FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
27551**

ISO/IEC JTC **1**/SC **27**

Secretariat: DIN

Voting begins on:
2021-06-09

Voting terminates on:
2021-08-04

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

Reference number
ISO/IEC FDIS 27551:2021(E)

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 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.

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.

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 29100, *Information technology — Security techniques — Privacy framework*

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

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 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 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

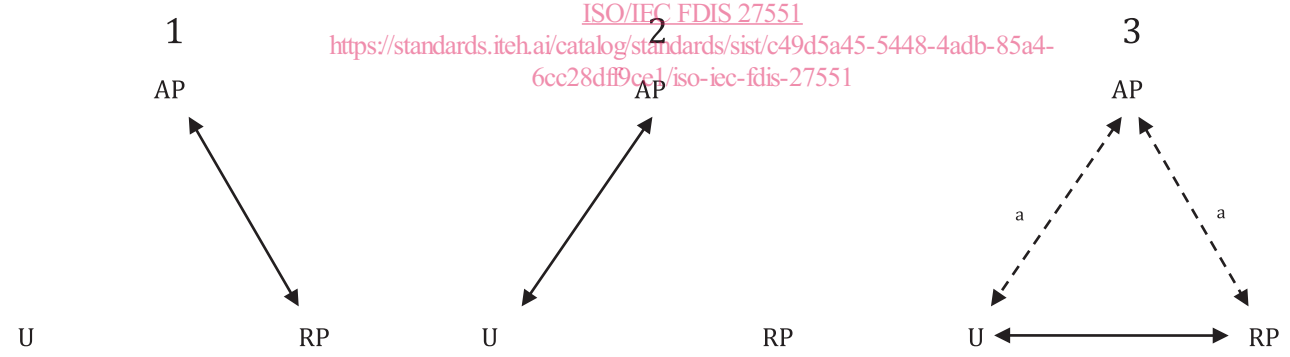
4 Symbols and abbreviated terms

A	adversary
AO	active outsider
AP	attribute provider
OIDC	OpenID Connect
PII	personally identifiable information
PO	passive outsider
RP	relying party
SIOP	self-issued OpenID provider
U	user-agent
UL	unlinkability level

5 General objectives of attribute-based entity authentication

Attribute-based entity authentication is a means to establish a form of trust between two unfamiliar parties that share trust in a common third-party entity.

This clause defines the notion of attribute-based entity authentication in a minimal communication three parties model involving three entity roles U, RP and AP as depicted in Figure 1.



Key

1 setup phase (optional)
2 user registration phase
3 authentication phase
[a] Optional.

Figure 1 — Phases of attribute-based entity authentication

RP trusts AP in the sense that RP is convinced of the correctness of statements expressed by AP. RP and AP can have engaged in some optional preliminary procedure, referred to as the setup phase, which enables the RP to ascertain that statements expressed by AP are genuine.

A PII principal, referred to as a user hereafter, uses a software called user-agent or U to communicate with AP and RP. U has a number of attributes which collectively represent its distinct identity. U and AP can also have carried out a preliminary procedure referred to as the user registration phase, in which AP validates the user's attributes and links them to U's attributes. During this process, U can be given data material to enable later attribute-based entity authentication towards RP.

There is no such preliminary procedure between U and RP, meaning that U and RP are a priori strangers to one another.

An attribute-based entity authentication protocol is a sequence of computations and communications among U, RP and AP which, when conducted successfully throughout, results in a state at RP where RP is convinced that a statement made by U about its attributes is correct or not. The purpose of the protocol is to reach that state.

The authentication phase is the protocol stage where U and RP interact, which can involve the participation of AP or not.

The description of a particular attribute-based entity authentication protocol requires a specification of the attributes, of the statements that can be made on them, as well as of all computations and communications between the three parties. It includes a description of the authentication phase, the setup phase if any, and the user registration phase if any.

NOTE Attribute-based entity authentication can also be achieved in communication models that extend beyond the minimal U-RP-AP model either by involving additional specific-purpose entities or by limiting the use of communication channels at determined stages of the protocol. Annex B describes some examples of attribute-based entity authentication protocols and their underlying model.

Attributes are defined in ISO/IEC 24760-1. As properties, they can have:

— a **type**, a Boolean, or a character string of alphabetical characters, or an integer in a certain range, or a compound type built on these basic types (such as a fixed length vector of integers or a dynamic list of mixed strings and integers, and so forth);

— a name, which is a string in a prescribed alphabet;

— a value selected within the range of admissible values for the considered type.

Other properties of attributes such as their origin or level of assurance, or more generally classes or categories of sorts, can exist and be involved in the attribute-based authentication protocol. However, they are usually encoded as additional attributes. Therefore, it is enough to rely on the notions of type, name and value when describing an attribute.

A policy decision function is a function that takes a policy and other information for the purpose of returning a boolean value. It is defined as a logic predicate combining basic relational expressions using logic operators such as OR, AND or possibly more complex ones such as threshold gates (t-out-of-n). A relational expression can express:

— equality of an attribute value to a particular value;

— non-equality of an attribute value to a particular value;

— inequality of an attribute value towards a particular value (less than, greater than). This requires that the attribute type support an ordering over its set of admissible values.

It is usual to rely on a structured language to express policies when some level of genericity is desired. OASIS eXtensible Access Control Markup Language (XACML) is one such example. In other applications, the policy may be fixed and hard-coded into the attribute-based entity authentication protocol itself.

It should also be noted that some attribute-based entity authentication protocols may only support restricted policies, where:

— attribute values can only be compared to constants and not to other attribute values;

— the nature or the number of logic operators is limited; or

— some other restriction applies.

The purpose of an attribute-based entity authentication protocol is for RP to be convinced that the set of attributes A_U temporarily associated to an a-priori unknown entity U satisfies a certain policy P,

namely that the policy decision function returns true for $P(A_U)$. For attributes that originate from a neutral AP that the RP trusts, some form of interaction with that AP is necessary.

Annex D describes examples of use cases in which ABUEA systems are used.

6 Properties of attribute-based entity authentication protocols

6.1 Correctness

Under the assumptions that:

— RP is always convinced by the statements expressed by AP;

— All parties U, AP and RP engage in the correct execution of the protocol;

the protocol is correct when, if the user has a set of attributes A_U and A_U satisfies the policy P, then the protocol terminates in an acceptance state by the RP, meaning that RP acknowledges that $P(A_U)$ = true.

6.2 Unforgeability

6.2.1 General

Unforgeability is a security property that exists for attribute-based entity authentication protocols.

The protocol is unforgeable if it is infeasible for U to make RP terminate the protocol in the acceptance state when $P(A_U)$ =false.

Clause A.2 describes the conditions of achieving unforgeability.

6.2.2 Replay protections

Unforgeability requires two security measures to be taken into consideration for any kind of entity authentication protocol, namely:

— replay protection against one relying party; and

— replay protection against different relying parties.

The first kind of protection requires the use of a time-variant parameter that can either be a challenge sent by the relying party and then reused by the U or be a unique number presented by the U to the SP. These time-variant parameters are part of the computation of the credentials presented by the U to the RP.

The second kind of protection requires the use in the protocol of a data item containing a characteristic unique to the intended relying party.

7 Unlinkability properties of attribute-based entity authentication protocols

7.1 General

In this document, unlinkability refers to a family of properties that an attribute-based entity authentication protocol can or cannot fulfil. The purpose of this clause is to provide a definition for these properties and show how they interrelate.

Note that these definitions are formulated for attribute-based entity authentication protocols operating in the minimal U-RP-AP model. They can give rise to distinct definitions in extended communication models.

7.2 Generic definition of unlinkability

Linking is defined as the ability for an entity or a group of colluding entities to distinguish protocol executions where:

— an entity role is played by the same entity; from

— that entity role is played by different entities.

Unlinkability refers to the inability to link protocol executions. The entity or group of entities attempting to link protocol executions is called the adversary while the entity role under observation is the target entity role. Considering different settings for the adversary and target entity role produces entirely different notions of unlinkability.

For example, if U visits an RP more than twice and if the RP can link these visits together to recognize the repeated visits, then the RP is linking the user visits. In this case, U is not “anonymous” but only “pseudonymous” at best and if U was wishing to be “anonymous”, then RP is acting as an adversary against the user’s wish. Similarly, when U is trying to authenticate itself to RP using attributes provided by AP, U may wish so that AP cannot find out to which RP U has provided those attributes. Under such circumstances, if AP identifies that U provided attributes to RP, then AP is acting as an adversary.

The protocol itself is said to be unlinkable if its executions cannot be linked, given explicit settings for the adversary and target entity role.

NOTE A clear distinction is to be made between the various unlinkability properties that a protocol can or cannot achieve and the traceability or linkability of data transfers at the data transport level. It is usual to assume that an anonymization tool such as TOR[2] can be used to avoid a trivial form of linking through network connections instead of the nature of the exchanged messages. This consideration is independent of the actual unlinkability properties that a protocol possess or not.

This document is concerned with achieving unlinkability of the protocol executions without external context (metadata). Even if a protocol is unlinkable, linking may be achieved with metadata (e.g. by considering the timings or location when authentication takes place). Techniques to prevent linking via metadata are out of scope for this document.

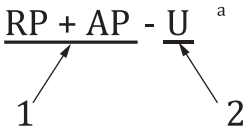
The level of anonymity also depends on the size of the anonymity set resulting from the combination of policy P and the set of user attributes A_U such that A_U satisfies the policy P. An example is a policy that asks for a user's year of birth but the user is over 100 years old. The resulting anonymity set can be very small.

7.3 Specific definitions of unlinkability

7.3.1 General

While the terms “unlinkable” or “anonymous” are often used, the meaning actually varies depending on the context of the use of the terms. To speak about them precisely, it is necessary to speak of from which adversary role, what target entity role is unlinkable.

This document adopts a naming convention for notions of unlikability where the adversarial role constitutes the first part of the name and the second part describes the target entity role. The two parts are separated by a “-”, as show in Figure 2.



Key

1 adversary

2 target entity

a Unlinkability.

Figure 2 — Naming convention for notions of unlinkability

This document provides the following notions of unlinkability for attribute-based entity authentication protocols, indicating this aspect together with “unlinkability”.

1) Passive outsider unlinkability (PO-U). The adversary plays none of the U, RP or AP roles but can passively observe the content of all exchanged messages. The target entity role is U.

2) Active outsider unlinkability (AO-U). The adversary plays none of the U, RP or AP roles but can observe, actively intercept and modify exchanged messages in a man-in-the-middle fashion. The target entity role is U.

3) RP-U unlinkability. The adversary can observe, actively intercept and modify exchanged messages and additionally plays the role of RP. The target entity role is U.

4) AP-U unlinkability. The adversary can observe, actively intercept and modify exchanged messages and additionally plays the role of AP. The target entity role is U.

5) RP+AP-U unlinkability. The adversary can observe, actively intercept and modify exchanged messages and additionally plays the role of both RP and AP. The target entity role is U.

6) AP-RP unlinkability. The adversary can observe, actively intercept and modify exchanged messages and additionally plays the role of AP. The target entity role is RP.

7) AP-RP+U unlinkability. The adversary can observe, actively intercept and modify exchanged messages and additionally plays the role of AP. The target entity roles are U and RP. This means that neither U nor RP can be linked.

8) RP+RP'-U unlinkability. The adversary can observe, actively intercept, and modify exchanged messages and additionally plays the roles of RP and RP'. The target entity role is U. In this case, unlinkability of U by RP is not in question. Here, a different type of linking is considered. That is, linking as the ability for RP and RP’ to distinguish:

   — two protocol executions between U and RP and U and RP’ from;

   — two protocol executions between U and RP and U’ and RP’.

Table 1 summarizes, for each notion of unlinkability, the settings for the adversary and target entity roles.

Table 1 — Relationship between adversarial and target roles and notions of unlinkability

Notion of unlinkability	Adversarial role(s)	Target role(s)	Explanations
Passive outsider (PO-U)	PO	U	Attempt to track U across authentications while these are being monitored (read-only).
Active outsider (AO-U)	AO	U	Attempt to track U across authentications while these are being controlled (read-write).
RP-U	RP	U	The RP attempts to track the U across authentications

Table 1 *(continued)*

Notion of unlinkability	Adversarial role(s)	Target role(s)	Explanations
AP-U	AP	U	The AP attempts to track the U across authentications.
RP+AP-U	RP and AP	U	The colluding RP and AP attempt to track U across authentications.
AP-RP	AP	RP	The AP attempts to track the RP across authentications.
AP-RP+U	AP	RP and U	The AP attempts to track U, RP, and the pair (U, RP) across authentications.
RP+RP'-U	RP and RP'	U	Colluding RPs attempt to track the U across authentications. RP may be able to track U in transaction with RP, but cannot track the same U communicating with RP'

For each of the roles controlled by the adversary, the adversary may arbitrarily deviate from the protocol specification in attempts to defeat the unlinkability.

It is common that after a successful authentication, a session is held between U and RP. The session management ensures that during the session, it is same U that is talking to RP, thus it is linkable within the session. In this document, the notion of unlinkability discussed is between the sessions and not within.

Annex A describes each of the unlinkability notions in more detail.

7.3.2 Passive outsider unlinkability (anti-tracking from passive outsiders)

An attribute-based authentication protocol is said to achieve passive outsider unlinkability if an adversary that is only allowed to observe the exchanges among U, AP and RP cannot link these observations to U. For example, when Alice, assuming the role of U, authenticates herself to RP via the help of the AP, if the adversary cannot link the run of the protocol to Alice, passive outsider unlinkability is satisfied.

Achieving this notion of unlinkability is not considered technically difficult. Usually, passive observations can be neutralised by careful use of encryption throughout the protocol.

7.3.3 Active outsider unlinkability (anti-tracking from active outsiders)

Unlike in the passive outsider unlinkability case, the adversary now can intercept the message exchanges among U, AP and RP and can potentially modify them. In other words, the adversary is an entity that remains external to all parties but has read-write access to the contents of the messages exchanged at each stage of the protocol. In particular, the adversary may carry out man-in-the-middle attacks while parties are interacting as per the protocol. The adversary attempts to link a protocol run to U and active outsider unlinkability is satisfied when it is shown that this is not possible.

Achieving this notion of active outsider unlinkability is not considered technically difficult. Active outsiders can be neutralized by carefully using the correct combination of existing encryption and authentication throughout the protocol.

7.3.4 RP-U unlinkability ("anonymous visits" to an RP)

This is a common notion of user anonymity towards RP. The RP cannot tell whether the user-agent U that arrived at the RP has visited it before. If RP-U unlinkability is not satisfied and RP can link visits made by the same user-agent, then U is not anonymous from the point of view of the RP but is only pseudonymous. RP-U unlinkability is satisfied when an adversary that assumes the role of RP and has also read-write access to all transmissions between U, RP and AP, cannot link U across authentications.