AS/NZS ISO/IEC 9798.6:2006
ISO/IEC 9798-6:2005

AS/NZS ISO/IEC 9798.6:2006

Australian/New Zealand Standard™

Information technology—Security techniques—Entity authentication

Part 6: Mechanisms using manual data transfer

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 9798.6-2006

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT-012, Information Systems, Security and Identification. It was approved on behalf of the Council of Standards Australia on 23 June 2006 and on behalf of the Council of Standards New Zealand on 30 June 2006.
This Standard was published on 2 August 2006.

The following are represented on Committee IT-012:

Attorney General's Department
Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Chamber Commerce and Industry
Australian Electrical and Electronic Manufacturers Association
Certification Forum of Australia
Department of Defence
Department of Social Welfare, NZ
Government Communications Security Bureau, NZ
Internet Industry Association
NSW Police Service
New Zealand Defence Force
Reserve Bank of Australia

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop at www.standards.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

Alternatively, both organizations publish an annual printed Catalogue with full details of all current Standards. For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

This Standard was issued in draft form for comment as DR 06256.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 9798.6-2006

Australian/New Zealand Standard™

Information technology—Security techniques—Entity authentication

Part 6: Mechanisms using manual data transfer

First published as AS/NZS ISO/IEC 9798.6:2006.

COPYRIGHT

© Standards Australia/Standards New Zealand

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Jointly published by Standards Australia, GPO Box 476, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6020

ISBN 0 7337 7658 2

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

AVA Documents Document Sharing Hub

Full document details: AS NZS ISO IEC 9798.6-2006

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Systems, Security and Identification.

The objective of this Standard is to provide information security practitioners with an entity authentication mechanism, referred to as a manual authentication mechanism, where there is no 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.

This Standard is identical with, and has been reproduced from ISO/IEC 9798-6:2005, *Information technology—Security techniques—Entity authentication*—Part 6: *Mechanisms using manual data transfer*.

As this Standard is reproduced from an international standard, the following applies:

(a) Its number appears on the cover and title page while the international standard number appears only on the cover.

(b) In the source text 'this part of ISO/IEC 9798' should read 'this Australian/New Zealand Standard'.

(c) A full point substitutes for a comma when referring to a decimal marker.

The term 'informative' has been used in this Standard to define the application of the annex to which it applies. An 'informative' annex is only for information and guidance.

The document referenced in this Standard has not been adopted as an Australian or Australian/New Zealand Standard.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 9798.6-2006

CONTENTS

Page

1 Scope ... 1

2 Normative references ... 1

3 Terms and definitions ... 1

4 Symbols and abbreviated terms ... 2

5 Requirements ... 3

6 Mechanisms using a short check-value ... 4
6.1 General ... 4
6.2 Mechanism 1 – One device with simple input, one device with simple output ... 4
6.2.1 Requirements ... 4
6.2.2 Specification of data exchanged ... 4
6.2.3 Manual authentication certificates ... 5
6.3 Mechanism 2 – Devices with simple input capabilities ... 6
6.3.1 Requirements ... 6
6.3.2 Specification of data exchanged ... 6

7 Mechanisms using a MAC ... 7
7.1 General ... 7
7.2 Mechanism 3 – Devices with simple output capabilities ... 7
7.2.1 General ... 7
7.2.2 Requirements ... 7
7.2.3 Specification of data exchanged in mechanism 3a ... 7
7.2.4 Specification of data exchanged in mechanism 3b ... 9
7.3 Mechanism 4 – One device with simple input, one device with simple output ... 10
7.3.1 General ... 10
7.3.2 Requirements ... 10
7.3.3 Specification of data exchanged in mechanism 4a ... 10
7.3.4 Specification of data exchanged in mechanism 4b ... 11

Annex A (informative) **Using manual authentication protocols for the exchange of secret keys** ... 12
A.1 General ... 12
A.2 Authenticated Diffie-Hellman key agreement ... 12
A.3 Authenticated Diffie-Hellman key agreement using a manual authentication certificate ... 12
A.3.1 General ... 12
A.3.2 Stage 1 ... 13
A.3.3 Stage 2 (initiated by either device at some later time) ... 13
A.4 More than two components ... 13

Annex B (informative) **Using manual authentication protocols for the exchange of public keys** ... 14
B.1 General ... 14
B.2 Requirements ... 14
B.3 Private key generated in device ... 14
B.4 Private key generated externally ... 15

Annex C (informative) **On mechanism security and choices for parameter lengths** ... 16
C.1 General ... 16
C.2 Use of mechanisms 1 and 2 ... 16
C.3 Use of mechanisms 3 and 4 ... 17

Annex D (informative) **A method for generating short check-values** ... 18
D.1 General ... 18

Bibliography ... 20

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

AVA Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 9798.6-2006

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.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 9798.6-2006

AUSTRALIAN/NEW ZEALAND STANDARD

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.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 9798.6-2006

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

[ISO 7498-2]

3.4
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, these values can be used to complete the manual authentication process at some later time

3.5
Message Authentication Code
MAC
string of bits which is the output of a MAC algorithm

[ISO/IEC 9797-1]

3.6
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]

3.7
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

3.8
simple input interface
interface for a device that shall allow 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

3.9
simple output interface
interface for a device that shall allow 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	Data string whose value is established between devices *A* and *B* as the result of performing a manual entity authentication mechanism

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 9798.6-2006

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_A, K_{Ai}, K_B, K_{Bi}	Random MAC keys used in mechanisms 3 and 4
MAC	Message Authentication Code
R	(Short) random bit-string used in mechanisms 3 and 4

5 Requirements

The authentication mechanisms specified in this part of ISO/IEC 9798 have the following requirements.

a) The pair of devices performing the manual authentication procedure shall be connected via a communications link (e.g. a wireless 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 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 C. A construction for an unconditionally secure check-value function suitable for use with mechanisms 1 and 2 is given in Annex D.

f) For mechanisms 3 and 4, 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 Guidance on appropriate choices for MAC algorithms and lengths for MACs and random keys for use in mechanisms 3 and 4 is provided in Annex C.

g) Prior to invocation of one of the manual authentication mechanisms, the two devices performing the mechanism shall have exchanged a data string D. This 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 communications link.

h) 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.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 9798.6-2006