
**Information technology — Security
techniques — Entity authentication —**

**Part 1:
General**

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

Partie 1: Généralités

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 9798-1:2010

<https://standards.iteh.ai/catalog/standards/sist/ae2fd4c4-be3e-4104-8a65-d7773d347a4c/iso-iec-9798-1-2010>

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 9798-1:2010

<https://standards.iteh.ai/catalog/standards/sist/ae2fd4c4-be3e-4104-8a65-d7773d347a4c/iso-iec-9798-1-2010>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2010

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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	iv
Introduction.....	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	5
5 Authentication model	6
6 General requirements and constraints	6
Annex A (informative) Use of text field	7
Annex B (informative) Time variant parameters	8
Annex C (informative) Certificates	10
Bibliography	11

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 9798-1:2010

<https://standards.iteh.ai/catalog/standards/sist/ac2fd4c4-be3e-4104-8a65-d7773d347a4c/iso-iec-9798-1-2010>

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.

iTeh STANDARD PREVIEW **(standards.iteh.ai)**

ISO/IEC 9798-1:2010

<https://standards.iteh.ai/catalog/standards/sist/ae2fd4c4-be3e-4104-8a65-d7773d347a4c/iso-iec-9798-1-2010>

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)