

COMMITTEE DRAFT		Reference number:	
ISO/IEC 1st CD 24760-3		ISO/IEC JTC 1/SC 27 N14152	
Date: 2014-07-21		Supersedes document SC 27 N13377	
THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.			
ISO/IEC JTC 1/SC 27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for comments by: 2014-10-21 Please submit your comments via the online balloting application by the due date indicated.		
ISO/IEC 1st CD 24760-3			
Title: Information technology -- Security techniques – A framework for identity management – Part 3: Practice			
Project: 1.27.50.03 (ISO/IEC 24760-3)			
Explanatory Report			
Status	SC 27 Decision	Reference documents	
		Input	Output
<i>For details regarding previous development stages please see the second page of the explanatory report.</i>			
ISO/IEC 24760-3 2nd WD	12 th WG 5 meeting, Oct. 2011, resolutions 1, 4, 10 (N10525).	NL com (N10352).	Advice f. editors (N10547); Liaison to SC 37 (N10528); DoC (N10554) N/A; Text f. 2 nd WD (N10568) N/A
	13 th WG 5 meeting, May 2012, resolutions 1, 2, 5, (N11280)		Text f. 2nd WD (N11241).
ISO/IEC 24760-3 3rd WD	14 th WG 5 meeting, Oct. 2012, resolutions 1,13, (N11701).	SoCom (N11542); Kantara liaison (N11552).	Liaison to Kantara (N11720) Formal ballot on limit dates extension (N11769); SoV on N11769 (N12070); Text f. 3rd WD (N11731)..
	15 th WG 5 meeting, April 2013, resolutions 1, 2, 5 (N12555).		Liaison to Kantara (N12520); DoC (N12533); Text f. 3rd WD (N12534).
ISO/IEC 24760-3 4th WD	16 th WG 5 meeting, Oct. 2013, resolutions 1, 2, 5 (N13373).	SoCom (N12818); Kantara com. (N12992); AT NB com. (N12997); KR NB contr. (N13004).	Editors' report (N13494); Liaison to Kantara (N13) DoC (N13372); Text f. 4 th WD (N13373).
ISO/IEC 24760-3 1st CD	17th WG 5 meeting, April 2014, resolutions 1, 5, P1, P2, (N14199); 26 th SC 27 Plenary, April 2014, Resolutions 1, 8 (N14200).	SoCom. (N13773); Kantara com. (N13797); JP NB contr. (N13833).	Liaison to Kantara (N14142); DoC (N14151); Text f. 1 st CD (14152).
1st CD Registration and Consideration In accordance with resolution 1 (see SC 27 N14200) of the 26th Plenary meeting held Hong Kong, China, 14th -15th April 2014, the hereby attached document has been registered with the ISO Central Secretariat (ITTF) as a 1st Committee Draft (CD) and is being circulated for a 1st CD letter ballot closing by <div style="text-align: center; font-size: 24pt; font-weight: bold;">2014-10-21</div>			
MEDIUM: http://isotc.iso.org/livelink/livelink/open/jtc1sc27 NO. OF PAGES: 2 + 41			

Explanatory Report (2 nd page)			
Status	SC 27 Decision	Reference documents	
		Input	Output
Recommendation on subdivision ISO/IEC 24760-3 1st WD	9 th WG 5 meeting, April 2010, resolutions 3, 5, 6, P1, P7, P8 (N8828rev).		Request/endorsement for /on Proposed modification to PoW (J1 N10170/N9404); Text f. 1 st WD (N8826) N/A.
	10 th WG 5 meeting, Oct. 2010, resolutions 1, 5, P9, (N9402).		Text f. 1 st WD (N9399) N/A
	11 th WG 5 meeting, Apr. 2011, resolutions 1, 4, P8, (N9920).		Text f. 1 st WD (N9399).

ISO/IEC JTC 1/SC 27 **N14152**

Date: 2014-07-15

ISO/IEC CD 24760-3.1

ISO/IEC JTC 1/SC 27/WG 5

Secretariat: DIN

Information technology — Security techniques — A framework for identity management — Part 3: Practice

Technologies de l'information — Techniques de sécurité — Gestion d'identité cadre — Partie 3:

Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

Secretariat, ISO/IEC JTC 1/SC27
DIN - Deutsches Institut fuer Normung e.V.
Burggrafenstrasse 6
DE-10772 Berlin
Germany

Telephone: + 49 2601-2652
Facsimile: + 49 2601-1723
E-mail: krystyna.passia@din.de
Web: www.jtc1sc27.din.de/en
<http://isotc.iso.org/isotcportal/index.html> (SC 27 documents)

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Contents	Page
Foreword	vi
Introduction	vii
1. Scope	1
2. Normative references	1
3. Terms and definitions	2
4. Symbols and abbreviated terms	2
5. Assurance in control of identity information use	3
5.1 Overview	3
5.2 Identity assurance	3
5.2.1 General	3
5.2.2 Risk Assessment	3
5.2.3 Identity proofing	3
5.2.4 Identity profile	4
6. Accessing identity information	5
6.1 Overview	5
6.2 Policy on accessing identity information	5
6.3 Access management	5
6.4 Identifiers	5
6.4.1 Personal identifiers	5
6.4.2 Device identifiers	6
6.4.3 Information object identifiers	6
6.4.4 Pseudonyms	6
7. Identity management and the authorization of using resources	7
7.1 Overview	7
7.2 Authorization of using resource	7
7.3 Account life cycle	7
7.4 Identity life cycle and accounts authorization life cycle	8
8. Tracing and monitoring identity information usage	10
9. Control objectives	11
9.1 Contextual components of a framework for identity management	11
9.1.1 Establishing a framework for identity management	11
9.1.2 Establishing identity	13
9.1.3 Managing identity information	14
9.2 Architectural components of a framework for identity management	15
9.2.1 Establishing an identity management system	15
9.2.2 Controlling an identity management system	16
Annex A (normative) Identity federation	18
A.1 General	18
A.2 Characteristics of trusted identity federations	19
A.3 Management and organisational considerations	20
A.4 Discovery	21
A.4.1 IIP Discovery	22
A.4.2 IIA Discovery	22
A.5 Considerations in inter-federation (federation of federation) scenarios	23
A.6 Threats and Controls	23
A.6.1 Requesting authenticated identity	23
A.6.2 Performing authentication	24
A.6.3 Authorizing the release of attributes	24
A.6.4 Returning the authenticated identity	25
A.6.5 Obtaining auxiliary attributes	25

A.6.6	Resource registration.....	25
A.7	Merging identity information authorities.....	25
Annex B (normative) Privacy-respecting identity management scheme using attribute-based		
	credentials	27
B.1	General.....	27
B.2	Actors.....	27
B.2.1	Principal.....	28
B.2.2	Relying party	28
B.2.3	Identity information provider	29
B.2.4	Identity Information Authority	29
B.3	Control steps	29
B.3.1	Credential issuance	29
B.3.2	Presentation	29
B.3.3	Invalidation	30
B.4	Architecture layers and components	30
B.4.1	Application deployment layer.....	31
B.4.2	Core components - proof generation/verification layer (ABCE).....	31
	Bibliography	33

Figures

Figure 1 – Account life cycle.....	8
Figure 2 – Entity' identity and associated authorizations life cycle	9
Figure 3 – Pair-wise Federation model	19
Figure 4 – Typical Federation model	19
Figure 5 – Federation Gateway model	20
Figure 6 – Federation basic discovery dialog example	23
Figure 7 – Actors of the ABC4Trust architecture and their interactions.....	28
Figure 8 – Main components of a principal's token and relying party equipment	30
Figure 9 – Architecture principal's token [1]	31

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 24760-2 has been prepared by the Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

It is common for computer systems to make automated decisions based on the *identity* of a person, piece of equipment or piece of software connected to it. Such decisions may control access to applications or other resources.

To address the need to efficiently and effectively implement systems that make identity based decisions this series of International Standards specify a framework for the issuance, administration, and use of data that serves to identify individuals, organizations and information technology components operating on behalf of individuals or organizations.

For many organizations the proper management of identity information is crucial to maintain security of the organizational processes. For individuals correct identity management is important to protect privacy.

ISO/IEC 24760 specifies fundamental concepts and operational structures of identity management with the purpose to realize information systems that can meet business, contractual, regulatory and legal obligations.

This International Standard recommends good practices for identity management.

ISO/IEC 24760 consists of the following parts:

- Part 1: Terminology and concepts
- Part 2: Reference architecture and requirements
- Part 3: Practice

ISO/IEC 24760 is also intended to provide foundations for other identity management related international standards including:

- ISO/IEC 29003 Identity Proofing,
- ISO/IEC 29100 Privacy framework,
- ISO/IEC 29101 Privacy Reference Architecture,
- ISO/IEC 29115 Entity Authentication Assurance Framework,
- ISO.IEC 29146 A framework for access management.

Information technology — Security techniques — A framework for identity management —

Part 3: Practice

1 Scope

This part of International Standard provides guidance for good practice for administrating identity management systems, and for ensuring that identity management systems meet the requirements stated in ISO24760 Part 1, Terminology and Concepts, and in ISO24760 Part 2, Reference Architecture and Requirements.

This International Standard is applicable to an information system where data relating to a digital identity are acquired, processed, stored, transferred or used according to the consent provided by the principal.

2 Normative references

The following referenced documents are indispensable for the application 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.

[Editor's note: to be reviewed]

ISO/IEC 10181:1996	<i>Information technology — Open Systems Interconnection — Security frameworks for open systems: Security audit and alarms framework</i>
ISO/IEC 18014 (all parts)	<i>Information technology — Security techniques — Time-stamping services — Part 1: Framework</i>
ISO/IEC 27002:2005	<i>Information technology — Security techniques — Code of practice for information security management</i>
ISO/IEC 29100:2011	<i>Information technology — Security techniques — Privacy framework.</i>
ISO/IEC 29101:2013	<i>Information technology — Security techniques — Privacy reference architecture</i>
ISO/IEC 29115:2013	<i>Information technology – Security techniques — Entity authentication assurance framework</i>
ISO/IEC 29146 –†	<i>Information technology — Security techniques — A framework for access management</i>
ISO/IEC 29003–†	<i>Information technology — Security techniques — Identity proofing</i>

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 24760-1 and the following apply.

[Editor's Note TBC]

0.1

federation operator

actor in a federation responsible to manage the issues arising from the operation of the federation.

NOTE: The role can be carried out by an existing federation member or and independent third party.

4 Symbols and abbreviated terms

[Editor's note: to be reviewed for actual use in the document]

ICT	Information and Communication Technology
IDM	Identity Management
IDMS	Identity Management System
IIP	identity information provider also IIP
IIA	Identity Information Authority
ISMS	Information Security Management System
PII	Personally Identifiable Information
RP	Relying party
SSO	Single Sign On
UUID	Universal Unique Identifier

5 Assurance in control of identity information use

5.1 Overview

An identity management system implements controls processes that deliver identity information. These processes include:

- The management of the identity lifecycle, from (initial) identification of an entity until removal of the entity's identity information (see ISO/IEC 24760-2).
- The provision and management of identity assurance, authentication of the identity and the assessment of identity-related risk associated with any resource the entity need to access.
- The management of identity attributes at the level of the relevant identity authorities.

Requirements for processes that manage identity information depend on the nature of the entity. For example a domain where personally identifiable information (PII) is processed and stored needs to gain the consent of the PII principal and provide suitable privacy safeguards.

Management of identity information for a particular domain of application may duplicate or substantially overlap with a process using the same information performed by an identity management system for another domain. For example, identity proofing may be undertaken by a service provider acting in the role of an identity information provider operated by government or by an industry group, as well as at an organization level where the organization is managing identity information pertaining identities in its domain.

5.2 Identity assurance

5.2.1 General

One function of an identity management system is to provide accurate identity information". This assurance is given with a specific level of confidence. The range of authentication capabilities of an IMS determines the different levels of confidence that can be provided.

Authenticating an identity can take place at every transition in the identity lifecycle as specified in ISO/IEC 24760-1. Authentication also takes place as part of entities interacting with each other when an identity is active, e.g. prior to accessing a service delivered by a relying party.

5.2.2 Risk Assessment

Whenever identity and personal information is collected and stored an identity-related risk assessment shall be carried out in relation to the context and objectives of the service to be provided to entities. Levels of confidence in identity information and access services shall be specified according to assessed levels of risk.

5.2.3 Identity proofing

In identity proofing, the level of assurance in identity information required by any relying party consuming the identity information in a particular domain determines the type, scope and reliability of evidence for identity information used to establish an identity in that domain. Identity proofing processes also extend to other techniques which are not solely document-based. In general, the more of the controls can be met and the greater the access to authoritative sources can be validated during identity proofing with the higher the level of assurance.

Note A higher number of independent sources could compensate for a lower level of assurance in the information provided by those sources.

ISO/IEC 29003, "Identity proofing" gives requirements for that process. ISO/IEC 29115, "Entity authentication assurance" provides the objectives and controls to achieve particular levels of assurance.

The result of identity proofing is an identity for a specific entity with a particular level of assurance.

An explicit level of assurance in identity information and derived from other processes such as the use of trusted referees to vouch for a claimed identity, the entity presenting the claimed identity and evidence of the claimant's use of the identity in the community' provides a qualified trust in the result of processes that base

decisions on this information, e.g. access control. An identity management system may create a credential, for an entity, e.g. a passport. A credential may explicitly refer to the level of assurance of the identity information it contains. The use of a credential can never convey a higher level of assurance in than the level of assurance achieved in the identity management system that created the credential.

5.2.4 Identity profile

An identity profile is of a set of attribute types used as template for gathering, structuring or presenting identity information.

Note Although a profile may contain identity information, it is not intended for identification. Its purpose is to provide identity information about an entity to system processes that need the information for their functioning

The set of identity attributes in different identity profiles may differ. There should be a clear distinction between identity attributes and additional personal attributes may be added to an identity management system due to their common use across. For instance, a language preference may be present in a profile for the user interface and in a profile for book interests.

A profile may be based on a template of attribute types. A profile template may be established by international or industry standards.

Note a profile based on a standard template might support cross-domain use of the identity information in the profile.

An identity profile may be used in an identity management system to determine a role or privilege for an entity in access management.

An identity profile may be used by a process to select a pre-configured subset of identity information to present in interacting with services in the domain of applicability.

In an identity management system an identity profile may be associated with a specific level of assurance in the identity information it contains.

Note A profile may contain a reference identifier that can be used to distinguish between two entities that otherwise have the same identity information in their profile. For instance, speak the same language, are interested in the same authors, like the same food and are in the same age bracket.

6 Accessing identity information

6.1 Overview

The objective of an organization in terms of information security is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. In terms of identity management, the management of organizations should understand their liabilities in ensuring adequate controls and the consequences of information leakage when processing information, e.g. when collecting, storing, using, transmitting, disposing of organizational information. This should be adequately policed in any organization with control objectives.

6.2 Policy on accessing identity information

The identity of an entity should be properly managed to ensure that:

- Accountability for all ICT system actions and outcomes is assigned to appropriate identifiable human entities that interact with or are responsible for the system.
- Only authorized entities have access to the identity information they need
- The organization fulfils its obligations from regulations and contractual agreements, and
- Entities are protected against the risk of identity theft and other identity related crime.

An information security policy shall highlight the necessity to manage and secure users' identity information. The preservation and protection of any entities identity information may also be required when dealing with third parties. This shall be clearly documented within the operation procedures.

6.3 Access management

An identity management system may provide the foundation of a system for access management. ISO/IEC 29146 specifies the framework for realizing a system for access management.

Resources and services for which access is managed may be present as entities in an identity management system.

6.4 Identifiers

Different identifiers of the same identity may be used in different situations to represent the same entity. This may facilitate unambiguously representing the entity in critical systems or hiding an entity's identity when providing the entity's identity information for use in some processes examples of personal indirect identifiers (pseudonyms) see clause 7.3.4 Pseudonyms ahead below

6.4.1 Personal identifiers

Examples of personal identifiers are:

- A combination of attributes such as full name, date of birth, place of birth; and
- A reference number assigned by an authority such as a birth registration number or any other random reference that can be used as pseudonymous.

Examples of pseudonyms are passport numbers and identity card numbers. In this case, the referenced passport or identity card contains information about a person that can be used to construct the required identifier for a domain.'

The use of indirect identifiers can enhance privacy because an identity authentication exchange with an unauthorized entity reveals less personal information if an indirect identifier is used than if a direct identifier is used. This is illustrated by the example of a personal identifier that is the combination of full name, date of birth and place of birth attributes and an indirect identifier that is a passport number referring to a passport. In this case, if an authentication exchange is initiated with someone using a passport number as an indirect identifier, then unless the authenticating party has access to the information contained in the passport, they cannot determine the person's full name, date of birth and place of birth.

6.4.2 Device identifiers

Device identifiers allow distinction between similar devices in the domain in which they operate. In the domain of GSM mobile telephone services, the International Mobile Equipment Identity (IMEI) is an identifier of the mobile telephone handset. The GSM SIM card number used by the equipment is another example of device identifier in the domain of some mobile telephone service. It is an identifier for the telephone handset and may also be an identity attribute or part of the identifier of the phone's owner.

6.4.3 Information object identifiers

Information objects may also have attributes that can be used as identifiers: process name, session name, path name, uniform resource names (URN), uniform resource identifier (URI), are examples identifiers for information resources. It should be noted that if, for example, an URI is an example where what is identified is the location, but the object at that location may change at any time.

6.4.4 Pseudonyms

As defined in ISO/IEC 24760-1 Information technology — Security techniques — A framework for identity management, pseudonym is an identifier that contains the minimal identity information sufficient to allow a verifier to establish it as a link to a known identity. Pseudonyms are frequent in identification and can be used to prevent or tightly control the ability to associate the identity of an entity in one domain with the identity of the same entity in a different domain.

The use of different pseudonyms for the same entity in different domains can help to prevent the association of activities performed by the entity across different domains. However to be effective it is also necessary to restrict access to explicit identifying information for the entity stored in the domains. Pseudonyms can also be useful within a domain to prevent or tightly control the ability to associate attributes of an entity with other identifiers associated with that entity.

Pseudonyms are par-domain reference identifier. Identity information associated only with pseudonym as the identifier cannot be correlated with identity information related to the same entity in another domain. This prevents the formation of new identity information about an entity by two or more colluding domains.

Pseudonyms are commonly implemented in a way that prevents or tightly controls the ability to link the pseudonym identifier with any other identifiers associated with the identity of an entity. Thus, identity management systems shall restrict visibility of some identity attribute values when identity related requests are made concerning an identifier by a pseudonym.

Pseudonyms can be used in association with privacy enhancing technologies to protect the privacy of people. The objective of privacy enhancing technologies is to be able to collect personal data relating to individuals without having to know their identity because, for instance, the law forbids it.

Pseudonymization is a process applied to personally identifiable information (PII) which replaces identifying information with an alias. The alias can be a pseudonym. Consequently, following pseudonymization, associating attributes of an entity with other identifiers associated with that entity is prevented or tightly controlled.

Pseudonymization can be done in a reversible way by using correspondence lists of identity references and their pseudonyms or by using two-way cryptography algorithms for pseudonymization in a reversible way, i.e., information related to the identity of an individual is replaced by a code, while the key showing the correspondence between the code and the identity reference of the entity is kept separate, as well as other identity information, e.g., name, date of birth and address.

For further information about pseudonymization, see ISO/IEC 29100 Information technology -- Security techniques – Privacy framework.

7 Identity management and the authorization of using resources

7.1 Overview

For the purpose of using system resources, each entity has to be described in systems. Each ICT application system typically has accounts associated with an entity to store the various information required by the business logic of the system. This information evolves over time with the use of the system resources and the changes in the identity information of the entity.

7.2 Authorization of using resource

Authorization is the granting of access to the resource to an entity. Typically, at the time of access, entity is represented by some form of authenticated identity. Authenticated identity may be entirely provided by the IIP and IIA or as the combination of that and the information contained in the ICT application account. The combination of such identity and the metadata about the resource is evaluated against the policy to determine the authorization.

Note metadata of resource is also an identity of the resource.

Refer to ISO/IEC 29146 for the full description of authorization.

7.3 Account life cycle

The account follows a lifecycle starting from it being established to it being terminated. Account is always valid for a period of time, has a start date and an end date as it relates to the ability of an entity accessing a system or using it. The account may also persist after the entity ceases to use the system. Typical account lifecycle has following stages:

- *-Not Existing*: the account is defined but not yet activated. The account is just associated with the entity and one of its identifiers.
- *- Created*: the account is activated.
- *- Active*: the account is recognized as valid and the entity can exercise activities. The account is also recognized as being 'unlocked'.
- *- Inactive*: the account is recognized as valid but the entity is enable to act. Its status is also called 'locked'.
- *- Archived*: the account may be required to remain available after the business need for its use cease to exist, to determine whether or not the account has in the past been associated with a particular action that may refer to an entity. The status is marked as 'not-reusable'.
- *Terminated*: the account (and any reference) is deleted.

Next figure shows the state-transition model for the account authorization life cycle.

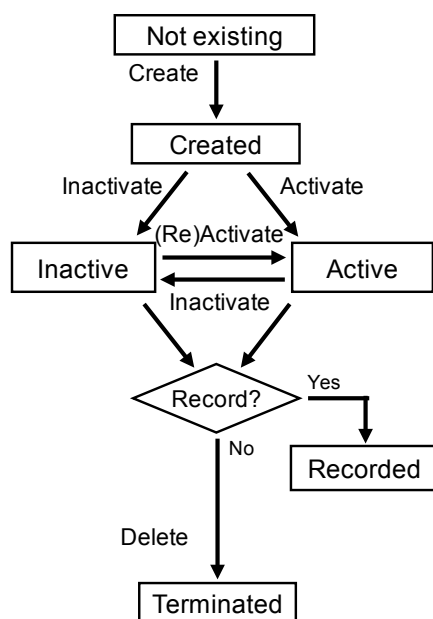


Figure 1 – Account life cycle

Account for the particular ICT application system may be created before or at the first time use of the system by the user. Typically, when the application system needs to start accumulating information before the first use, the account is created in advance.

7.4 Identity life cycle and accounts authorization life cycle

Authorizations associated to entities will occur in addition to the entity's identity activation at the accessed resource system to reflect the additional business needs of the entity in the domain. All authorizations are tied to the existence of the entity's identity and cease to exist when the entity quits. Enrolment may, however, have shorter lifecycle than the associated entity's identity, for instance on entity move or change of function.

Enrolment will be initiated in due time in respond to business needs. They will modify over time, and will also ends when the businesses need ceases to exist.

Each domain must adequately architect the provisioning and the de-provisioning of account authorizations for systems controlling access to resources within that domain. An identity management system must provide the foundation for supporting ICT application systems in controlling any entity account authorization over time in any domain where the entity may be authorized to access. The authorizations in one domain may be provisioned for an identity presented in and trusted by another domain, with the explicit consent of the entity of the identity (more detail on the management of identity information in a federated environment can be found in Annex A).

Next figure shows the different evolutions of the states of an entity's identity and the impacts on the associated enrolment of an ICT account.

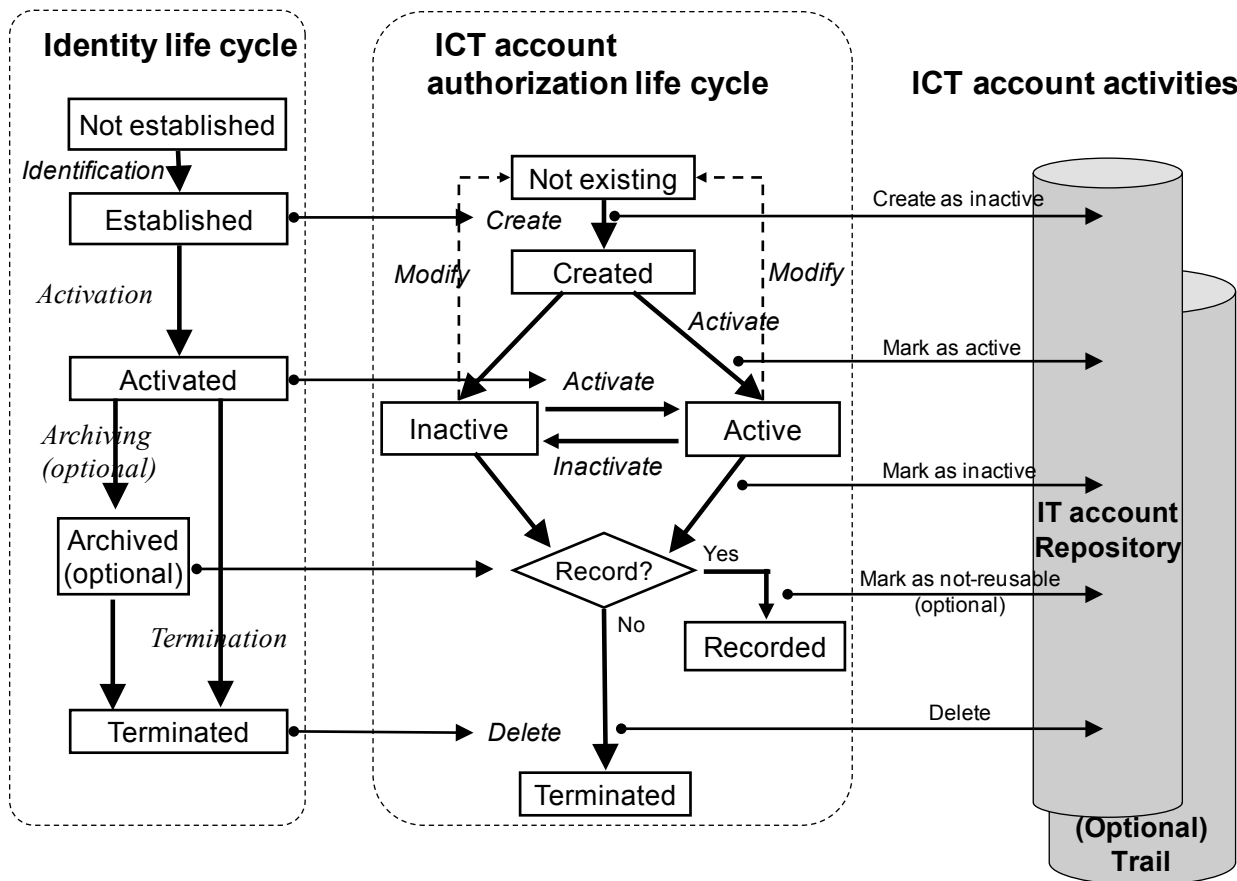


Figure 2 – Entity' identity and associated authorizations life cycle

7.4.1.1 Creation

The process of creating an account in a domain involves systems management action within the domain that allows an entity to interact with other entities according to the goals of the domain and authorized privileges.

7.4.1.2 Activation

The process of activating an account in a domain enables the use of provisioned means and consequently enables the entities to interact with each other.

7.4.1.3 Modification

Over time, the provisioned means may require modification because the business needs change but also because during their lifecycle, entity attributes may change. This may affect the recognized identity of the entity. In such cases, additional identification is required to allow the recognized entity to be updated / modified. In such cases, this additional identification causes a transition back to the established or non-established state, followed, as relevant, by transition to one of the other states. Modification is, however, not necessary valid for all provisioned means.

7.4.1.4 Inactivation

Under certain circumstances, it may be required that the enrolment is suspended (i.e., person on long vacation leave or suspected of fraud). In these situations, it does not represent that the entity is leaving the domain or the domain, but only a temporary revocation of rights.

An enrolment is being suspended when

- The business need disappears,
- The associated entity ceases to have interactions in the domain according to a predefined pattern e.g. a person doesn't use a service for a long period and loose a related business function,

- Confidence to the entity is lost.

The process of inactivation commonly requires a check to ensure that the enrolment is subject to suspension.

7.4.1.5 Reactivation

Reactivation from the suspended state is sometimes required, e.g. when returning after a period of unavailability).

Some reactivations may require proofing and therefore considered as a modification imposing a transaction back to the establishment.

7.4.1.6 Delete or De-provisioning

De-provisioning shall assure that when an entity leaves the domain, the means being provided for authorized services are effectively removed along with the removal of the authorization.

7.4.1.7 Archiving

Inactivation may take the form of archiving, i.e., when the associated entity is no longer active in the domain but when the possibility exists that in future the referred entity becomes active again. The reactivation takes the form of "restoration".

8 Tracing and monitoring identity information usage

Identity management and the associated processes controlling the authorized activities of a domain may be subject to a variety of legal, regulatory and industry business requirements that necessitate some level of monitoring and traceability. These requirements can be wide ranging, including everything from log-files and other measures for the protection of personal information, to maintaining required time-stamp accuracy and traceability (refer also to ISO/IEC 18014, *Time-stamping services*). All entities that provide services associated with identity management should provide any mechanisms needed to exchange, verify and protect identity management auditing information.

9 Control objectives

This clause summaries objectives and associated controls to be verified when setting up or reviewing a framework for identity management.

9.1 Contextual components of a framework for identity management

9.1.1 Establishing a framework for identity management

Objective: To establish a management framework to initiate and control the implementation of managing identity of entities

9.1.1.1 Defining the domains of applicability of a framework

Control

The environments where entities, or groups of entities, can use and referred with a set of attributes for their identification and other purposes shall be clearly defined and documented.

Implementation guidance

The boundaries of a framework for identity management shall clarify the limits where the entities can be verified.

The objective, or the existing or legal reason, and the associated liabilities, of a domain clarify the limits where it can apply its control on entities.

Other information

A domain of an identity is well defined in relation to a particular set of attributes defining groups of entities.

An IT system within an organization that allows users (a group of entities) to login is a sub-domain for the user's login name in that organization.

9.1.1.2 Documenting the framework

Control

The limits of the domains of a framework, its possible extensions to domains of other frameworks, the groups of entities recognized in the framework, their identification process, and the means by which each recognized entity may be verified across its lifecycle in the framework shall be documented.

Implementation guidance

A framework for identity management can be centralized or distributed, user centric or federated, conformed to ISO/IEC 24760 part 1. Each implementation aspect leads to different documentation requirements.

An entity can have more than one identity. In a particular domain of applicability an identity can become a distinguishing identity or an identifier to allow entities to be distinguished or uniquely recognized within that domain. The repository of a framework for identity management shall be able to gather the various identities of the different groups of entities it recognized. Attributes describing an entity in a domain are values of an identity maintain in the repository of the framework.

As a consequence of a possible implementation of a framework, any entity's attribute can be used as an identifier outside of the identified domains of a framework and shall therefore be officially registered in the framework repository.

Each domain of an attribute that specifies the where the attribute was created or its value was assigned should be documented in the framework repository.

9.1.1.3 Identifying identity information authorities, IIA, identity management authorities, and regulatory bodies

Control

ISO/IEC CD 24760-3.1

Entities that can make provable statements on the validity and/or correctness of attribute values of identities of other entities (IIA) should be recognized in domains of a framework for identity management.

Entities endorsing management and regulator responsibilities for the preservation of identity information should also be identified.

Implementation guidance

An identity information authority is typically associated with the domain, for instance the domain of origin, in which the attributes, which the IIA can make assertions on, have a particular significance.

Other information

An entity can combine the functions of identity information provider and identity information authority.

9.1.1.4 Identifying Identity information providers, IIP

Control

Entities that make available identity information to other entities should be recognized in domains of a framework for identity management.

Implementation guidance

The operations performed by an identity information provider are to create and maintain identity information for entities known in a particular domain.

Other information

An entity can combine the functions of identity information provider and identity information authority.

9.1.1.5 Identifying Identity relaying parties, RP

Control

Entities that rely on the verification of identity information for a particular entity should be recognized in domains of a framework for identity management.

Implementation guidance

A relying party has a trust relationship with one or more identity information authorities. Any RP is exposed to risk caused by incorrect identity information.

9.1.1.6 Maintaining the framework

Control

Domains of a framework for identity management may use over time different identity information authorities, identity providers, and relaying parties to support their interactions with entities. Domains may also be created and terminated or their conditions of applicability may change. A documented process should be described that ensures the maintenance of the important entities in a framework.

Implementation guidance

Identity Management should include the governance, policies, processes, data, technology, and standards that ensure the control of the lifecycle of keys important entities of IIA, IIP and RP, from initial enrolment to archiving or deletion in a framework.

9.1.1.7 Privacy assurance

Control

To ensure the privacy of entities is preserved at any time as the basic objective of establishing a framework for identity management

Implementation guidance

A framework for identity management should establish the necessary controls that provide the guarantee, when required, to protect the privacy of the human entities it interacts with.

A framework for identity management shall document any sensitive information it processes about human entities to conform to ISO/IEC 24760 part 1.

Other information

Requirements for the handling of sensitive identity information are given in:

- ISO/IEC 29100[9] Information technology — Security techniques — Privacy framework
- ISO/IEC 29101[10] Information technology — Security techniques — Privacy reference architecture

9.1.2 Establishing identity

Objective: To define, document and communicate on identity of entities

9.1.2.1 Identity representation

Control

The reference of an entity in a framework that is intended to remain the same for the duration an entity is known in the domains of a framework is referred as reference identifier and shall not be associated with another entity even when the entity ceases to exist in the domains of the framework, and for a period specified in a policy and compliant with regulations.

Implementation guidance

A reference identifier persists at least for the existence of the entity in a framework and may exist longer than the entity, e.g., for archival purposes and authorities' needs.

A reference identifier for an entity may change during the lifetime of an entity at which point the old reference identifier is no longer applicable for that entity but should not necessary be reused for another entity for the same reasons.

A reference-identifier generator is a tool that may help providing unique values for reference identifiers

Other information

A database management system can be a reference identifier generator when it assigns a unique record number to a new record being added to a table and the record number is used as reference identifier.

9.1.2.2 Identity information

Control

The set of values of attributes required to compose an identity of any entity in domains of a framework for identity management shall be fixed, validated by the verifiers, and communicated.

Implementation guidance

The verifications, of the values of the required attributes composing an identity, result in an authenticated identity for an entity in a framework.

The authentication process involves tests by a verifier of one or more identity attributes provided by an entity to determine, with the required level of assurance, their correctness.

9.1.2.3 Distinct identity of different entity types

Control

The number of distinct entity types in the domains of a framework of identity management shall be recognized and described with distinct attributes values composing their identity.

Implementation guidance

items inside or outside an ICT system, such as a person, an organization, a device, a subsystem, or a group of such items that has recognizably distinct existence in domains of a framework for identity management, are distinct entity types that may be described with different attribute values.

Each entity type should be documented covering semantic and syntax with the list of required attribute values for their identity being validated.

9.1.2.4 Authenticating an identity

Control

A formalized process should be documented that verify the identity information for an entity.

Implementation guidance

The authentication process involves tests by a verifier of one or more identity attributes provided by an entity to determine, with the required level of assurance, their correctness.

Verifiers may be the same as, or act on behalf of, the identity information authority for a particular domain.

9.1.3 Managing identity information

Objective: To ensure that identity information is maintained and protected in all domains of a framework for identity information, from initial enrolment until archiving or deletion.

9.1.3.1 Assurance in collecting and managing identity information

Control

All information security responsibilities for the collection and the management of identity information should be defined and allocated.

Implementation guidance

Allocation of information security responsibilities for collecting and managing identity information shall be established in accordance with the information security policies. Responsibilities for the protection of individual identity information and for carrying out specific information security processes on collecting and managing identity information should be identified.

Responsibilities for information security risk management activities and in particular for acceptance of residual risks when defining levels of assurance in collecting identity information should be defined.

Identity management activities should include:

- Application(s) implementing an identity register;
- Ensuring correctness of the identity information with a defined level of assurance;
- Establishing the domain of origin of identity information;
- Maintaining the identity information over the lifecycle of the identity;
- Authenticating the identity;
- Mitigating the risk of identity information theft or misuse.

Other information

The information security manager of an organization, if identified, should take overall responsibility for the development and implementation of the different levels of assurance to support the collection of identity information, and for the management of identity information.

9.1.3.2 Defining and controlling Identity lifecycle

Control

A formalized process should be documented that define and maintained the lifecycle of identities in domains, and that control the status of any identity in each domain.

Implementation guidance

The lifecycle of identity information starts from initial enrolment and ends with archiving or deletion.

Other information

The following stages in the identity lifecycle are, according to ISO/IEC 24760 part 1, identified: Unknown, Established, Active, Suspended, Archived or Deleted.

9.2 Architectural components of a framework for identity management

9.2.1 Establishing an identity management system

Objective: To ensure a system is implemented and well document for the management of identity information

9.2.1.1 Documenting an identity management system

Control

An identity management system should be documented prior being implemented for managing identity information

Implementation guidance

The documented design for the architecture of an identity management system should specify the system in its deployed context based on *stakeholders* and *actors* defined requirements.

The documented design shall address requirements for both actor and non-actor stakeholders.

Other information

The documented design shall exhaustively describe

- actors requirements
- stakeholders requirements
- view points
- models
- components
- maintenance processes
- information flows and actions.

The list of actor's types and their interactions with the systems should also be documented.

9.2.1.2 Identifying an identity registration authority

Control

An identity registration authority should be identified for any identity management system.

Implementation guidance

An identity registration authority has the duty and capabilities to set and enforce operational policies for

ISO/IEC CD 24760-3.1

collecting, recording and updating identity information.

Responsibilities of an identity-management authority include:

- to modify, create or revoke operational policies;
- to authorize modification of mechanisms to establish a required level of assurance in entity authentication for accessing identity information and system control functions;
- to authorize changes in the type of information recorded in the repository;
- to authorize modification of identity information recorded in the repository.

Other information

If not identified, the information security manager should play the role of the identity registration authority.

9.2.2 Controlling an identity management system

Objective:

9.2.2.1 Accessing an identity management system

Control

Access to an identity management system should be limited to people dedicated to its maintenance, identity information providers and other relaying and relying parties, and to individuals for the consultation of information collected on their person in the context of privacy preservation.

Implementation guidance

An information management system should develop the required interfaces to provide access to the need to have with rights defined and authorized by the Identity information authority or the identity registration authority.

9.2.2.2 Required components of an identity management system

Control

An identity information system should include, at a minimum,

- a repository for identity information related to the entities types recognized in domains of the relevant framework with different attributes sets, semantic and syntax
- a central management system, capable of collecting identity information from various validated sources (attributes domains of origins), and deleting the information when the conditions for storing identity information cease to exist
- management interfaces for providing access to the need to have identity information
- a storage component archiving the information on entities that ceased to exist
- a generator of unique reference identifiers.

Implementation guidance

Identity management systems may vary in components depending on the model developed for its implementation. The identity management system should, however, remain independent as it needs to respond to functional requirements specific and largely different from any other usual IT system.

It is not advice to integrate an identity management system with other organizational systems such as a Human system or a procurement system.

9.2.2.3 Auditing an identity management system

Control

An identity management system should be assessed or audited on regular basis (a year per default)

Implementation guidance

The audit or assessment should validate that the identity management system is operating in accordance with its documented policies and procedures, and is compliant with legal and other externally imposed requirements (e.g., privacy requirements).

Assessments or audits should:

- Include statements describing the operations performed by the identity management system, in particular in respect to meeting operational policies;
- Validate that the identity management system reports on specific operations (e.g., vulnerabilities), assess if the operations meet applicable policies (e.g., privacy control), and alert on any discrepancies;

Annex A (normative)

Identity federation

A.1 General

Identity federation represents an agreement between two or more domains specifying how identity information will be exchanged and managed. Federation agreements include common protocols, formats and procedures to be used across the federation covering security, privacy, governance and auditing.

Identity federations are typically established with the objective to broaden the interoperable exchange of identity information and leverage the benefits derived from it, such as expanded consumer eCommerce and enterprise productivity and efficiency that in turn enable a growing and prosperous digital economy.

In an identity federation, an identity management system for a domain is formally recognized by other domains in the federation for the entities known in that domain for use in the other domains. A federation could be internal to a larger organization, e.g. multi-division corporation, informal (for example among friendly groups), or created as a distinct entity depending on the threat and risk vectors and the extent of controls required to manage risks. If a federation does assert trust, it must be able to accept risk, which points to the establishment of some form of legal entity.

The emergence of threat and risk arising from identity federation arises from the information asymmetry inherent in the federation structure: how the parties trust and rely on each other's different policies and management processes, supported by differing features and functionality at different states of maturity. The main control mechanism to mitigate and manage the risk is a trust framework, in some contexts known as a circle of trust or chain of trust.

This clause offers practitioners guidance on the requirements and features that characterize trusted identity federations, the role they play in the broader federated trust framework mechanisms, and their respective risks and controls.

An identity federation may establish rules for the format and encoding for the exchange of identity information.

An identity federation shall specify security and operational requirements, rules and mechanisms:

- to request, deliver, store, use and dispose of identity information,
- to recognize the identity information providers of participating domains,
- to assert identity information requested by a relying party in one of the federated domains,
- to protect the privacy of human entities,
- for identity proofing for enrolment in any of the federated domains,
- for the security and privacy of operating the identity management system,
- to join the federation.
- level of assurance according to ISO/IEC 29115
- associated with identity proofing for credential issuance; and
- associated with entity authentication within the federation.

Note 1 The specified requirements provide the basis for trust in the identity information.

Note 2 The specification may refer to a recognition process e.g., providing agreed evidences, a certification process e.g., providing evidences of being accredited by independent third party, bilateral or centrally organized.

Note 3 A federation may be formed with a commonly established requirement or by mutual recognition of these requirements as independently established by each domain or chain of trust.

A.2 Characteristics of trusted identity federations

Identity federations emerge in a range of structures and sizes. A simple Identity federation may typically have a mix of actors performing different roles such as trust framework operator (in some contexts known as federation operator, FO), identity information authority (IIA), identity information provider (IIP), and associated brokers, delivering identity attribute or credential, relying party (in some contexts known as a service provider, RP), subject (in some contexts known as principal, subscriber or requestor). Selections of these actors are defined in Part 1 of this standard, terminology and concepts, and described in more detail in Part 2 of this standard; architecture and requirements.

At a minimum, a federation involves two types of actor - the identity information provider (IIP) and the relying party (RP). An IIP manages entity identity-relevant information, and the RP offers services to users who satisfy the policy requirements associated with these services.

Three party federation models that include a subject are the typical baseline in user-centric consumer contexts, but can expand to four and five party models. Many identity federations are more complex and involve more actors to reflect their objectives, such as those models described as hub-and-spoke, and federation of federations (in some contexts known as inter federations).

A pair-wise federation is most basic federation as depicted in Figure 3.



Figure 3 – Pair-wise Federation model

A more typical federation may comprise four, five or more party models as depicted in Figure 4.

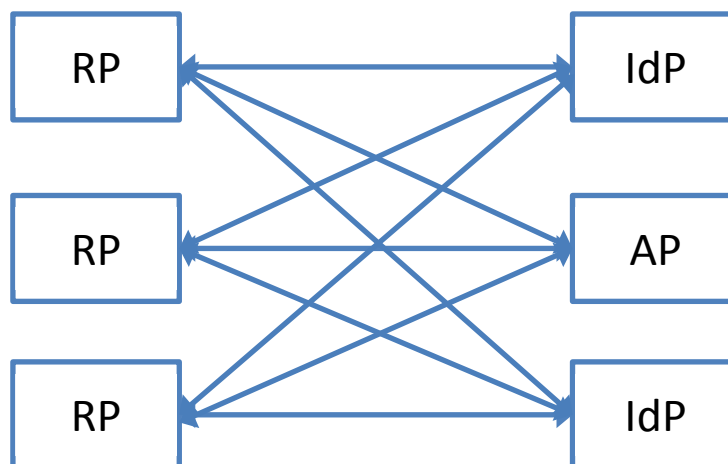


Figure 4 – Typical Federation model

Federations at this complexity and beyond, begin to exhibit additional features to assist their ease of operation.

The role of federation operator may be, i.e., to manage the issues arising from the operation of the federation. The role can be carried out by an existing federation member or an independent third party.

In previous figure the subject/requester is totally excluded from the relying party (RP) <-> identity information provider orchestration. Best practice in user-centric and privacy-friendly discovery processes is for the user/subject/requester to intervene in the message exchange between the RP and IIP in order to consent to the release of an attribute from the IIP.

The federations themselves may take on different structural forms to manage their complexity. Hub and spoke structures as depicted in next figure below offer the benefits of a central gateway with concentrated technical expertise. Without the use of privacy enhancing techniques such as anonymity or pseudonymity and consent,

privacy issues arise as the gateway structure is challenged to manage the data minimization concepts of anonymity, unlinkability and unobservability.

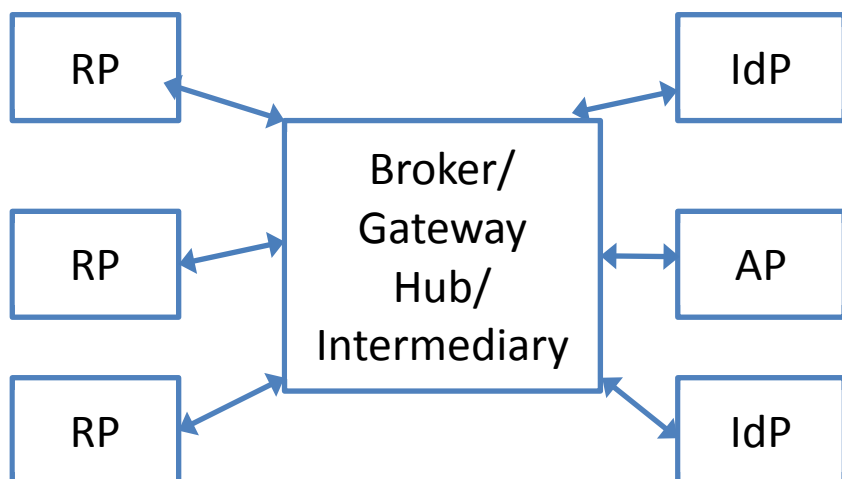


Figure 5 – Federation Gateway model

An identity federation uses a communication network. This network may be open with peer-to-peer communication between all participating identity information providers or it may use hierarchical relations where identity information is provided via one or more intermediate identity information providers.

Note Hierarchical communication may for instance occur when existing identities forms an identity federation.

The main players of a federation, i.e., identity information providers (IIP) and the relying parties (RP), may interact among them in different way forming trust relationships or a circle of trust. In this way they can have pertinent business agreements in place regarding how to do business and interact with identities.

A.3 Management and organisational considerations

An identity federation should establish rules governing the policy fabric and subsequent operational mechanisms of the trust framework to delineate the responsibilities of the parties:

- to be responsible for maintaining and/or adjudicating the semantics and/or syntax of identity information
- to discover and recognize the identity information providers and other actors of participating domains,
- to authenticate and assert identity information claims by a relying party in one of the federated domains,
- to protect the security and privacy of entities, and the confidentiality, integrity and availability of the operation
- to define and agree what inter-federation records may be maintained for auditing purposes, for how long, and under what circumstances they may be accessed;
- to define and agree standards, mechanisms, processes, technologies to transfer the identity information between federation participants.
- to participate in funding and/or cost recovery models
- to join and leave the federation.

Note 1 The specified requirements provide the basis for trust in the identity information.

Note 2 The specification may refer to a membership compliance and trust mark or accreditation, e.g., providing evidences of being audited by an independent third party, bilateral or centrally organized entity such as the federation operator.

Note 3 A federation may be formed with a commonly established requirement or by mutual recognition of these requirements as independently established by each domain, or by a combination.

Typically, federations are structured such that the subject has a 'home' IIP that verifies the subject's authoritative identity information in a federation for the purposes of recognition, authentication and subsequent

confirmation. The 'home' IIP will guarantee identity proof, register, enrol, request, deliver, store, use and dispose of identity information within an agreed identity lifecycle and scope, noting that, in the human context, identity information can exist before birth and remain after death, with similar concepts of creation and destruction applying to NPEs.

A typical process flow may then see the subject attempt to access a resource at an RP, and the RP assembles the information at applicable assurance levels it requires, and re-directs the subject to an IIP to authenticate using a credential. Subsequent message exchange may involve the RP seeking additional attributes from the subject's 'home' APs, which may be released to the RP subject to (in the case of humans) the subject's consent, after which the subject is given access to the requested resource.

The merge of identity information from different authorities in two distinct domains is a typical requirement when two organizations are merging in a federation. In these use cases, procedures shall be specified to resolve collisions and inconsistencies such that within the resulting domain:

- Reference identifiers are unique, and
- Where applicable pseudonyms are used, and
- It is not possible to associate an identity with the wrong entity.

Means should exist for arbitration between authorities of identity providers that contain conflicting identity information.

A.4 Discovery

The technique of Discovery may also be used to exchange the required identity information within a federation. The parties in the federation can then be located quickly and dynamically. This is particularly useful in large federations where there is membership churn. Federations and the trust frameworks that underpin them can operate listing services to further enhance discovery and interoperability.

(Editor's Note: a definition of a 'listing service' will be required)

But guidance on Discovery organization is then required. Depending on contextual and cross-contextual rules the mechanisms for discovery are enforced in different ways.

This feature is an intrinsic part of trusted identity federation and its development has been motivated by the increasingly complex requirements of trust frameworks.

The most common targets for discovery are typically identity information providers. The discovery process is the capability provided by the IIPs and IIA in a federation, with the user/subject/requestor's consent or by a legislative/regulatory requirement, to dynamically locate an identity information authority for a particular entity to provide a particular required attribute where:

- identity information does not exist or
- the RP lacks the level of confidence in the information sufficient to mitigate the subject's identity related risk for the service being accessed or,
- the RP does not indicate which IIP or AP to use.

Discovery throughout the federation can be achieved using static methods such as white lists, or reference to listing services. Listing services expose the existence of a range of identity services, typically Trust Frameworks, the Federation Operators involved in managing them, participating entities in the federation, and their certification status. The listing service function can be augmented by the use of dynamic methods of discovery, such as the publication and consumption of metadata of the services. Dynamic discovery helps the efficient operation of modern federations which typically see an ebb and flow of parties joining and leaving the federation.

Benefits of discovery include relying parties being relieved of the burden to cache or retain identity information as long as the requirements or obligations of the relying party do not necessitate data retention, thereby substantially reducing the liability of handling PII, and the freshness and accuracy of the data. Discovery mechanisms also facilitate dynamic registration and de-registration of federation relationships. Dynamic discovery can potentially support 'Bring Your Own Identity' and personal (device or cloud) data store use cases depending on the particular approach taken to enable it. See 1.

As for any other element of a framework for identity management, applicable requirements, e.g. law, regulation, policy, may limit the discovery activities. Identity providers and relying parties should be able to support mechanisms for discovering other identity providers in a federation.

A.4.1 IIP Discovery

IIP Discovery is the process of finding in the federation an IIP to provide identity information for an entity. This process may be:

- a user providing a reference to the IIP, e.g. by selecting from a presented list of options,
- a user providing a credential, e.g. an email address that contains a reference to the IIP,
- a user providing an identifier that is broadcast to all IIPs, with the one knowing the identifier responding.

It could be the process in which the user selects the IIP from the list of providers or the automatic discovery of the IIP from the user agreeing to provide information such as username or email address.

A.4.2 IIA Discovery

IIA Discovery is the process of finding in the federation an IIA that can authenticate information for a particular IIP. The discovery process may use a capability provided by an IIP in the federation to dynamically locate an identity information authority for a particular entity to provide a particular required attribute where available identity information does not indicate which IIA to use.

Note 1: A benefit of discovery capabilities in an identity framework is that relying parties are not required to cache or retain identity information as long as the requirements or obligations of the relying party do not necessitate data retention. The resultant benefits to a relying party include the substantial reduction in the liability of handling PII, and the freshness and accuracy of the data.

Note 2: As for any other element of a framework for identity management, applicable requirements, e.g. law, regulation, policy, may limit the discovery activities. Identity information providers and relying parties should be able to support mechanisms for discovering other identity information providers in a federation.

Note 3: A discovery mechanism facilitates dynamic registration and de-registration of federation relationships.

Next figure below is an example of a basic discovery dialogue in an enterprise context. Precise protocol flows may vary to some extent depending on the federation's objectives and context, and should include additional user directed information release consent steps to satisfy privacy requirements and support trust. It also demonstrates the fulfillment of the need to support multiple sources of identity information.

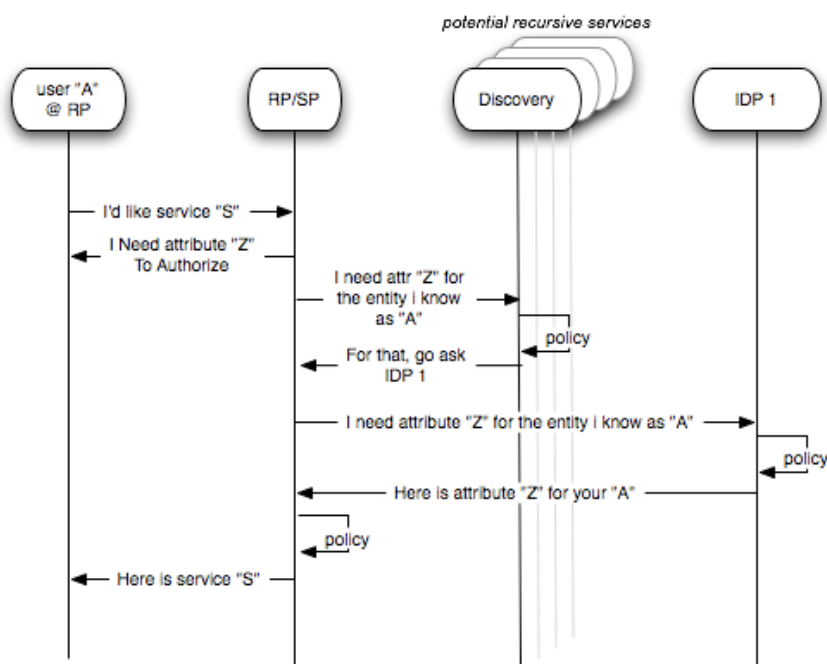


Figure 6 – Federation basic discovery dialog example

Note: IDP1 in Figure 6 example is an IIP

A.5 Considerations in inter-federation (federation of federation) scenarios

Inter federations were introduced in clause 1 above. While the considerations applicable within a federation apply to inter-federation, additional considerations fall into two broad categories; trust and interoperability. Where an entity with an identity in one federation may need, or want, to access services provided by another federation, an inter federation agreement should be reached, such that at least, an IIP in the first federation can have a trust relationship with the appropriate IIP (and AP where applicable) in the other federation. Interoperability between heterogeneous federations (each may use different federation software, different platforms, or different deployment profiles) requires strong adherence to agreed fixed policies and procedures to avoid identity and identifier duplication and ultimate collision.

When developing agreed procedures for inter-federation, the following requirements should be considered;

Compare policies and procedures of the participating federations to ensure they are consistent (or at least mappable) and there are no gaps;

Compare terms of service and end user license agreements to ensure they are consistent (or at least mappable) and there are no gaps;

Mechanisms for access control to information for individuals, based on their identity in one federation or another, must be explicitly defined, and should be exposed and reside in the home federation;

Defined controls to prevent identity theft while roaming between federations;

Defined rules on the use of privacy enhancing techniques such as anonymity or pseudonymity and consent when identity information is exchanged in the federation;

Defined controls to meet applicable requirements expectations, e.g. law, regulation, policy, from the various federations, particularly in pan jurisdiction contexts;

Compare law, regulation, and policy, from the various federations (particularly in pan jurisdiction contexts) of the participating federations to ensure they are consistent (or at least mappable) and there are no gaps.

A.6 Threats and Controls

To achieve its objectives, the identity federation faces a range of threats and risks that arise from the information asymmetry amongst the different parties with regard to the considerations, characteristics and requirements above. The range of threats applies, to a great or lesser extent, depending on the context (for example enterprise or user centric consumer). Phases in the identity lifecycle applying to users of the federation such as identity proofing, enrolment, provisioning, authentication and authorization, along with processes involved with the operation of the federation itself such as onboarding the participants in the federation, all carry inherent threats that require controls to mitigate and manage those risks. Identity related threats and controls are described Parts 1 and 2 of this standard, along with ISO 29115 Entity Authentication Assurance, and for privacy threats and controls in ISO 29100 Privacy Framework, ISO 29101 Privacy Architecture Framework and ISO 27018 Code of practice for data protection controls for public cloud computing services. This standard does not repeat those but describes the most common threats and controls as they relate to identity federation.

Typical identity authentication and authorization threats and their respective controls should be considered as shown below.

A.6.1 Requesting authenticated identity

When the user requests an access to the resource provided by the ICT application system, the ICT application system requests authenticated identity that holds the attributes it requires making decisions as to the access authorization is concerned. It may also request the additional attributes that are needed for the business

process in addition.

The following threats and controls should be considered.

A.6.1.1 Unauthorized request

It is also known as request forgery. The request is fabricated by the attacker masquerading the ICT Application being attacked.

Following controls apply:

- The request should be signed by the requester;
- Request disclosure.

Request may contain sensitive information thereby disclosing it making a security and privacy risk. In particular, the disclosure of the credential would cause a grave security risk to the entire system.

Following controls apply:

- Audience of the request should be restricted through the authentication of the destination;
- The request should be encrypted or transmitted through a protected channel;

A.6.1.2 Request tampering

In this threat, a request is modified by the attacker.

Following controls apply:

- The request should be integrity protected either by having the request signed or message authenticated or by transmitting it through a protected channel;

A.6.1.3 Request substitution

In this attack, the request is substituted with other request. Cross site request forgery (CSRF) is a typical example of such threat.

Following controls apply:

- The request should be cryptographically bound to the session between the user agent and the requester, user agent and IIP.

A.6.2 Performing authentication

Editor's Note: Contribution text needs to be provided.

A.6.3 Authorizing the release of attributes

Authorization of the release of attribute may be decided by the subject or by the policy set by the administrator of the domain. The following threats and controls apply:

A.6.3.1 Policy injection

The attacker may inject the policy to the policy engine through policy administration point.

Following controls apply:

- When an entity is pushing a policy, the entity should be authenticated and policy should be cryptographically bound to the entity.
- The policy being pushed into should be authenticated (tamper proofed / signed) ;
- SQL injection and other application vulnerability should be closed.

A.6.3.2 User Interface Hijacking

The attacker hijacks the user interface and tricks the user to authorize the release of attributes. Typical example of such attack is click jacking.

Following controls apply:

Editor's Note: Contribution text needs to be provided.

A.6.3.3 Term obfuscation

The attacker hides the attributes that is being requested, their purpose, and their distribution range by including them in a long agreement.

The federation operator or other entity should certify that the request conforms to the requirements set by the federation.

A.6.4 Returning the authenticated identity

A.6.4.1 Unauthorized response

Editor's Note: Contribution text needs to be provided.

A.6.4.2 Response disclosure

Editor's Note: Contribution text needs to be provided.

A.6.4.3 Response tampering

Editor's Note: Contribution text needs to be provided.

A.6.4.4 Response substitution

Editor's Note: Contribution text needs to be provided.

A.6.5 Obtaining auxiliary attributes

For the purpose of the authorization decision and other business processing, the ICT application may require additional attributes. They can be obtained from IIP or IIA.

All the threats and control of 6.4 and 6.7.4 applies. In addition, the following control applies:

A.6.5.1 Wrong IIA

An attribute may be available from multiple IIA. Attribute value may be different among them, and what is correct may be determined by context.

Following controls apply:

- Location of the IIA for the context should be obtained through the IIP in the context of the original request of source of attributes for a control;

A.6.6 Resource registration

Editor's Note: Contribution text needs to be provided.

A.7 Merging identity information authorities

The merge of identity information of different authorities is sometimes required. The typically happens when two organizations are merging in a federated organization. But before merging identity management systems of two distinct domains procedures shall be specified to resolve inconsistencies and in particular ensure that within the resulting domain:

ISO/IEC CD 24760-3.1

- Reference identifiers are unique, and
- It is not possible to associate an identity with the wrong entity.

Means should exist for arbitration between authorities of identity information providers that contain conflicting identity information.

Annex B (normative)

Privacy-respecting identity management scheme using attribute-based credentials

B.1 General

An identity management system may be built using attribute-based credentials.

Attribute-based credentials consists in a user-centric approach of an identity management system that has for benefit the protection of the privacy interests of the User, while also respecting the multilateral interests of all the entities [1].

B.2 Actors

An attribute based identity management system recognizes the following main actors:

- principal, which carries one or more credentials that can be used to claim that certain attributes are applicable when presented to a relying party,
- relying party, which accepts proofs from the credentials of the principal, and trusts the authority that has issued the credential (the identity information provider),
- identity information provider, which issues attribute-based credential(s) to the Principal, vouching for the correctness of the information contained, and
- identity information authority, which is responsible for maintaining the level of assurance in identity information made available to a relying party.

Note In the ABC4Trust implementation of this identity management system, a principal a principal is referred to as “*user*,” a relying party is referred to as “*verifier*,” an information provider is referred to as “*issuer*” and an identity information authority as “*revocation authority*.”

Figure 7 shows an overview of actors in this architecture of an identity management system.

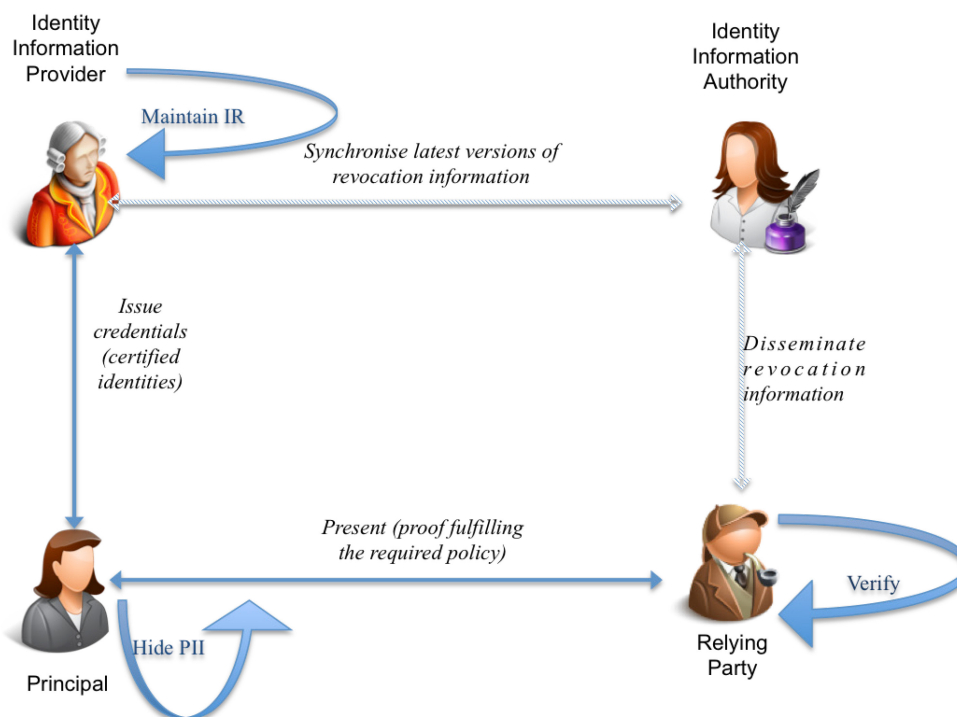


Figure 7 – Actors of the ABC4Trust architecture and their interactions

B.2.1 Principal

A principal is the central actor in the architecture, whose interests are:

- using services offered by the relying party;
- remain unidentified when using services of the relying party;
- have the possibility to remain unlinkable for different communications with the relying party (avoid profiling);
- avoid linkage of the use of her identity information with the relying party with the issuance of the attributes from the Identity Information Authority; and
- be able to create pseudonyms, whenever she likes to create a profile with a certain relying party.

The principle operates an IT device, referred to in this clause as “principal’s token,” that contains the credentials can communicate with equipment operated by a relying party.

B.2.2 Relying party

A relying party is a typical service provider, which provides services to the customers (Principals). In doing so, the interest of the relying party is to be able to provide the services to authentic principals only. The relying party publishes a presentation policy, which specifies the conditions the Principals are required to fulfil (for authentication) in order to use its services.

The relying party has an established relation with the Identity Information Authority, whose certification it accepts.

The interests of the relying party are:

- the accepted identity information must be verifiably correct;
- that only the Identity Information Authority is able to issue/manipulate certified identity information about Principals; and
- it needs to be assured that the principal cannot manipulate the certified attribute values of the Principal; and

- be synchronised with the Identity Information Authority about the latest version of the Identity Register in order to check credentials received and to prohibit any invalidated (revoked) credentials from being accepted as valid.

B.2.3 Identity information provider

An identity information provider is a system component to provide principals with certified identity information to be presented as needed by the principal.

The identity information provider vouches for the correctness and validity of provided information.

This actor is the one who is able to:

- issue credentials for one or more attributes to the principal;
- determine that previously provide identity information of an identity is no longer valid.

A credential of which the contained identity information is no longer valid is revoked.

B.2.4 Identity Information Authority

The task of the identity information is to

- Pro-actively provide relying parties information on credentials that have been revoked consisting of:
 - synchronising the latest revocation (invalidation) information with the identity information provider ,
 - synchronising the versions of the identity register,
 - disseminating the latest Identity Register version to the relying parties
- Upon request of a relying party assist in validation of a credential;
- Provide information to be included in a credential to enable its validation.

B.3 Control steps

An attribute based identity management system recognizes the following main control steps:

- The credential issuance, pertaining of providing the principal with the adequate attributes
- The presentation, when the principal requires interaction with the system
- The invalidation, when the principal has attributes being revoked.

B.3.1 Credential issuance

Credential issuance is an interactive protocol between the principal's token and an identity information provider. As result of credential issuance, a principal is in possession of one or more attribute credentials, each representing identity information pertaining to the principal.

An attribute credential consists of the following information:

- a description of the attribute type,
- an encoded representation of the attribute value,
- parameters for the cryptographic process of validating the identity information,
- a specification of the identity information authority that asserts the validity of the credential.

B.3.2 Presentation

Figure 8 shows the system components and their interaction involved in "*presentation*." Presentation is a process of communication between a principal's token and relying party equipment performed when the principal requires access to a service offered by the relying party.

Presentation starts when the principal's token receives from the relying party the information describing its presentation policy. A presentation policy defines:

- information to be provide to the relying party including

- the type of attribute
- the level of disclosure of the attribute value,
- authentication mechanisms that can be used to validate the attribute value,
- identity information authorities, that are accepted by the relying party as providing security in validation.

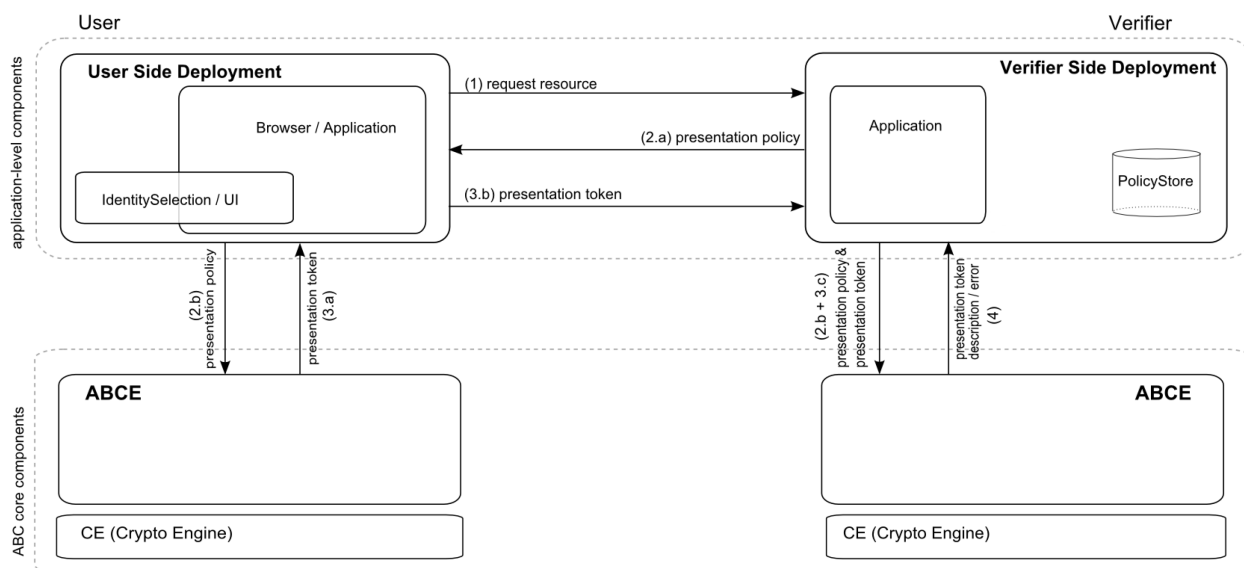


Figure 8 – Main components of a principal's token and relying party equipment

On the principal's token a process determines which combinations of the credentials in its memory will meet the policy of the relying party, in which the interaction of the principal may be required (in case different combinations are possible, i.e. if the principal can use different credentials from different identity information provider s). The principal then sends the completed claim to the relying party.

Upon receiving the presentation token, the relying party can verify whether the claims in it are correct (authentic from one of the trusted identity information providers it trusts), but also whether they are still valid. The final outcome of the verification is an "accept" or "reject", depending on the validity of the presentation token.

B.3.3 Invalidation

It is the responsibility of the system using the identity management system to define the cases when certain credentials need to be invalidated (revoked). This is typically when certain relations of the principal with the issued credentials (certified identity information) do not hold, such as cases of violation of terms of use by the Principal, termination of the legal contract between the principal and the identity information provider, etc.

In any case, invalidation is an important process in the lifecycle of the identity management using privacy-enhancing attribute based credentials. When an attribute is invalidated, the credential containing that attribute is also invalid. In the architecture process above, this would be an update of the Identity Register by the identity information provider, thereby ending the validity of the previously issued credential. This update then will be synchronized with the Identity Information Authority.

B.4 Architecture layers and components

The ABC4Trust architecture defines for each entity the core-components required to operate with attribute-based credentials. Each of the entities in the architecture for attribute-based credentials has separate components, which are required for their interaction. Figure 1.2 shows an overview of the components for the principal's and relying party's side, whereas a more detailed presentation of the components on the Principal's side is shown in Figure 1.3. The main components of each entity can be summarized in two main layers:

- Application deployment layer
- Core components - proof generation/verification layer (ABCE)

B.4.1 Application deployment layer

The application layer is not part of the Privacy-ABC architecture, but will operate on top of that. Roughly, this layer comprises all application-level components, which in the case of the User-side (Principal) deployment includes the main application and the Identity Selection (see description below). The application layer of Verifiers and Issuers will also contain the policy store and access control engine.

The Identity Selection component provides methods, possibly presented by a graphical user interface, to support a User in choosing a preferred combination of credential and/or pseudonyms, if there are different possibilities to satisfy a given presentation policy. A user interface is also used to obtain User consent, whenever personal data is revealed.

B.4.2 Core components - proof generation/verification layer (ABCE)

The proof layer contains the ABCE (Attribute-based Credential Engine) and the underlying technology specific components, as depicted in Figure 9.

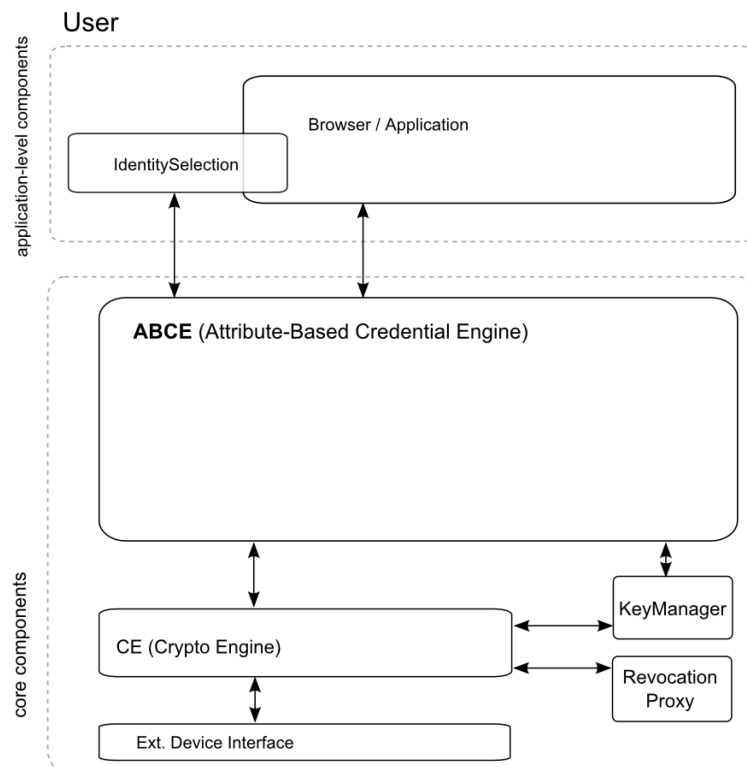


Figure 9 – Architecture principal's token [1]

The ABCE contains all technology-agnostic methods and components for a Privacy-ABC system. It contains the functionalities to parse an obtained presentation policy, perform the selection of applicable credentials for a given policy or to trigger the mechanism-specific generation or verification of the cryptographic evidence. The upper (deployment) layer then communicates with the same layer on the other entity (relying party or identity information provider) side.

The ABCE is invoked by the application-layer and calls out the other components, as shown in previous figure:

- Crypto Engine
- Key Manager
- Revocation Proxy;
- Policy Store; and
- External Device Interface.

B.4.2.1 Crypto Engine

Crypto Engine is the first component to be called by the ABCE the mechanism-specific cryptographic data. It provides common interfaces to generate the cryptographic information required e.g., to create, present, verify or inspect a presentation/issuance token. It internally orchestrates and performs the mechanism-specific cryptographic methods, such as the computation of signatures (e.g., U-Prove signature), commitments, zero-knowledge proofs, etc.

B.4.2.2 Key Manager

The Key Manager deals with the (cryptographic) keys of all parties and keeps them up to date (key life cycle management). On input of an identifier (URI) for a key, it returns a (list of) cryptographic key(s) that are currently valid for that URI. This component takes also care of fetching the current (public) revocation information that will be needed to keep the credentials up to date, or to verify whether a received presentation token is still valid.

B.4.2.3 Revocation Proxy

The Revocation Proxy handles the communication between the Crypto Engine and the Revocation Authority for the generation or presentation of tokens/credentials that are subject to revocation (invalidation). The concrete communication pattern strongly depends on the specific revocation mechanisms, which may be chosen.

B.4.2.4 Device Interface

The Device Interface components provide optional generic interfaces to ease the integration of external devices, such as smart cards, for both the “outsourcing” of computation and also to obtain data stored externally on the device. The integration of an external device might for instance be necessary if key binding to a smart card is required.

B.4.2.5 Policy Store

On the side of the relying party, the Policy Store stores the presentation policies accepted by the entity, and may also save the received presentation tokens for archiving or other security-related purposes (see Figure 9).

Bibliography

- [1] Jan Camenisch, Ioannis Krontiris, Anja Lehmann, Gregory Neven, Christian Paquin, and Harald Zwingelberg. D2.1 Architecture for Attribute-based Credential Technologies, 2011
<https://abc4trust.eu/index.php/pub/107-d21architecturev1>