INTERNATIONAL STANDARD

ISO/IEC 9798-6

Second edition
2010-12-01

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 9798-6:2010(E)

© ISO/IEC 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.

This document is a preview generated by EVS

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 3
5 Overall requirements 4
6 Mechanisms using a short check-value 5
6.1 General 5
6.2 Mechanism 1 – One device with simple input, one device with simple output 5
6.3 Mechanism 2 – Devices with simple input capabilities 7
7 Mechanisms using a manual transfer of a short digest-value or a short key 8
7.1 General 8
7.2 Mechanism 3 – One device with simple input, one device with simple output 8
7.3 Mechanism 4 – One device with simple input, one device with simple output 10
7.4 Mechanism 5 – Devices with simple input capabilities 11
7.5 Mechanism 6 – Devices with simple input capabilities 13
8 Mechanisms using a MAC 15
8.1 General 15
8.2 Mechanism 7 – Devices with simple output capabilities 15
8.3 Mechanism 8 – One device with simple input, one device with simple output 18
Annex A (normative) **ASN.1 modules** 20
Annex B (informative) **Using manual authentication protocols for the exchange of secret keys** 21
Annex C (informative) **Using manual authentication protocols for the exchange of public keys** 23
Annex D (informative) **On mechanism security and choices for parameter lengths** 25
Annex E (informative) **A method for generating short check-values** 28
Annex F (informative) **Comparative analysis in security and efficiency of mechanisms 1–8** 30
Annex G (informative) **Methods for generating short digest-values** 33
Bibliography 34

This document is a preview generated by EVS

© ISO/IEC 2010 – All rights reserved

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*.

This second edition cancels and replaces the first edition (ISO/IEC 9798-6:2005), to which a new Clause 7 has been added to provide four new mechanisms. It also incorporates the Technical Corrigendum ISO/IEC 9798-6:2005/Cor.1:2009. Implementations conformant to the first edition will be conformant to the second edition.

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*

This document is a preview generated by EVS

 © ISO/IEC 2010 – All rights reserved

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 can 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 ISO/IEC 9798 specify 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 where there is no such assumption of pre-established keying relationships, referred to as manual authentication mechanisms, are specified. 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 from 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 the 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 B and C, a manual authentication mechanism can be used as the basis for secret key establishment or the reliable exchange of public keys. A manual authentication mechanism could also be used for the reliable exchange of other secret or public security parameters, including security policy statements or timestamps.

This document is a preview generated by EVS

© ISO/IEC 2010 – All rights reserved

Information technology — Security techniques — Entity authentication —

Part 6: Mechanisms using manual data transfer

This document is a preview generated by EVS

1 Scope

This part of ISO/IEC 9798 specifies eight entity authentication mechanisms based on manual data transfer between authenticating devices. It indicates how these mechanisms can be used to support key management functions, and provides guidance on secure choices of parameters for the mechanisms. A comparison of the levels of security and efficiency provided by the eight mechanisms is given.

Such mechanisms can 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 9798-1:2010, *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 the data recipient that enables the recipient of data to check its correctness

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

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

— it is computationally infeasible to find a pair of distinct 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 In practice, a short key would typically contain 4–6 digits or alphanumeric characters.

© ISO/IEC 2010 – All rights reserved