INTERNATIONAL STANDARD

ISO/IEC 27551

First edition
2021-09

Information security, cybersecurity and privacy protection — Requirements for attribute-based unlinkable entity authentication

Sécurité de l'information, cybersécurité et protection de la vie privée — Exigences relatives à l'authentification des entités non rattachables par des attributs

Reference number
ISO/IEC 27551:2021(E)

© ISO/IEC 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

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
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols and abbreviated terms ... **2**
5 General objectives of attribute-based entity authentication ... **2**
6 Properties of attribute-based entity authentication protocols ... **4**
6.1 Correctness ... 4
6.2 Unforgeability ... 4
6.2.1 General ... 4
6.2.2 Replay protections ... 4
7 Unlinkability properties of attribute-based entity authentication protocols ... **4**
7.1 General ... 4
7.2 Generic definition of unlinkability ... 5
7.3 Specific definitions of unlinkability ... 5
7.3.1 General ... 5
7.3.2 Passive outsider unlinkability (anti-tracking from passive outsiders) ... 7
7.3.3 Active outsider unlinkability (anti-tracking from active outsiders) ... 7
7.3.4 RP-U unlinkability ("anonymous visits" to an RP) ... 7
7.3.5 AP-U unlinkability ... 8
7.3.6 RP+AP-U unlinkability (anti-RP-AP-collusion) ... 8
7.3.7 AP-RP unlinkability (anti-tracking of RP from AP) ... 8
7.3.8 AP-RP+U unlinkability ... 8
7.3.9 RP+RP'-U unlinkability (anti-tracking of U from a set of colluding RPs) ... 8
7.4 Relationships between notions of unlinkability ... 9
7.5 Unlinkability levels for attribute-based entity authentication ... 9
7.6 Models ... 10
8 Attributes ... **10**
8.1 Categories of attributes ... 10
8.1.1 Personal attributes ... 10
8.1.2 Self-claimed attributes ... 10
8.1.3 Verified attributes ... 10
8.1.4 Static attributes ... 11
8.1.5 Semi-static attributes ... 11
8.1.6 Dynamic attributes ... 11
8.1.7 Computed attributes ... 11
8.1.8 Identifying attributes ... 11
8.1.9 Supporting attributes ... 11
8.2 Verified attribute expiry and revocation ... 11
8.3 Attribute assurance ... 11
9 Requirements for level N attribute-based unlinkable entity authentication ... **11**
Annex A (informative) **Formal definitions for security and unlinkability notions** ... **13**
Annex B (informative) **Examples of attribute-based entity authentication protocols** ... **19**
Annex C (informative) ... **26**
Annex D (informative) **Use cases for attribute-based unlinkable entity authentication** ... **33**
Bibliography ... **34**

© ISO/IEC 2021 – 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 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 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*.

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.

© ISO/IEC 2021 – All rights reserved

Introduction

ISO/IEC 29100 sets forth eleven privacy principles which apply to all actors that can be involved in the processing of PII. The second principle is the collection limitation. Despite this recommendation, the current state of the art is that internet sites collect more than necessary information during the PII principal's access to the service. For example, if the site only requires verification that the PII principal is over a certain age, only that information should be necessary for the consumption of the service. However, it is often the case that other information such as the user's persistent identifier is supplied, making it possible to link visits from the same PII principal to different sites or to link two or more visits from the same PII principal to the same site.

To adhere to the principle of the collection limitation, the site in the above case should instead use a type of entity identifier that does not allow the site to link two or more visits by the PII principal. This means that, when two transactions are performed, it is difficult to distinguish whether the transactions were performed by the same user or by two different users. This is one type of unlinkability. Several other types of unlinkability can also be considered and desired in applications.

Attribute-based unlinkable entity authentication (ABUEA) provides a means for PII principals to establish the authenticity of a selected subset of their identity attributes without revealing a larger subset. Special focus is put on unlinkability and a metric that measures the strength of this property in implementations of ABUEA is introduced. This document focuses on cases where at least one attribute is attested by a third party. This document also identifies security properties to be met to achieve various protections as well as unlinkable properties.

The methodology developed by this document may be tailored and applied to other privacy principles. The requirements identified in this document apply at the application communication layer. However, some properties met at the application layer protocol can be ruined by a lower layer protocol, such as the network layer, which means that the lower layers' privacy and security properties should also be taken into consideration to ensure that the properties met at the application communication layer are still valid when considering the privacy and security characteristics of the lower communication layers.

© ISO/IEC 2021 – All rights reserved

Information security, cybersecurity and privacy protection — Requirements for attribute-based unlinkable entity authentication

1 Scope

This document provides a framework and establishes requirements for attribute-based unlinkable entity authentication (ABUEA).

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 24760-1, *IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts*

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 29100, ISO/IEC 24760-1, and the following 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
anonymity set
set of identities that shares certain characteristics

3.2
attribute provider
authority trusted by one or more users and one or more relying parties to issue or verify attributes related to an entity

3.3
significantly
not vanishing faster than any inverse polynomial in the security parameter

3.4
user-agent
software and/or hardware used by the PII Principal to interact with the system

© ISO/IEC 2021 – All rights reserved