INTERNATIONAL STANDARD

ISO/IEC 20009-3

First edition
2022-02

Information security — Anonymous entity authentication —

Part 3: Mechanisms based on blind signatures

Sécurité de l'information — Authentification d'entité anonyme —

Partie 3: Mécanismes fondés sur des signatures aveugles

Reference number
ISO/IEC 20009-3:2022(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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.

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 or www.iec.ch/members_experts/refdocs).

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 https://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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 20009 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

Introduction

In an anonymous entity authentication mechanism, the entity to be authenticated (the claimant) provides evidence to a verifier that it has knowledge of a secret without revealing its identifier to any unauthorized entity. That is, given complete knowledge of the messages exchanged between the parties, an unauthorized entity cannot discover the identifier of the entity being authenticated. Moreover, it is possible that even an authorized verifier is not authorized to learn the identifier of the entity being authenticated.

The anonymous entity authentication mechanisms specified in this document are based on blind signatures, specified in the ISO/IEC 18370 series.

Information security — Anonymous entity authentication —

Part 3: Mechanisms based on blind signatures

1 Scope

This document provides general descriptions and specifications of anonymous entity authentication mechanisms based on blind digital signatures.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

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

3.1
anonymous entity authentication
corroboration that an entity possesses certain *attributes* (3.2), without distinguishing this entity from other entities with the same attributes

[SOURCE: ISO/IEC 20009-1:2013, 2.2]

3.2
attribute
application-specific data element

[SOURCE: ISO/IEC 18370-1:2016, 3.1]

3.3
claimant
entity which is or represents a principal for the purposes of authentication

Note 1 to entry: A claimant includes the functions and the private data necessary for engaging in authentication exchanges on behalf of a principal.

[SOURCE: ISO/IEC 9798-1:2010, 3.6]

3.4
claimant information field
special *credential* (3.6) *attribute* (3.2) encoded within a credential that is not seen by the *issuer* (3.13) during credential issuance, and that is always disclosed to a *verifier* (3.15)