BS ISO/IEC 9798-6:2010

BSI Standards Publication

Information technology — Security techniques — Entity authentication

Part 6: Mechanisms using manual data transfer

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS ISO/IEC 9798-6:2010

National foreword

This British Standard is the UK implementation of ISO/IEC 9798-6:2010. It supersedes BS ISO/IEC 9798-6:2005 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© BSI 2010

ISBN 978 0 580 68073 1

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2010.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 9798-6:2010

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)

Documents
Document Sharing Hub
© ISO/IEC 2010

Full document details: BS ISO/IEC 9798-6:2010

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.

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

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 9798-6:2010

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

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 9798-6:2010

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 9798-6 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*

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 9798-6:2010

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.

Documents
Document Sharing Hub

© ISO/IEC 2010 – All rights reserved

Full document details: BS ISO/IEC 9798-6:2010

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 9798-6:2010

INTERNATIONAL STANDARD ISO/IEC 9798-6:2010(E)

Information technology — Security techniques — Entity authentication —

Part 6: Mechanisms using manual data transfer

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 9798-6:2010

3.3
data origin authentication
corroboration that the source of data received is as claimed

[ISO 7498-2]

3.4
digest-value
string of bits, computed as the output of a digest function, sent from the data originator to the data recipient that enables the recipient of data to check its correctness

3.5
digest function
function d which maps a string of bits and a long secret key to a short and fixed-length string of bits, i.e. a b-bit digest-value, that can readily be entered into or read from a user device, satisfying the following properties:

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

— it is computationally infeasible to find a pair of distinct data strings (m, m') for which the proportion of keys which satisfy $d(m, k) = d(m', k)$ is greater than $(2^{-b} + \varepsilon)$, where b is the bit length of a digest-value and ε is a value that is negligible relative to 2^{-b}.

NOTE 1 In practice, the second digest function property should be satisfied if the key k is of the size of a typical cryptographic hash value, for example, 160 bits. This requirement derives from theoretical lower bounds on the key length for universal hash-functions, which are a general class of digest functions. More detailed discussions of this issue can be found in Annex F.

NOTE 2 See Annexes D, F, and G for further discussions of key and digest lengths.

3.6
hash-function
function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:

— it is computationally infeasible to find for a given output an input which maps to this output;

— it is computationally infeasible to find for a given input a second input which maps to the same output.

[ISO/IEC 10118-1]

3.7
manual authentication certificate
combination of a secret key and a check-value, generated by one of the two devices engaging in manual authentication, with the property that, when entered into the other device, this pair of values can be used to complete the manual authentication process at some later time

3.8
Message Authentication Code
MAC
string of bits which is the output of a MAC algorithm

[ISO/IEC 9797-1]

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 9798-6:2010

3.9
Message Authentication Code algorithm
MAC algorithm
algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following properties:

— for any key and any input string the function can be computed efficiently;

— for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the ith input string may have been chosen after observing the value of the first i-1 function values.

[ISO/IEC 9797-1]

3.10
manual entity authentication
process achieving entity authentication between two devices using a combination of message exchanges via a (potentially insecure) communications channel and the manual transfer of limited amounts of data between the devices

3.11
simple input interface
interface for a device that allows the user to indicate to the device the successful or unsuccessful completion of a procedure, e.g. as could be implemented as a pair of buttons or a single button which is either pressed or not within a certain time interval

3.12
simple output interface
interface for a device that allows the device to indicate to the user the successful or unsuccessful completion of a procedure, e.g. as could be implemented by red and green lights or as single light which is lit in different ways to indicate success or failure

4 Symbols and abbreviated terms

A, B	Labels used for the two devices engaging in a manual entity authentication mechanism
d	Digest function, used in mechanisms 3 and 5, where $d(D,k)$ denotes the digest value computed on data string D using key k
D	Data string whose value is established between devices A and B as the result of performing a manual entity authentication mechanism
h	Hash-function, used in mechanisms 3–6
I_A, I_B	Distinguishing identifiers of A and B respectively
K	(Short) secret key used with a check-value function in mechanisms 1 and 2
k	(Long) secret key used in mechanisms 3–6
K_A, K_{Ai}, K_B, K_{Bi}	Random MAC keys used in mechanisms 7 and 8
MAC	Message Authentication Code
R	(Short) random bit-string used in mechanisms 4, 6, 7, and 8

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 9798-6:2010

|| As defined in ISO/IEC 9798-1, $X||Y$ is used to mean the result of the concatenation of data items X and Y in the order specified. In cases where the result of concatenating two or more data items is input to a function as part of one of the mechanisms specified in this document, 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 [10]

NOTE Annexes D and F provide guidance on appropriate choices for the lengths of short secrets and MAC keys.

5 Overall requirements

The authentication mechanisms specified in this document have the following requirements in addition to the specific requirements specified in Clauses 6, 7 and 8.

a) The pair of devices performing the manual authentication procedure shall be connected via a communications link (e.g. a wireless or Internet link). No security assumptions are made regarding this link; that is, the mechanisms are designed to operate securely even in an environment where an attacker can monitor and change data transferred on this link.

b) The pair of devices performing the manual authentication procedure shall both have a user interface capable of data input and data output.

c) The user data input interface for a device shall, at minimum, be capable of indicating successful or unsuccessful completion of a procedure (e.g. as could be implemented by using either two buttons or a single button which is either pressed or not within a certain time interval); such a means of data input is referred to below as a *simple* input interface. By contrast, a *standard* input interface shall provide means for the input of a short string of symbols, e.g. a numeric, hexadecimal, or alphanumeric keypad. Unless explicitly stated otherwise, it is necessary that every device has a standard means of data input.

d) The user data output interface for a device shall, at minimum, be capable of indicating either success or failure of an authentication procedure (e.g. as could be implemented by means of red and green lights); such a means of data output is referred to below as a *simple* output interface. By contrast, a *standard* output interface shall provide means for the output of a short string of symbols, e.g. a numeric, hexadecimal or alphanumeric display. Unless explicitly stated otherwise, it is necessary that every device has a standard means of data output.

e) For mechanisms 1 and 2, the two devices performing the entity authentication procedure shall have agreed on the use of a specific check-value function, and shall have the means to implement this function.

NOTE 1 Guidance on appropriate choices for check-value functions and lengths for check-values and random keys for use in mechanisms 1 and 2 is provided in Annex D. A construction for an unconditionally secure check-value function suitable for use with mechanisms 1 and 2 is given in Annex E.

f) For mechanisms 3–6, the two devices performing the entity authentication procedure shall have agreed on the use of a specific hash-function h, and shall have the means to implement this function.

NOTE 2 Guidance on appropriate choices for bit lengths for hash-function inputs and outputs for use in mechanisms 3–6 is provided in Annex D.

g) For mechanisms 3 and 5, the two devices performing the entity authentication procedure shall have agreed on the use of a specific digest function d, and shall have the means to implement this function.

NOTE 3 Guidance on digests lengths for use in mechanisms 3 and 5 is provided in Annex D. Constructions for digest functions using MAC algorithms and hash-functions, which are suitable for use with mechanisms 3 and 5, are given in Annex G.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 9798-6:2010

h) For mechanisms 7 and 8, the two devices performing the entity authentication procedure shall have agreed on the use of a specific MAC algorithm, and shall have the means to implement this algorithm.

NOTE 4 Guidance on appropriate choices for MAC algorithms and lengths for MACs and random keys for use in mechanisms 7 and 8 is provided in Annex D.

i) Prior to invocation of mechanisms 1–8, the two devices performing the mechanism shall have exchanged a data string D (in combination with a hash-value in mechanisms 3–6). D may be generated by one device and sent to the other device, or it may consist of the concatenation of data generated by both devices and sent in both directions across the shared communications link.

j) Either a single human user shall be in possession of both devices and shall operate them both, or the two devices shall be operated by two users who share a trusted means of communication.

k) The users of the devices shall be present through the complete running operation to ensure correct processing of these mechanisms. There shall not be a significant delay in manual transfer of data between the devices during this operation. The devices shall automatically time out as indicated in the mechanism specifications to preclude certain attacks.

6 Mechanisms using a short check-value

6.1 General

In this clause two manual authentication mechanisms are specified that are based on the use of a check-value. The two mechanisms are appropriate for different types of devices. Specifically,

— the first mechanism (mechanism 1) is appropriate for the case where one device has a simple input interface and the other has a simple output interface, and

— the second mechanism (mechanism 2) is appropriate for the case where both devices have a simple input interface.

A standard input or output interface can emulate a simple interface, and hence if both devices have standard input and output interfaces then either of the mechanisms may be used.

Both mechanisms operate in the following general way. A data string D is transferred from one device to the other (or is the concatenation of data transferred in both directions) via the shared communications link. The manual entity authentication mechanism is then executed. As a result of the mechanism both devices are provided with assurance that the data string D they possess is the same as the value held by the other device.

6.2 Mechanism 1 – One device with simple input, one device with simple output

6.2.1 Specific requirements

This mechanism has the following specific requirements.

a) The mechanism specified in this subclause is appropriate for the case where one device (device A) has a simple input interface and the other (device B) has a simple output interface.

b) Device A shall have the means to generate keys.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 9798-6:2010

6.2.2 Specification of data exchanged

The following data exchanges and operations shall take place (see also Figure 1).

a) Both devices shall output a signal to acknowledge that they have received data D and that they are ready for the authentication mechanism to commence. On observing that both devices are ready, the user shall then enter a signal into device A to notify A that the mechanism can start.

b) Device A shall generate a random key K, where K is suitable for use with the check-value function shared by the two components. Using this key K, device A shall compute a check-value as a function of the data D. The check-value and the key K shall then be output via the output interface of device A. The user shall read the check-value and the key K from the output interface.

c) The user shall enter the check-value and the key K output by device A to device B using its input interface. Device B shall use the key K to re-compute the check-value as a function of its stored version of data D. If the two check-values agree, then device B shall output a success signal to the user via its simple output interface. Otherwise it shall give a failure signal.

d) The user shall enter the result output by device B, i.e. success or failure, into device A via its simple input interface.

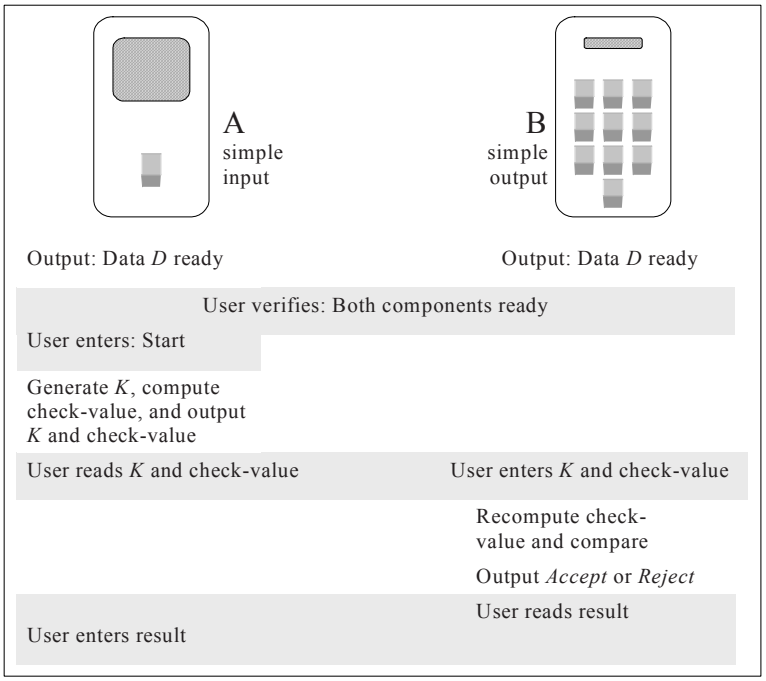

Figure 1 — Manual authentication mechanism 1

6.2.3 Manual authentication certificates

Manual authentication mechanism 1 has the property that no authentication information is transmitted over the insecure channel. Therefore, it does not affect the security of the mechanism if the manual authentication values K and check-value are transferred from device A to device B before the latter has received the actual data D. Naturally, such an approach is applicable only to situations where device A generates the data D. However, in such a case, mechanism 1 offers a means of authenticating data to be received at some later time. Such authentication means is called a manual authentication certificate. A protocol for data origin authentication using a manual authentication certificate is now specified (with the same requirements as specified in subclause 6.2.1). Note that this protocol does not provide entity authentication.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 9798-6:2010