the lines indicate potential information flow. Entities A and B may directly interact with each other, directly interact with the trusted third party through B or A respectively, or use information issued by the trusted third party.

The details of the authentication mechanisms of ISO/IEC 9798 are specified in the subsequent parts.

6 General requirements and constraints

In order that an entity can authenticate another entity, both shall use a common set of cryptographic techniques and parameters.

During the operational life of a key, the values of all time-variant parameters on which the key operates (i.e. time stamps, sequence numbers and random numbers) shall be non-repeating, at least with overwhelming probability.

It is assumed that, during use of an authentication mechanism, the entities A and B are aware of each other's claimed identities. This may be achieved by the inclusion of identifiers in information exchanges between the two entities, or it may be apparent from the context of the use of the mechanism.

The authenticity of the entity can be ascertained only for the instant of the authentication exchange. To guarantee the authenticity of subsequent communicated data, the authentication exchange must be used in conjunction with a secure means of communication (e.g. an integrity service).

Annex A
(informative)

Use of text field

The tokens specified in the following parts of ISO/IEC 9798 contain text fields. The actual use of and the relationship between the various text fields in a given pass depend on the application.

Text fields may contain additional time variant parameters. For instance, a time stamp may be included in the text field(s) of a token if the mechanism uses sequence numbers. This would allow the detection of forced delays by requiring the recipient of a message to verify that any time stamp contained in the message is within a prespecified time window (see also Annex B).

If more than one valid key exists, then an identifier for the key may be included in a text field in the plaintext. If more than one trusted third party exists, then text fields could be used to include the distinguishing identifier of the trusted third party in question.

Text fields could also be used for the distribution of keys (see ISO/IEC 11770-2 and ISO/IEC 11770-3).

Should any of the mechanisms specified in the following parts of ISO/IEC 9798 be embedded in an application which allows either entity to initiate the authentication by using an additional message prior to the start of the mechanism, certain intruder attacks may become possible. Text fields may be used to state which entity requests the authentication in order to counteract such attacks, which are characterised by the fact that an intruder may reuse a token obtained illicitly (see ISO/IEC 10181-2).

The above examples are not exhaustive.

Annex B
(informative)

Time variant parameters

B.1 The three time variant parameters

Time variant parameters are used to control uniqueness / timeliness. They enable replay of previously transmitted messages to be detected. To achieve this, the authentication information should vary from one exchange instance to the next.

Some types of time variant parameters may also allow for the detection of "forced delays" (delays introduced into the communication medium by an adversary). In mechanisms involving more than one pass, forced delays may also be detected by other means (such as "timeout clocks" used to enforce maximum allowable time gaps between specific messages).

The three types of time variant parameters used in the following parts of ISO/IEC 9798 are time stamps, sequence numbers, and random numbers. Implementation requirements may make different types of time variant parameters preferable in different applications. In some cases it may be appropriate to use more than one type of time variant parameter (e.g. both time stamps and sequence numbers). Details regarding the choice of these parameters are beyond the scope of this part of ISO/IEC 9798.

B.2 Time stamps

Mechanisms involving time stamps make use of a common time reference which logically links a claimant and a verifier. The recommended reference clock is Coordinated Universal Time (UTC). An acceptance window of some fixed size is used by the verifier. Timeliness is controlled by the verifier computing the difference between the time stamp in a verified received token and the time as perceived by the verifier at the time the token is received. If the difference is within the window the message is accepted. Uniqueness can be verified by logging all messages within the current window, and rejecting the second and subsequent occurrences of identical messages within that window.

Some mechanism should be used to ensure that the time clocks of the communicating entities are synchronised. Moreover, time clocks need to be synchronised well enough to make the possibility of impersonation by replay acceptably small. It should also be ensured that all information relevant to the verification of time stamps, in particular the time clocks of the two communicating entities, are protected against tampering.

Mechanisms using time stamps allow the detection of forced delays.

B.3 Sequence numbers

Uniqueness can be controlled using sequence numbers as they enable a verifier to detect the replay of messages. A claimant and verifier agree beforehand on a policy for numbering messages in a particular manner, the general idea being that a message with a particular number will be accepted only once (or only once within a specified time period). Messages received by a verifier are then checked to see that the number sent along with the message is acceptable according to the agreed policy. A message is rejected if the accompanying sequence number is not in accordance with the agreed policy.

Use of sequence numbers may require additional "book keeping". A claimant may need to maintain records of sequence numbers which have been used previously and/or sequence numbers that remain valid for future use. The claimant may need to keep such records for all potential verifiers with whom the claimant may wish to communicate. Similarly, the verifier should maintain such records corresponding to all potential claimants. Special procedures may also be required to reset and/or restart sequence number counters when situations (such as system failures) arise which disrupt normal sequencing.

Use of sequence numbers by a claimant does not guarantee that a verifier will be able to detect forced delays. For mechanisms involving two or more messages, forced delays can be detected if the sender of a message measures the time interval between transmission of a message and receipt of an expected reply, and rejects it if the delay is more than a prespecified period of time.

B.4 Random numbers

The random numbers used in mechanisms specified in the following parts of ISO/IEC 9798, prevent replay or interleaving attacks. It is therefore required that all random numbers used in ISO/IEC 9798 are chosen from a sufficiently large range so that the probability of repetition is very small when used with the same key, and also that the probability of a third party predicting a specified value is very small. In the context of ISO/IEC 9798, the use of the term random numbers also includes pseudo-random numbers satisfying the same requirements.

In order to prevent replay or interleaving attacks, the verifier obtains a random number which is sent to the claimant, and the claimant responds by including the random number in the protected part of the returned token. (This is commonly referred to as challenge-response). This procedure links the two messages containing the particular random number. If the same random number were to be used by the verifier again, a third party that recorded the original authentication exchange could send the recorded token to the verifier and falsely authenticate itself as the claimant. The requirement that the random number be non-repeating with very high probability is present in order to prevent such attacks.

Use of random numbers by a claimant does not guarantee that a verifier will be able to detect forced delays.

ISO/IEC 18031 specifies techniques for the generation of random numbers for cryptographic applications.

Annex C
(informative)

Certificates

In some of the mechanisms specified in the following parts of ISO/IEC 9798, public key certificates (certificates) can be used to ensure the authenticity of public keys. In this case a certificate contains an entity's public key information, which consists of at least the entity's distinguishing identifier and public key. Other information may be included in the public key information regarding the trusted third party, the entity, and the public key, such as the validity period of the public key, the validity period of the associated private key, or the identifiers of the involved algorithms. The certificate consists of the public key information signed by the trusted third party.

The verification of a certificate involves verifying the signature of the trusted third party, and checking, if required, other conditions related to the validity of the certificate such as the revocation or the validity period.

Certificates are not the only way of guaranteeing the authenticity of public keys. To allow an entity to obtain the public keys of other entities by other means, the use of certificates is optional in all mechanisms in the following parts of ISO/IEC 9798. Other methods of guaranteeing the authenticity of public keys include identity-based signature schemes such as those specified in ISO/IEC 14888-2.

Bibliography

[1] ISO/IEC 7498-1:1994, *Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*

[2] ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

[3] ISO/IEC 8825-1:2002, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

[4] ISO/IEC 9594-8:2005, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks*

[5] ISO/IEC 9796-2:2002, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

[6] ISO/IEC 10181-1:1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview*

[7] ISO/IEC 10181-2:1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Authentication Framework*

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

[9] ISO/IEC 11770-2:2008, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*

[10] ISO/IEC 11770-3:2008, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

[11] ISO/IEC 13888-1:2009, *Information technology — Security techniques — Non-repudiation — Part 1: General*

[12] ISO/IEC 14888-1:2008, *Information technology — Security techniques — Digital signatures with appendix — Part 1: General*

[13] ISO/IEC 14888-2:2008, *Information technology — Security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms*

[14] ISO/IEC 14888-3:2006, *Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*

[15] ISO/IEC 18031:2005, *Information technology — Security techniques — Random bit generation*

ICS 35.040

Price based on 11 pages