BS ISO/IEC 9798-3:2019

BSI Standards Publication

IT Security techniques — Entity authentication

Part 3: Mechanisms using digital signature techniques

bsi.

National foreword

This British Standard is the UK implementation of ISO/IEC 9798-3:2019. It supersedes BS ISO/IEC 9798-3:1998+A1:2010, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/2, Cryptography and Security Mechanisms.

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.

Published by BSI Standards Limited 2019

ISBN 978 0 580 94987 6

ICS 35.030

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 January 2019.

Amendments/corrigenda issued since publication

Date	Text affected

BS ISO/IEC 9798-3:2019

INTERNATIONAL STANDARD

ISO/IEC 9798-3

Third edition
2019-01

IT Security techniques — Entity authentication —

Part 3: Mechanisms using digital signature techniques

Techniques de sécurité IT — Authentification d'entité —

Partie 3: Mécanismes utilisant des techniques de signature numériques

Reference number
ISO/IEC 9798-3:2019(E)

COPYRIGHT PROTECTED DOCUMENT

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

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.

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).

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 Joint Technical Committee JTC 1, *Information Technology*, Subcommittee SC 27, *IT Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC 9798–3:1998), which has been technically revised. It also incorporates the amendment ISO/IEC 9798–3:1998/Amd 1:2010, and corrigenda ISO/IEC 9798–3:1998/Cor 1:2009 and ISO/IEC 9798–3:1998/Cor 2:2012. The main changes compared to the previous edition are as follows:

— all mechanisms have been technically revised to resolve security issues and make the mechanism secure by default;

— all mechanisms have been renamed and editorially improved to represent them more clearly;

— three additional mechanisms have been included using an on-line trusted third party;

— guidance to explain the security properties of the mechanisms and guide users in selecting the appropriate mechanism for their use case has been added (Annex B).

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.

INTERNATIONAL STANDARD **ISO/IEC 9798-3:2019(E)**

IT Security techniques — Entity authentication —

Part 3:
Mechanisms using digital signature techniques

1 Scope

This document specifies entity authentication mechanisms using digital signatures based on asymmetric techniques. A digital signature is used to verify the identity of an entity.

Ten mechanisms are specified in this document. The first five mechanisms do not involve an on-line trusted third party and the last five make use of on-line trusted third parties. In both of these two categories, two mechanisms achieve unilateral authentication and the remaining three achieve mutual authentication.

Annex A defines the object identifiers assigned to the entity authentication 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*

ISO/IEC 14888 (all parts), *Information technology — Security techniques — Digital signatures with appendix*

ISO/IEC 9796 (all parts), *Information technology — Security techniques — Digital signature schemes giving message recovery.*

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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
atomic transaction
transaction which cannot be split into multiple smaller transactions

3.2
claimant
entity which is or represents a principal for the purposes of authentication

[SOURCE: ISO/IEC 9798–1:2010, 3.6, modified — The Note to entry has been removed.]