BS ISO/IEC 9798-4:1999

Incorporating corrigenda September 2009 and July 2012

BSI Standards Publication

Information technology - Security techniques - Entity authentication

Part 4: Mechanisms using a cryptographic check function

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of ISO/IEC 9798-4:1999, incorporating corrigenda September 2009 and July 2012. It supersedes BS ISO/IEC 9798-4:1995 which is withdrawn.

ISO/IEC corrigendum September 2009 introduces two changes to the text: it inserts a bibliography, and adds a new paragraph to Clause 3.

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.

ISBN 978 0 580 76594 0

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 May 2012.

Amendments/corrigenda issued since publication

Date	Text affected
31 August 2012	Implementation of ISO/IEC corrigendum July 2012: Foreword and Clause 4 have been amended, Annex B has been inserted.

INTERNATIONAL STANDARD

ISO/IEC 9798-4

Second edition
1999-12-15

Information technology — Security techniques — Entity authentication —

Part 4: **Mechanisms using a cryptographic check function**

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

Partie 4: Mécanismes utilisant une fonction cryptographique de vérification

Reference number
ISO/IEC 9798-4:1999(E)

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.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 734 10 79
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Contents

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. 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 part of ISO/IEC 9798 may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 9798-4 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 9798-4:1995), which has been technically revised. Note, however, that implementations which comply with ISO/IEC 9798-4 (1st edition) will be compliant with ISO/IEC 9798-4 (2nd 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*

Further parts may follow.

Annex A of this part of ISO/IEC 9798 is for information only.

Annex B of this part of ISO/IEC 9798 is normative, and defines object identifiers.

Information technology — Security techniques — Entity authentication — Part 4: Mechanisms using a cryptographic check function

1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms using a cryptographic check function. Two mechanisms are concerned with the authentication of a single entity (unilateral authentication), while the remaining are mechanisms for mutual authentication of two entities.

The mechanisms specified in this part of ISO/IEC 9798 use time variant parameters such as time stamps, sequence numbers, or random numbers, to prevent valid authentication information from being accepted at a later time or more than once.

If a time stamp or sequence number is used, one pass is needed for unilateral authentication, while two passes are needed to achieve mutual authentication. If a challenge and response method employing random numbers is used, two passes are needed for unilateral authentication, while three passes are required to achieve mutual authentication.

Examples of cryptographic check functions are given in ISO/IEC 9797.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9798. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/IEC 9798 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 9797 (all parts), *Information technology — Security techniques — Message Authentication Codes (MACs).*

ISO/IEC 9798-1:1997, *Information technology — Security techniques — Entity authentication — Part 1: General*.

3 Definitions and notation

For the purposes of this part of ISO/IEC 9798, the definitions and notation described in ISO/IEC 9798-1 apply.

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 cryptographic check function as part of one of the mechanisms specified in this part of ISO/IEC 9798, 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 [1].

4 Requirements

In the authentication mechanisms specified in this part of ISO/IEC 9798 an entity to be authenticated corroborates its identity by demonstrating its knowledge of a secret authentication key. This is achieved by the entity using its secret key with a cryptographic check function applied to specific data to obtain a cryptographic check value. The cryptographic check value can be checked by anyone sharing the entity's secret authentication key, who can re-calculate the cryptographic check value and compare it with the value received.

The authentication mechanisms have the following requirements. If any one of these is not met then the authentication process may be compromised or it cannot be implemented.

a) A claimant authenticating itself to a verifier shares a common secret authentication key with that verifier. This key shall be known to the involved parties prior to the commencement of any particular run of an authentication mechanism. The method by which the key is distributed to the entities is beyond the scope of this part of ISO/IEC 9798.

b) The secret authentication key shared by a claimant and a verifier shall be known only to those two entities and, possibly, to other parties they both trust.

c) The strength of the mechanisms is dependent on the length and the secrecy of the key, on the nature of the cryptographic check functions, and on the length of the check value. These parameters shall be chosen to meet the required security level, as may be specified by the security policy.

d) The secret authentication key used in implementations of any of the mechanisms specified in this part of ISO/IEC 9798 shall be distinct from the keys used for any other purposes.

e) The cryptographic check values used at various places in an authentication mechanism shall not be interchangeable.

NOTE This could be enforced by including the following elements in the data string used to compute each cryptographic check value:

- The object identifier as specified in Annex B, in particular identifying the ISO standard, the part number, and the authentication mechanism.
- A constant that uniquely identifies the cryptographic check value within the mechanism. This constant may be omitted in mechanisms that include only one cryptographic check value.

The recipient of a cryptographic check value shall verify that the object identifier and the constant identifying the cryptographic check value are as expected.

5 Mechanisms

In these authentication mechanisms the entities A and B shall share a common secret authentication key K_{AB} or two unidirectional secret keys K_{AB} and K_{BA} prior to the commencement of any particular run of the authentication mechanisms. In the latter case, the unidirectional keys K_{AB} and K_{BA} are used respectively for the authentication of A by B and of B by A.

The mechanisms require the use of time variant parameters such as time stamps, sequence numbers or random numbers. The properties of the time variant parameters are important for the security of these mechanisms. In particular, the parameters shall be chosen so that it shall be most unlikely for them to repeat within the lifetime of an authentication key. For additional information see annex B of ISO/IEC 9798-1.

The use of the text fields specified in the following mechanisms is outside the scope of this part of ISO/IEC 9798 (they may be empty), and will depend upon the specific application. See annex A for information on the use of text fields.

A text field may only be included in the input to the cryptographic check function if the verifier can determine it independently, e.g., if it is known in advance, sent in clear or can be derived from one or both of those sources.

5.1 Unilateral authentication

Unilateral authentication means that only one of the two entities is authenticated by use of the mechanism.

5.1.1 One pass authentication

In this authentication mechanism the claimant A initiates the process and is authenticated by the verifier B. Uniqueness/timeliness is controlled by generating and checking a time stamp or a sequence number (see annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 1.

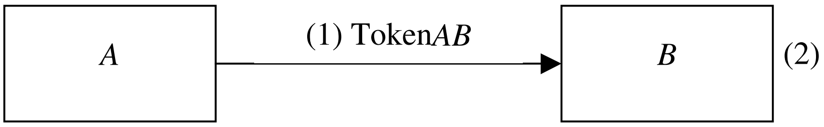

Figure 1

The form of the token (TokenAB), sent by the claimant A to the verifier B is:

$$\mathrm{Token}AB = \begin{matrix} T_A \\ N_A \end{matrix} \parallel \mathrm{Text2} \parallel f_{K_{AB}}(\begin{matrix} T_A \\ N_A \end{matrix} \parallel B \parallel \mathrm{Text1})$$

where the claimant A uses either a sequence number N_A or a time stamp T_A as the time variant parameter. The choice depends on the technical capabilities of the claimant and the verifier as well as on the environment. As defined in ISO/IEC 9798-1, $f_K(X)$ denotes the cryptographic check value computed by applying the cryptographic check function f to the data X using the key K.

The inclusion of the distinguishing identifier B in TokenAB is optional.

NOTE Distinguishing identifier B is included in TokenAB to prevent the re-use of TokenAB on entity A by an adversary masquerading as entity B. Its inclusion is made optional so that, in environments where such attacks cannot occur, it may be omitted.

The distinguishing identifier B may also be omitted if a unidirectional key is used.

(1) A generates and sends TokenAB to B.

(2) On receipt of the message containing TokenAB, B verifies TokenAB by checking the time stamp or the sequence number, calculating

$$f_{K_{AB}}(\begin{matrix} T_A \\ N_A \end{matrix} \parallel B \parallel \mathrm{Text1})$$

and comparing it with the cryptographic check value of the token, thereby verifying the correctness of the distinguishing identifier B, if present, as well as the time stamp or the sequence number.

5.1.2 Two pass authentication

In this authentication mechanism the claimant A is authenticated by the verifier B who initiates the process. Uniqueness/timeliness is controlled by generating and checking a random number R_B (see annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 2.

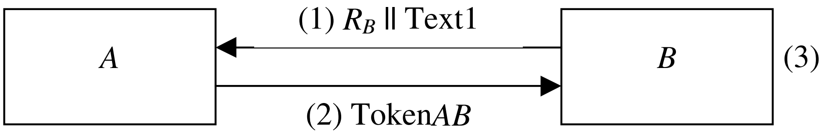

Figure 2

The form of the token (TokenAB), sent by the claimant A to the verifier B is:

$$\mathrm{Token}AB = \mathrm{Text3} \parallel f_{K_{AB}}(R_B \parallel B \parallel \mathrm{Text2}) .$$

The inclusion of the distinguishing identifier B in TokenAB is optional.

NOTE Distinguishing identifier B is included in TokenAB to prevent a so-called reflection attack. Such an attack is characterised by the fact that an intruder 'reflects' the challenge R_B to B pretending to be A. The inclusion of the distinguishing identifier B is made optional so that, in environments where such attacks cannot occur, it may be omitted.

The distinguishing identifier B may also be omitted if a unidirectional key is used.

(1) B generates a random number R_B and sends it and, optionally, a text field Text1 to A.

(2) A generates and sends TokenAB to B.

(3) On receipt of the message containing TokenAB, B verifies TokenAB by calculating

$$f_{K_{AB}}(R_B \,||\, B \,||\, \mathrm{Text2})$$

and comparing it with the cryptographic check value of the token, thereby verifying the correctness of the distinguishing identifier B, if present, and that the random number R_B, sent to A in step (1), was used in constructing TokenAB.

5.2 Mutual authentication

Mutual authentication means that the two communicating entities are authenticated to each other by use of the mechanism.

The two mechanisms described in 5.1.1 and 5.1.2 are adapted in 5.2.1 and 5.2.2, respectively, to achieve mutual authentication. In both cases this requires one more pass and results in two more steps.

NOTE A third mechanism for mutual authentication can be constructed from two instances of the mechanism specified in 5.1.2, one started by entity A and the other by entity B.

5.2.1 Two pass authentication

In this authentication mechanism uniqueness/timeliness is controlled by generating and checking time stamps or sequence numbers (see annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 3.

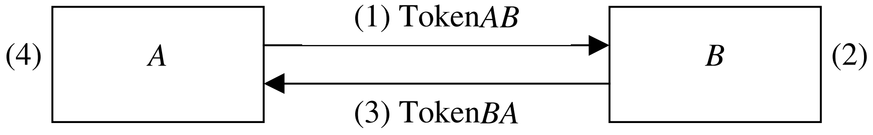

Figure 3

The form of the token (TokenAB), sent by A to B, is identical to that specified in 5.1.1.

$$\mathrm{Token}AB = \begin{matrix} T_A \\ N_A \end{matrix} \,||\, \mathrm{Text2} \,||\, f_{K_{AB}}(\begin{matrix} T_A \\ N_A \end{matrix} \,||\, B \,||\, \mathrm{Text1}).$$

The form of the token (TokenBA), sent by B to A, is:

$$\mathrm{Token}BA = \begin{matrix} T_B \\ N_B \end{matrix} \,||\, \mathrm{Text4} \,||\, f_{K_{AB}}(\begin{matrix} T_B \\ N_B \end{matrix} \,||\, A \,||\, \mathrm{Text3}).$$

The inclusion of the distinguishing identifier B in TokenAB and the inclusion of the distinguishing identifier A in TokenBA are (independently) optional.

NOTE 1 Distinguishing identifier B is included in TokenAB to prevent the re-use of TokenAB on entity A by an adversary masquerading as entity B. For similar reasons the distinguishing identifier A is present in TokenBA. Their inclusion is made optional so that, in environments where such attacks cannot occur, one or both may be omitted.

The distinguishing identifiers A and B may also be omitted if unidirectional keys (see below) are used.

The choice of using either time stamps or sequence numbers in this mechanism depends on the capabilities of the claimant and the verifier as well as on the environment.

Steps (1) and (2) are identical to those specified in 5.1.1, one pass authentication.

(3) B generates and sends TokenBA to A.

(4) The message in step (3) is handled in a manner analogous to step (2) of 5.1.1.

NOTE 2 The two messages of this mechanism are not bound together in any way, other than implicitly by timeliness; the mechanism involves independent use of mechanism 5.1.1 twice. Further binding together of these messages can be achieved by making appropriate use of the text fields (see annex A).

If unidirectional keys are used then the key K_{AB} in TokenBA is replaced by the unidirectional key K_{BA} and the appropriate key is used in step (4).

5.2.2 Three pass authentication

In this authentication mechanism uniqueness/timeliness is controlled by generating and checking random numbers (see annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 4.

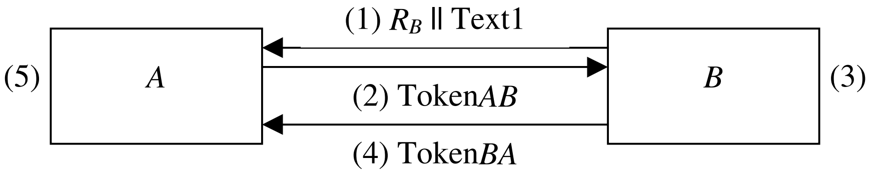

Figure 4

The tokens are of the following form:

$$\text{Token}AB = R_A \,\|\, \text{Text3} \,\|\, f_{K_{AB}}(R_A \,\|\, R_B \,\|\, B \,\|\, \text{Text2}),$$

$$\text{Token}BA = \text{Text5} \,\|\, f_{K_{AB}}(R_B \,\|\, R_A \,\|\, \text{Text4}).$$

The inclusion of the distinguishing identifier B in TokenAB is optional.

NOTE When present, distinguishing identifier B is included in TokenAB to prevent a so-called reflection attack. Such an attack is characterised by the fact that an intruder 'reflects' the challenge R_B to B pretending to be A. The inclusion of the distinguishing identifier B is made optional so that, in environments where such attacks cannot occur, it may be omitted.

The distinguishing identifier B may also be omitted if unidirectional keys (see below) are used.

(1) B generates a random number R_B and sends it and, optionally, a text field Text1 to A.

(2) A generates a random number R_A, and generates and sends TokenAB to B.

(3) On receipt of the message containing TokenAB, B verifies TokenAB by calculating

$$f_{K_{AB}}(R_A \parallel R_B \parallel B \parallel \mathrm{Text2})$$

and comparing it with the cryptographic check value of the token, thereby verifying the correctness of the distinguishing identifier B, if present, and that the random number R_B, sent to A in step (1), was used in constructing TokenAB.

(4) B generates and sends TokenBA to A.

(5) On receipt of the message containing TokenBA, A verifies TokenBA by calculating

$$f_{K_{AB}}(R_B \parallel R_A \parallel \mathrm{Text4})$$

and comparing it with the cryptographic check value of the token, thereby verifying that the random number R_B, received from B in step (1), was used in constructing TokenBA and that the random number R_A, sent to B in step (2), was used in constructing TokenBA.

If unidirectional keys are used then the key K_{AB} in TokenBA is replaced by the unidirectional key K_{BA} and the appropriate key is used in step (5).

Annex A
(informative)

Use of text fields

The tokens specified in clause 5 of this part of ISO/IEC 9798 contain text fields. The actual use of and the relationships between the various text fields in a given pass depend on the application.

For example, through its inclusion in an appropriate text field, e.g. Text1 of Token*AB* in clause 5.1.1, information can be used in the calculation of the cryptographic check value of the token. By this means, data origin authentication can be provided for this information.

See Annex A of ISO/IEC 9798-1 for further examples of the use of text fields.

Annex B
(normative)

Object Identifiers

This annex lists the object identifiers assigned to mechanisms specified in this part of ISO/IEC 9798.

```
EntityAuthenticationMechanisms-4   {iso(1)   standard(0)   e-auth-mechanisms(9798)
                                   part4(4) asn1-module(0) object-identifiers(0)}

DEFINITIONS EXPLICIT TAGS ::= BEGIN

-- EXPORTS All; --

-- IMPORTS None; --

OID ::= OBJECT IDENTIFIER -- alias

-- Synonyms --

is9798-4 OID ::= {iso(1) standard(0) e-auth-mechanisms(9798) part4(4)}

mechanism OID ::= {is9798-4 mechanisms(1)}

-- unilateral authentication mechanisms --

ua-one-pass OID ::= {mechanism ua-One-pass(1)}
ua-two-pass OID ::= {mechanism ua-Two-pass(2)}

-- mutual authentication mechanisms --

ma-two-pass OID ::= {mechanism ma-Two-pass(3)}

ma-three-pass OID ::= {mechanism ma-Three-pass(4)}

END -- EntityAuthenticationMechanisms-4 --
```

Bibliography

[1] ISO/IEC 8825-1, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ICS 35.040

Price based on 7 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™