INTERNATIONAL STANDARD

**ISO/IEC 9798-2**

Fourth edition
2019-06

# IT Security techniques — Entity authentication —

## Part 2: Mechanisms using authenticated encryption

*Techniques de sécurité IT — Authentification d'entité —*

*Partie 2: Mécanismes utilisant le chiffrement authentifié*

Reference number
ISO/IEC 9798-2:2019(E)

© ISO/IEC 2019



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

# Contents

Page

**Foreword** ... **iv**

**1 Scope** ... **1**

**2 Normative references** ... **1**

**3 Terms and definitions** ... **1**

**4 Symbols and abbreviated terms** ... **2**

**5 General** ... **3**

**6 Requirements** ... **3**

**7 Mechanisms not involving an on-line trusted third party** ... **4**
7.1 General ... 4
7.2 Unilateral authentication ... 4
7.2.1 General ... 4
7.2.2 Mechanism UNI.TS — One-pass authentication ... 5
7.2.3 Mechanism UNI.CR — Two-pass authentication ... 5
7.3 Mutual authentication ... 6
7.3.1 General ... 6
7.3.2 Mechanism MUT.TS — Two-pass authentication ... 6
7.3.3 Mechanism MUT.CR — Three-pass authentication ... 7

**8 Mechanisms involving an on-line trusted third party** ... **8**
8.1 General ... 8
8.2 Mechanism TP.TS — Four-pass authentication ... 8
8.3 Mechanism TP.CR — Five-pass authentication ... 10

**Annex A** (normative) **Object Identifiers** ... **12**

**Annex B** (informative) **Use of text fields** ... **13**

**Annex C** (informative) **Properties of entity authentication mechanisms** ... **14**

**Bibliography** ... **15**

© ISO/IEC 2019 – 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology,* Subcommittee SC 27, *IT Security techniques*.

This fourth edition cancels and replaces the third edition (ISO/IEC 9798-2:2008), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 9798-2:2008/Cor.1:2010, ISO/IEC 9798-2:2008/Cor.2:2012 and ISO/IEC 9798-2:2008/Cor.3:2013. The main changes compared to the previous edition are as follows:

— replacement of encryption by authenticated encryption;

— inclusion of constants uniquely identifying the mechanism and the instance of authenticated encryption within the mechanism.

A list of all parts in the ISO/IEC 9798 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

 © ISO/IEC 2019 – All rights reserved

# IT Security techniques — Entity authentication —

# Part 2:
# Mechanisms using authenticated encryption

## 1 Scope

This document specifies entity authentication mechanisms using authenticated encryption algorithms. Four of the mechanisms provide entity authentication between two entities where no trusted third party is involved; two of these are mechanisms to unilaterally authenticate one entity to another, while the other two are mechanisms for mutual authentication of two entities. The remaining mechanisms require an on-line trusted third party for the establishment of a common secret key. They also realize mutual or unilateral entity authentication.

Annex A defines Object Identifiers for the mechanisms specified in this document.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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, *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.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

**3.1**
**authenticated encryption**
(reversible) transformation of data by a cryptographic algorithm to produce *ciphertext* (3.2) that cannot be altered by an unauthorized entity without detection, i.e. it provides data confidentiality, data integrity, and data origin authentication

[SOURCE: ISO/IEC 19772:2009, 3.1]

**3.2**
**ciphertext**
data which has been transformed to hide its information content

[SOURCE: ISO/IEC 10116:2017, 3.2]

**3.3**
**claimant**
entity that is, or represents, a principal for the purposes of authentication

© ISO/IEC 2019 – All rights reserved

**3.4**
**time stamp**
time variant parameter which denotes a point in time with respect to a common time reference

[SOURCE: ISO/IEC 18014-1:2008, 3.12]

**3.5**
**trusted third party**
**TTP**
security authority, or its agent, trusted by other entities with respect to security related activities

[SOURCE: ISO/IEC 18014-1:2008, 3.20]

## 4 Symbols and abbreviated terms

| | |
|---|---|
| *A, B* | Labels used for the entities participating in a mechanism. |
| $d_K$ | An authenticated decryption process using secret key *K.* |
| $e_K$ | An authenticated encryption process performed using secret key *K.* |
| $e_K(X)$ | The result of the encryption process for data *X* with an authenticated encryption algorithm using a key *K*. |
| $I_U$ | A distinguishing identifier of entity *U*. |
| *K* | A secret key used with the encryption and decryption processes. |
| $K_{UV}$ | A secret key shared between entities *U* and *V* used only in authenticated encryption techniques. |
| $N_U$ | A sequence number issued by entity *U*. |
| *P* | A symbol used to represent the trusted third party. |
| $R_U$ | A random number issued by entity *U*. |
| $SID^i_{\mathrm{m}}$ | Constant uniquely identifying the mechanism m and the instance of authenticated encryption (number *i*) within the mechanism. |
| $TN_U$ | A time variant parameter originated by entity *U* which is either a time stamp $T_U$ or a sequence number $N_U$. |
| $Token_{UV}$ | A token sent from entity *U* to entity *V*. |
| $T_U$ | A time stamp issued by entity *U*. |
| $TVP_U$ | A time variant parameter originated by entity *U* which is a time stamp $T_U$, a sequence number $N_U$ or a random number $R_U$. |
| $X \mid\mid Y$ | 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 encrypted 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. |

NOTE This latter property can be achieved in a variety of ways, depending on the application. For example, it can 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[2].


© ISO/IEC 2019 – All rights reserved