INTERNATIONAL STANDARD

ISO/IEC 9798-6

First edition
2005-08-01

Information technology — Security techniques — Entity authentication —

Part 6: Mechanisms using manual data transfer

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

Partie 6: Mécanismes utilisant un transfert manuel de données

Reference number
ISO/IEC 9798-6:2005(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 9798-6 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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

Within networks of communicating devices it is often necessary for two devices to perform an entity authentication procedure using a channel which may be subject to both passive and active attacks, where an active attack may include a malicious third party introducing data into the channel and/or modifying, deleting or repeating data legitimately sent on the channel. Other parts of this International Standard describe entity authentication mechanisms applicable when the two devices share a secret key, or where one device has an authenticated copy of a public key for the other device.

In this part of ISO/IEC 9798, entity authentication mechanisms, referred to as manual authentication mechanisms, are specified where there is no such assumption of pre-established keying relationships. Instead entity authentication is achieved by manually transferring short data strings from one device to the other, or by manually comparing short data strings output by the two devices.

For the purposes of this part of ISO/IEC 9798, the meaning of the term entity authentication is different to the meaning applied in other parts of ISO/IEC 9798. Instead of one device verifying that the other device has a claimed identity (and vice versa), both devices in possession of a user verify that they correctly share a data string with the other device at the time of execution of the mechanism. Of course, this data string could contain identifiers for one or both of the devices.

As described in informative annexes A and B, a manual authentication mechanism may be used as the basis for secret key establishment or reliable exchange of public keys. A manual authentication mechanism could also be used for reliable exchange of other secret or public security parameters, including security policy statements or timestamps.

Information technology — Security techniques — Entity authentication —

Part 6: Mechanisms using manual data transfer

1 Scope

This part of ISO/IEC 9798 specifies four entity authentication mechanisms based on manual data transfer between authenticating devices. As described in Annexes A and B, these mechanisms may be used to support key management functions; guidance on secure choice of parameters for the mechanisms is provided in Annex C.

Such mechanisms may be appropriate in a variety of circumstances. One such application occurs in personal networks, where the owner of two personal devices capable of wireless communications wishes them to perform an entity authentication procedure as part of the process of preparing them for use in the network.

2 Normative references

The following referenced documents are indispensable for the application 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 9798-1:1997, *Information technology — Security techniques — Entity authentication — Part 1: General*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 9798-1 and the following apply.

3.1
check-value
string of bits, computed as the output of a check-value function, sent from the data originator to data recipient that enables the recipient of data to check its correctness

3.2
check-value function
function f which maps strings of bits and a short secret key, i.e. a key that can readily be entered into or read from a user device, to fixed-length strings of bits, satisfying the following properties:

— for any key k and any input string d, the function $f(d, k)$ can be computed efficiently;

— it shall be computationally infeasible to find a pair of data strings (d, d') for which the number of keys which satisfy $f(d, k) = f(d', k)$ is more than a small fraction of the possible set of keys.

NOTE 1 In practice, a short key would typically contain 4-6 digits or alphanumeric characters.

NOTE 2 In practice, security is maximized if the set of possible outputs from the check-value function is the same size as the set of possible keys.