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)

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