INTERNATIONAL STANDARD

ISO/IEC 24760-2

First edition
2015-06-01

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

Part 2: Reference architecture and requirements

Technologies de l'information — Techniques de sécurité — Cadre pour la gestion de l'identité —

Partie 2: Architecture de référence et exigences

Reference number
ISO/IEC 24760-2:2015(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee, SC 27, *Security techniques*.

ISO/IEC 24760 consists of the following parts, under the general title *Information technology — Security techniques — A framework for identity management*:

— *Part 1: Terminology and concepts*

— *Part 2: Reference architecture and requirements*

The following part is under preparation:

— *Part 3: Practice*

Further parts may follow.

Introduction

Data processing systems commonly gather a range of information on its users be it a person, piece of equipment, or piece of software connected to it and make decisions based on the gathered information. Such identity-based decisions may concern access to applications or other resources.

To address the need to efficiently and effectively implement systems that make identity-based decisions, this part of ISO/IEC 24760 specifies a framework for the issuance, administration, and use of data that serves to characterize individuals, organizations, or information technology components, which operate 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 system management so that information systems can meet business, contractual, regulatory, and legal obligations.

This part of ISO/IEC 24760 defines a reference architecture for an identity management system that includes key architectural elements and their interrelationships. These architectural elements are described in respect to identity management deployments models. This part of ISO/IEC 24760 specifies requirements for the design and implementation of an identity management system so that it can meet the objectives of stakeholders involved in the deployment and operation of that system.

This part of ISO/IEC 24760 is intended to provide a foundation for the implementation of other International Standards related to identity information processing such as

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

— ISO/IEC 29101, *Information technology — Security techniques — Privacy reference architecture*,

— ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*, and

— ISO/IEC 29146, *Information technology — Security techniques — A framework for access management.*

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

Part 2: Reference architecture and requirements

1 Scope

This part of ISO/IEC 24760

— provides guidelines for the implementation of systems for the management of identity information, and

— specifies requirements for the implementation and operation of a framework for identity management.

This part of ISO/IEC 24760 is applicable to any information system where information relating to identity is processed or stored.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*

3 Terms and definitions

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

3.1
documented design
authoritative description of structural, functional, and operational system aspects

Note 1 to entry: A documented design is the documentation created to serve as guidance for the implementation of an ICT system.

Note 2 to entry: A documented design typically includes the description of a concrete architecture of the ICT system.

3.2
identity management authority
entity responsible for setting and enforcing operational policies for an *identity management system* (3.3)

Note 1 to entry: An identity management authority typically commissions the design, implementation, and deployment of an identity management system.

EXAMPLE The executive management of a company deploying an identity management system in support of its services.

3.3
identity management system
mechanism comprising policies, procedures, technology, and other resources for maintaining identity information including metadata

Note 1 to entry: An identity management is typically used for identification or authentication of entities. It can be deployed to support other automated decisions based on identity information for an entity recognized in the domain of application for the identity management system.

3.4
principal
subject
entity to which identity information in an *identity management system* (3.3) pertains

Note 1 to entry: In the context of privacy protection requirements, a principal refers to a person.

3.5
invalidation
process performed in an *identity management system* (3.3) when a particular attribute is no longer valid for a particular entity to mark the attribute invalid for future use

Note 1 to entry: Invalidation of attributes may be part of updating the attribute value, for instance, with a change of address.

Note 2 to entry: Invalidation typically takes place for an attribute that is determined as no longer valid before the end of a validity period that had previously been associated with it.

Note 3 to entry: The term "revocation" is commonly used for invalidation of attributes that are credentials.

Note 4 to entry: Invalidation typically happens immediately after the determination that an attribute is no longer valid for a particular entity.

3.6
regulatory body
body tasked and empowered by law, regulation, or agreement to supervise the operation of *identity management systems* (3.3)

3.7
stakeholder
individual, team, organization, or classes thereof having an interest in a system

[SOURCE: ISO/IEC 42010]

4 Symbols and abbreviated terms

ICT Information and Communication Technology

IMS Identity management system

PII Personal identifiable information

5 Reference Architecture

5.1 General

This clause describes the architectural elements of an identity management system and their interrelationships.

The documented design for the architecture of an identity management system should be based on ISO/IEC 42010.

NOTE The reference architecture and architecture description defined in this standard are based on ISO/IEC 42010

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 in this part of ISO/IEC 24760. Business-level actors are stakeholders. Some stakeholders do not interact with the system. The documented design shall address requirements for both actor and non-actor stakeholders. The documented design shall exhaustively describe the actors.

A documented design of an identity management system conforming to this part of ISO/IEC 24760 should use an appropriate architecture description language and reference architecture components and functions by terms defined in this International Standards.

5.2 Architecture elements

5.2.1 Overview

Elements in this reference architecture are

— stakeholders (5.3.1),

— actors (5.3.2),

— views (5.3, 5.4),

— models (5.3.3, 5.3.4, 5.3.5, 5.4.1, 5.4.3),

— components (5.4.1),

— processes (5.4.2), and

— information flows and actions (5.4.2).

5.2.2 Viewpoints

5.2.2.1 General

The documented design of an identity management system shall include a context view and a functional view. It may include a physical view. The documented design may contain other views, e.g. an information view.

NOTE The required minimal set of viewpoints describes the system's interactions with its environment and the system's internal components and interactions.

The description of a view should be focused. Diagrams in the view descriptions should be accompanied with text defining the elements shown.

NOTE The description of viewpoints in this clause is based on Reference [2].

5.2.2.2 Context viewpoint

Definition — In the documented design the context viewpoint describes relationships, dependencies, and interactions between the system and its environment (the people, systems, and external entities with which it interacts).

Concerns — System scope and responsibilities, identity of external entities and services and data used, nature and characteristics of external entities, identity and responsibilities of external interfaces, nature

and characteristics of external interfaces, other external interdependencies, impact of the system on its environment, and overall completeness, consistency, and coherence.

Models — A context viewpoint may contain a context model, use cases and interaction scenarios. The context model is an informal box-and-line diagram that shows the system under discussion as a black box with interfaces, top-level interactions and dependencies on external entities. See 5.3.3.

Points to take care of — Missing or incorrect external entities, missing implicit dependencies, loose or inaccurate interface descriptions, inappropriate level of detail, scope creep, implicit or assumed context or scope, overcomplicated interactions, overuse of jargon.

5.2.2.3 Functional viewpoint

Definition — In the documented design the functional viewpoint describes the key functional elements with operational responsibilities, interfaces, and primary interactions.

Concerns — Refers to functional capabilities, external interfaces, internal structure, and functional design philosophy.

Models — A functional viewpoint may contain a component model, physical model or an infrastructure model.

In the documented design the functional viewpoint shall identify standards and guidelines applicable to each of the functions it describes.

See 5.4 for guidance on specifying a function viewpoint.

5.3 Context view

5.3.1 Stakeholders

5.3.1.1 General

This part of ISO/IEC 24760 recognizes the following direct and indirect stakeholders of primary importance

— principal,

— identity management authority,

— identity information authority,

— relying party,

— regulatory body,

— auditor, and

— consumer/citizen representative or advocate.

Each stakeholder performs a separate function in the identity management system. These functions imply specific responsibilities and liabilities. With the exception of regulatory bodies and consumer representatives, stakeholders interact with an identity management system, and thus are present in the reference architecture as actors (see 5.3.2).

Concerns of stakeholders in an identity management system are described in the following sub-clauses and should be addressed in the design, implementation and operation of the system.

5.3.1.2 Principal

Concerns of a principal in an identity management system include

— correctness of identity information collected, processed and stored,

— protection of privacy,

— minimisation of identity information collected, processed and stored by the identity management system,

— minimisation of identity information usage by the identity management system in its domain of applicability,

— errors in identification including false negative and false positive identification and the detection and handling of errors,

— knowledge of and consent to, identity information sharing with third parties,

— being correctly represented by identity information captured, processed or stored,

— correctness of operations in the delivery of services and the access to resources made available based on the attributes presented in a specific situation,

— collection, processing and storage of identity information only occurs with its informed consent,

— equitable treatment in its interactions with the system, and

— an easily understandable, effective, appropriate user interface.

NOTE a concern of a principal that relates to a third party service using identity information obtained from the identity management system is not a concern about the identity management system and therefore not in scope for this standard.

5.3.1.3 Identity management authority

Concerns of the identity management authority in an identity management system include

— definition of identity management objectives for the domain(s) served by the identity management system,

— specification of policies to maintain identity management objectives for the domain(s) served by the identity management system,

— fulfilling the business objectives of the identity management system with respect to principals and users of identity information,

— that the identity information provided by each principal is accurate and pertains to that principal to a specific level of assurance, and

— compliance with regulation.

5.3.1.4 Identity information authority

Concerns of an identity information authority in an identity management system include

— correctness of identity information,

— meeting requirements from relying parties,

— compliance with regulation, and

— meeting business obligations with principals.

5.3.1.5 Relying party

Concerns of a relying party in an identity management system include

— confidentiality, availability and integrity and applicability to a principal of identity information,

— provisioning of accurate identity information pertaining to relevant principals at the required level of assurance,

— effective, documented and secure interfaces,

— conformance to regulation applicable to its operations, and

— effective mechanism and procedures for auditing.

5.3.1.6 Regulatory body

As an external independent organization, concerns of a regulatory body in an identity management system include

— the proper documentation of operating policies,

— correctness of operation, in particular, in applying operational polices,

— proper accountability and audit of system operations,

— compliance of operational policy and operational practice with legal and regulatory requirements,

— effective reporting on system operations, including control effectiveness, incidents, and actions taken in overcoming incidents, and

— effective response to incidents that violate, or have a potential to violate privacy protection.

NOTE Effectively, auditors, as actors in an identity management system (see 5.3.2.9), in inspecting the operations of an identity management system (see 5.4) may represent the interests of regulatory bodies.

5.3.1.7 Consumer/citizen representative or advocate

Consumer/citizen advocates are individuals or groups that emerge from civil society and try to protect consumers and citizens from surveillance and lobby for improved privacy regulations.

Consumer/citizen representatives are individuals appointed by a principal or selected by consumer organisations to represent a consumer or citizen in its rights with respect to privacy.

Consumer/citizen representative and advocates' main concerns are

— transparency, notification, compliance and protection against complex legal language, and

— access of services to disadvantaged populations

NOTE 1 Consumer and citizen representatives participate in recognised multi-stakeholder societal processes such as governance and establish good practices and requirements to be met by those providing goods and services to consumers and citizens.

NOTE 2 Consumer and citizen representatives are selected, briefed and where necessary trained to ensure that they participate through reasonable and reasoned discussion, based wherever possible on good quality evidence.

5.3.2 Actors

5.3.2.1 General

An actor interacts with an identity management system to participate in identity management operations. An entity may interact with the same identity management system as multiple, different actors. The document design shall define all interactions by any actor supported by the system.

The documented design should describe actor interactions in terms of the functions that the interactions relate to. Where an actor that interacts with the identity management system needs to be authenticated before interactions are allowed to proceed, the documented design shall specify the basis for authentication (e.g. entity based; role based etc. authentication), the authentication method and the assurance level required for each interaction as defined in ISO/IEC 29115.

NOTE One purpose of specifying actors in the design of an identity management system is to be able to describe all intended interactions with the system.

A documented design may recognize the following actors:

— principal;

— identity management authority;

— identity registration authority

— relying party;

— identity information provider;

— identity information authority;

— verifier;

— auditor.

The documented design shall specify the level of assurance needed to identify and authenticate entities requesting access to identity information contained in its identity management system as specified in ISO/IEC 29115. The level of assurance may be different for different types of information and the type of access granted i.e. read, write etc. Authorization may be implemented as specified in ISO/IEC 29146.

5.3.2.2 Principal

A principal is an actor who provides identification information to establish and validate its identity within identification management processes. The Principal has the following responsibilities

— as an entity when applying to become registered in a domain of applicability, to provide accurate identity information for enrolment as a new principal,

— as system user once enrolled, to request to be recognized by the identity management system and to be approved for access to services or use of resources available in the domain of applicability associated with the identity management system, and

— as the subject of observation to obtain identity information, to facilitate the observation;.

NOTE As a subject of observation the identity information obtained is anonymous, until its relation to the principal has been established.

A principal can use an identity management system to

— request to be recognized by information in the identity management system and to be approved for access to services or use of resources available in the domain of applicability associated with the identity management system, and

— be informed, as human, of the identity information pertaining to itself is held in the identity management system and to request any errors in the identity information to be corrected

NOTE In appropriately defined circumstances, a legally authorised representative may act on behalf of a principal.

5.3.2.3 Identity management authority

An identity management authority is associated with a domain of applicability with the duty and capabilities to define and adjust business objectives for identity management in that domain and set management policies to meet these objectives.

An identity management authority uses policies to regulate the use of registered identity information. Policies may specify levels of service to provide including the level of assurance on identity information that may be provided by the identity management system. Policies may also specify how to obtain authorisation for access and modification of identity information in unforeseen circumstances.

The identity management authority shall define identity management objectives for a domain of applicability served by the identity management system operating under its authority. The identity management authority shall specify policies to meet identity management objectives for an associated domain.

Responsibilities of an identity management authority include

— to create, modify or revoke operational policies,

— to ensure legal and regulatory compliance of the policies and operation of the identity management system,

— to require and approve modification of mechanisms to establish a required level of assurance in entity authentication for access to identity information and system control functions

— to respond to incidents,

— to approve changes in the type of information recorded in the identity register

— to initiate regular audits, and

— to evaluate audit reports, in particular on the effectiveness of policies,

An identity management authority may enter into formal association with one or more other identity management authorities to form a "*federation*."

NOTE The purpose is to extend the domain of applicability for principals with the other domains of applicability in a federation. This extension is achieved with strictly controlled sharing of identity information.

In a federation, responsibilities of each identity management authority include:

— to provide a level of assurance of identity information that meets the specified requirement of any other member of the federation,

— to maintain control over access to the identity information contained in its identity management system,

— to ascertain that the level of assurance realized by any other member of the federation in authorizing access to identity information in the federated identity management systems meets its requirements for access to its own identity information,

— to operate with common policies for information sharing, and

— to specify policies to maintain its trust in the level of assurance of identity authentication.

NOTE 1 Typically, in a federation, some of the identity management policies, in particular on authorization for access, will be part of an agreement between the identity management authorities involved in the domains.

NOTE 2 Identity management policies for use in multiple domains of applicability may be established by international standards.

NOTE 3 Changes to structure, organisation and extent of a data federation may be subject to external constraints such as legal or regulatory requirements or the granting of permission by regulatory bodies.

NOTE 4 Members of a federation may agree to delegate operational responsibilities of the identity management authority to a common operator, designated as the "federation authority".

5.3.2.4 Identity registration authority

An identity registration authority is an actor in a system for identity management with the duty and capabilities to set and enforce operational policies for gathering, recording and updating identity information in the identity register.

Identity registration policies shall identify different types of modifications to identity information and the operational and security conditions under which these modifications are allowed. These policies shall specify the procedures for achieving the level of assurance in gathered identity information.

Responsibilities of an identity registration authority include

— to modify, create or revoke operational policies,

— to approve changes in the type of information recorded in the repository, and

— to approve modification of identity information recorded in the repository.

5.3.2.5 Relying party

A relying party is an actor that relies on the identity information of a particular principal provided by the identity management system. A relying party uses verified information to provide access to services and resources under its control.

The responsibilities of a relying party include

— to process and store identity information in accordance with the policies set by the identity management authority, in particular to protect privacy,

— to specify the level of assurance needed in the identity information used for access control commensurate to the value of specific services and resources, and

— to provide information on its interactions with the identity management system for auditing.

5.3.2.6 Identity information authority

An identity information authority is an actor in an identity management system to provide authoritative status to for identity information provided to relying parties. An identity information authority provides identity information on entities known in the domain. Operationally an identity information authority may be a service provider equipped to supply authoritative metadata associated with identity information. Metadata may be complemented with information to establish its reliability, e.g. cryptographic data authentication.

A domain may support one or more identity information authorities. An identity information authority may be distinct from the identity management authority. An independent service provider may act as an identity information authority.

NOTE Delegation of identity information provisioning to an independent service provider typically involves a service level agreement.

The procedures to establish an entity as identity information authority are beyond the scope of this part of ISO/IEC 24760.

The documented design of an identity management system shall specify policies with procedures and criteria to determine the level of assurance in the information that may be obtained from a particular identity information authority. The following criteria should be considered in these policies:

— quality of identity proofing;

— level of assurance of the information recorded at enrolment;

— quality of the reference identifier generator (see 5.4.2.3.3);

— quality of identity information maintenance;

— nature of the procedures used to obtain attribute values;

— syntax and semantics of attributes;

— security of the identity management system;

— qualities of the secure communication protocols used for provisioning.

The documented design of an identity management system may specify policies for adding, removing and qualifying an identity information authority as suitable in support of operating the identity management system. These policies shall address maintaining the required level of assurance when replacing a particular identity information authority with another one.

If the identity management system supports such use, the documented design of an identity management system shall specify procedures to resolve differences in the identity information for the same entity simultaneously obtained from two different identity information authorities.

5.3.2.7 Identity information provider

An identity information provider is an actor in an identity management system that provides identity information for a specific entity.

The core responsibilities of an identity information provider are

— to collect identity attributes from principals,

— ensuring that the collection of PII complies with relevant legislation and system policies,

— informing the principal about the PII to be collected, the use to which the PII will be put and any third parties that the PII will be passed to,

— obtaining the consent of the principal for the collection of PII,

— to assemble the requisite identity attributes into identity information that is used by the identity management system to identify principals,

— to format the identity information into an identity record and to store the record in the identity register of the identity management system,

— to maintain identity information in the identity register to reflect changes that may occur in the identity attributes of principals,

— to extract identity information from the identity register and provide it to relying parties, and

— to ensure that identity information passed to others is minimised removing sensitive personal data unless specifically needed and authorised within for the purpose of the processing by the party to whom the identity information is relayed.

NOTE Although the identity management authority is responsible for establishing and approving policies relevant to the above concerns, the identity information provider is responsible for implementing and operating them.

The documented design of an identity management system shall specify policies for observation, computation, generation and provisioning of identity information that define a level of assurance in the process commensurate with the level of assurance of the resulting identity information. ISO/IEC 29003 provides guidance on the processes for obtaining identity information.

An identity information provider may also create metadata describing the identity information that could include

— descriptions of the identity attribute types that comprise the identity information,

— format(s) for names of attributes and attribute values suitable for displaying to human viewers,

— details of the structure and format of identity information used by the identity management system for storage and communication,

— date and time of creation of identity information,

— date and time of expiration of validity of identity information,

— reference to the source of identity information, and

— cryptographic data used to protect the confidentiality and integrity of stored and communicated identity information and any associated metadata.

An identity information provider may create a credential to be used in authenticating the principal holding the credential. A credential may contain cryptographic data created by an identity information authority. A credential may be in the form of a physical token containing identity information that is human or machine readable.

Issuance of physical credentials is beyond the scope of this part of ISO/IEC 24760.

5.3.2.8 Verifier

A verifier is an actor in an identity management system to establish the validity, accuracy and precision of identity information as pertaining to a particular entity.

The activities of a verifier may include background checks using evidence of identity provided by the entity. If evidence of identity is supported with a credential, the verifier should establish the temporal validity of the identity information the credential contains.

An identity management system may contain multiple complementary verifiers. To avoid ambiguity in the documented design,

— an actor dedicated to checking background using provided evidence of identity should be labelled "*proofing verifier,*"

— an actor dedicated to establishing that an entity is the principal it claims to be in the course of a process of entity authentication should be labelled "*authentication verifier,*" and

— an actor primarily using authoritative identity information provided by an external identity management system should be labelled "*assertion consumer,*"

NOTE A proofing verifier is associated with the proofing process during enrolment. Its correct operation provides the foundation for the correct operation of an identity management system.

5.3.2.9 Auditor

The role of the auditor is to confirm that it is operating in accordance with its documented policies and procedures and is compliant with legal and other externally imposed requirements. The auditor reports its findings principally to the identity management authority but may also have an obligation to report findings on legal and externally imposed requirements to regulatory and other external bodies.

NOTE Auditing normally involves the examination and analysis of records of system operations and transactions and is therefore dependent on the availability of such records.

Concerns of an auditor include

— clear policy documents for the operation of the identity management system,

— availability of records of identity management information at all relevant stages of identity management transactions including collection, storage, usage, transferral and disposal of identity information, and

— clear and attainable criteria for audits.

Responsibilities of an auditor include

— as reporter, to periodically prepare statements describing the operations performed by an identity management system, in particular in respect to meeting operational policies,

— as monitor, to timely obtain reports of specific operations performed by an identity management system, to assess if the operations meet applicable policies and to alert the identity management authority of any discrepancies,

— as advisor, to advise the identity management authority on possible improvements in the operational policies and their enforcement, and

— as supervisor, to report to outside parties, including regulatory bodies, on conformance of operations to applicable policies, rules and regulations.

5.3.3 Context model

Figure 1 shows the context model for an identity management system, showing acting and non-acting stakeholders as specified in this part of ISO/IEC 24760.

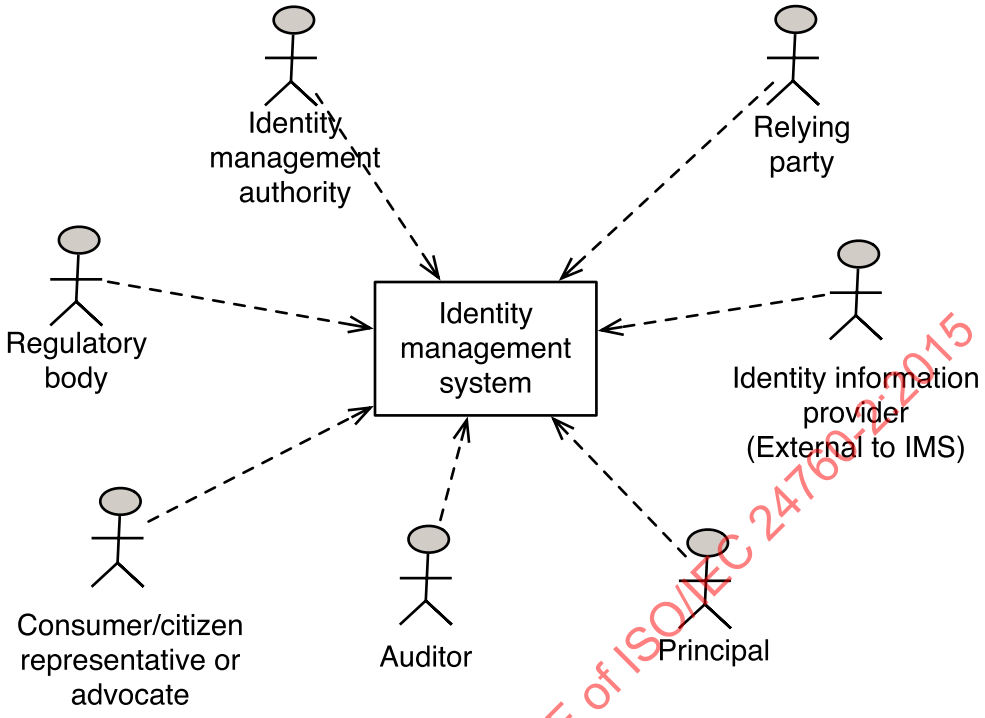

Figure 1 — Context model for identity management

The documented design shall specify concrete representations of the stakeholders and actors defined in 5.3.1 and 5.3.2, respectively. The documented design may add additional stakeholders or actors. It may specify the stakeholders and actors identified in the figure with multiple distinct representations.

5.3.4 Use case model

5.3.4.1 General

A use case model defines interactions of actors with the identity management system. It identifies functional requirements.

Figure 2 illustrates a simple use case with actors interacting with an identity management system used by a relying party to control access to services or resources in its domain of applicability. Extended use cases and related component diagrams covering the major aspects of an identity management system are included in Annex B.

Figure 2 shows:

— a principal establishing a relationship with an identity management system under the control of an identity management authority;

— a principal providing identity information to a relying part in order to obtain access to a resource;

— a relying party requesting authentication of the principal;

— a relying party requesting attributes for an authenticated principal;

— a relying party giving access to a resource under its control;

— a principal accessing a resource under control of a relying party.

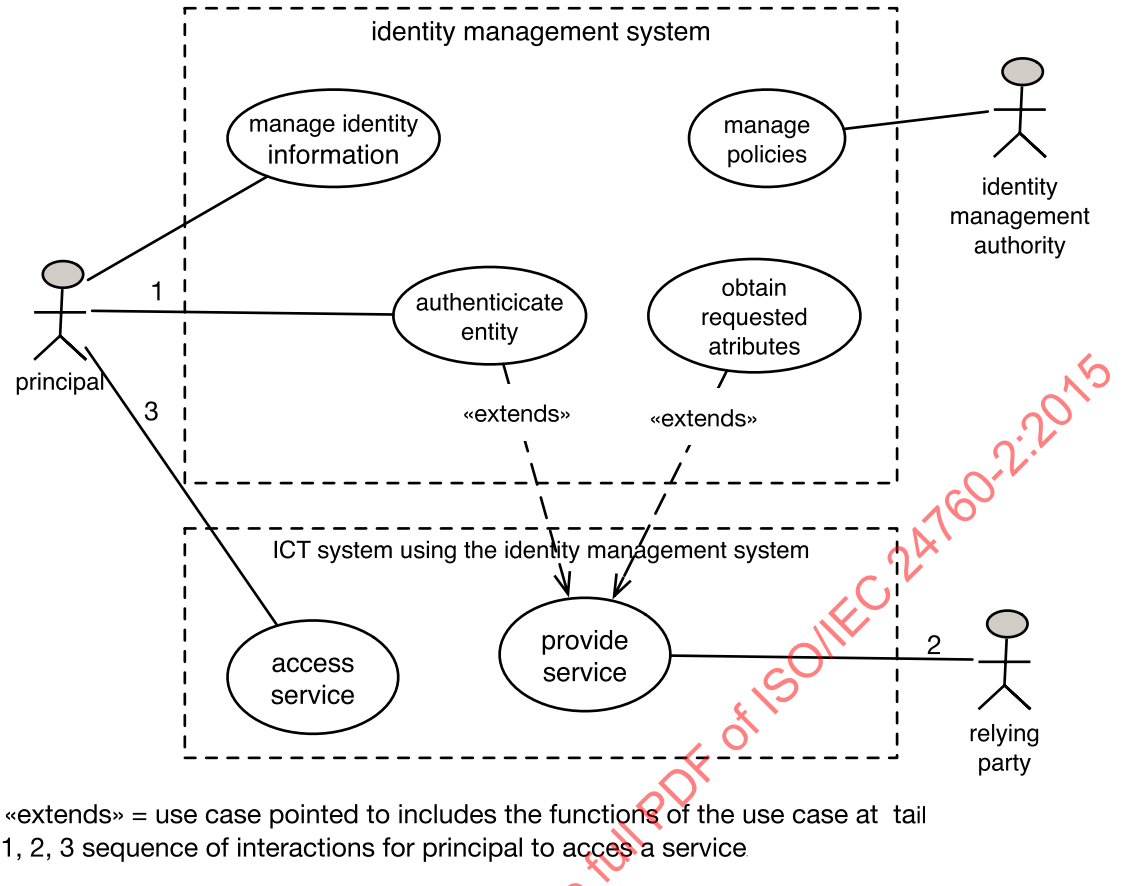

Figure 2 — Identity information baseline use case

The example use case diagram in the figure contains both administrative activity (manage identity information, manage policies) and resource access activity, which does include authentication and obtaining identity information.

To facilitate describing functional requirements from use cases, a use case and functional view may present actors as belonging to different communities. A community represents common interests in the operation of the identity management system. Communities include

— organisational users,

— administrative users, and

— non-organisational users.

Non-person entities can also make requests to access resources in IT systems, which will require authentication of the entity. Non-person entities can include devices as well as logical entities such as services and software.

5.3.4.2 Employee use cases

An employee uses the system for information retrieval. Consent for information processing and access is implicit.

Based on work duties assigned, an employee expects accurate identity information and access to identity information from the management system. From an employee point of view, the information should have been accurately acquired asserting the integrity of its origin and its maintenance.

5.3.4.3 Employer use cases

An employer has responsibilities to manage components of the system. In interactions with the identity management system, an employer can dealt with in the same way as an employee. (5.3.4.2)

From an employer point of view, the identity information should be accurately maintained and only be processed with approval.

5.3.4.4 Principal use cases

In principal use cases, unambiguous identification is most important. Access to information is either by the principal, by mandate from the principal or by commercial parties with explicit consent.

Consumer use cases describe the risks, and possible mitigation, of abuse of identity information in an identity management system for business purposes outside those identified in the documented design. To address these concerns consumer use cases typically describe aspect of compliance with legal and regulatory requirements.

The principal use case may describe a specific process for re-enrolment of an entity in order to re-establish its identity that includes processes to update identity information that any identity information stored in relying parties relating to the re-enrolled entity.

From a principal point of view, identity information should essentially be accessed in a protected manner, preventing any leakage of information. As information is collected for a specific purpose any other use should be with consent of the principal. The information should be protected from any risk of corruption and collusion.

5.3.4.5 Device use cases

Device use cases describe the use of devices as principals in an identity management system. Devices typically act on behalf of, and under the control of, other entities, which may or may not be principals. Risks of loss of physical control or compromise of device integrity may be addressed in the device use cases.

From a device point of view, identity information should be protected from risk of corruption or collusion.

5.3.5 Compliance and governance model

The compliance and governance model shows the conceptual mechanisms that can be employed to meet regulatory and other external constraints placed on an identity management system. This includes:

— to ensure accuracy of acquired identity information of managed entities at the appropriate level of assurance not only at initialization but for the full lifetime of the principal's identity information;

— to ensure uniqueness of identity information pertaining to a specific principal;

— to ensure the identity information is accurately acquired;

— to ensure that access to various types of identity information is restricted to users who are authorized to access the information type and are authenticated to an appropriate level of assurance;

— to ensure access to identity information is recorded and available for auditing;

— to prevent the processing of and the access to identity information without the principal's consent within the limits of the local, regional and global regulations;

— to comply with local, regional and global regulations, and meet conformance and governance requirements.

5.4 Functional view

5.4.1 Component model

5.4.1.1 General

The documented design of an identity management system may recognize components described below. Annex C presents a diagram showing components of an identity management system and their interactions. The documented design specifies each component needed to meet the operational requirements for concepts identified in its architecture views.

The documented design of an identity management system shall describe the operational elements of the system including stakeholders, actors, data structures, functional components and interfaces. Data structures to be defined should include

— cryptographic keys and properties, discovery services, policies and other capabilities and requirements;

— identity attribute data syntax, semantics and, where relevant, mapping rules to equivalent identity data representations in other systems;

— data structures used in for transactions, such as authentication requests, assertions and session keys.

5.4.1.2 Principal

Principals are actors in the identity management system, which access services and resources available in the domain of applicability.

Requirements for access of a principal to services and resources available in the domain of applicability are addressed in international standard ISO/IEC 29146.

5.4.1.3 Identity register

The purpose of the identity register is to provide an authoritative reference for identity information in the domain of an identity management system. An identity register may be implemented in different ways, for instance, centralized, distributed. Some identity information in an identity register may also be stored in a device that is held by the entity itself, e.g. a smart card.

The documented design of an identity management system shall specify the mechanism to control access to the identity information contained in the identity register (see 6.2).

Identity information that defines the identity of an entity may be stored in an identity register in one on more records. The partitioning of identity information into multiple records may be based on factors that could include

— differences in access conditions, e.g. to implement minimal disclosure;

— differences in the duration identity information will be retained in the identity register;

— differences in storage location, e.g. in a central repository and/or on a personal device.

The structure of the data storage for identity information and the methods of implementing an identity register and access control are beyond the scope of this document.

5.4.2 Processes and services

5.4.2.1 Documentation

The documented design should base its description of components and operations on the terminology in the tables in this clause.

The documented design should include UML diagrams to describe processes.

NOTE Diagrams in Annex C of this part of ISO/IEC 24760 can be used as templates.

The documented design may specify an implementation using components that perform a subset of the processes in these tables.

5.4.2.2 Identity information management processes

5.4.2.2.1 General

Information processing in an identity management system includes, but not limited to, the following processes

— identity information provisioning,

— identity information processing, and

— granting identity processing access.

NOTE The processes in this clause refer to identity information present in the identity register. Processes to enter identity information is not described here. See ISO/IEC 29003.

Table 1 presents an overview of information exchanged in an identity management system related to the processes described in this clause.

Table 1 — Overview of information exchanged in identity information management processes

Process	Actors			
	Source		Recipient	
	Architecture element	Action	Architecture element	Action
Identity information processing	Identity information provider	Applies information processing operations	Identity information provider	Retains results
			Register	Stores result of processing, possibly updating information in one or more identities.
Granting identity information-processing	Identity management authority	Informs on identity information processing. Solicits authorization for processing operations	Principal	Grants or denies information processing operations
	Principal	Requests information on identity processing.	Identity management authority	Provides requested information

Table 1 *(continued)*

Process	Actors			
	Source		Recipient	
	Architecture element	Action	Architecture element	Action
Provisioning	Relying party	Requests provisioning services	Identity management authority	Grants or denies provision service, specifies conditions.
			Identity information provider	Records relying party as receiver of provisioning service/
	Identity information provider	Transmits identity information	Relying party	Applies updated information to its service process.
	Identity information authority	Augments identity information with assertion on the level of assurance	Relying party	Confirms the assertions are valid and meet its requirements for level of assurance

5.4.2.2.2 Identity information maintenance

Identity information provisioning is the process of providing updated identity information pertaining to principals when an identity has been created or previously provided information is no longer correct. Access to identity information is controlled by permissions assigned to the relying party.

A documented design shall specify the procedures and conditions to initiate provisioning to a relying party.

5.4.2.2.3 Identity information provisioning

Identity information processing shall be performed according to policies. Identity information processing may generate new identity information by accessing identity information pertaining to one or more principals.

5.4.2.2.4 Granting identity processing access

Access to the identity information for identity information processing and to the information generated shall be controlled in accordance with applicable policies.

5.4.2.3 Specific identity information management processes

5.4.2.3.1 General

This clause specifies additional processes specific to different implementations of an identity management system. It includes

— auditing,

— generating reference identifiers, and

— invalidation.

Table 2 presents an overview of information exchanged in an identity management system related to the processes described in this clause.

Table 2 — Overview of information exchanged in specific identity management processes

Process	Actors			
	Source		Recipient	
	Architecture element	Action	Architecture element	Action
Auditing	Identity management authority	Defines actions to be logged, incidents to be reported.	All actors	Incorporate definitions in process implementation
	Principal	Registers complaint	Auditor	Investigates complaint
	Identity management authority	Maintains log of management actions		Reviews logs and incidents
	Identity register	Maintains log of data access operations		
	Identity information provider	Maintains log of identity information requests and information provisioning activities		
	Identity information authority	Maintains log of assurance assertions provided Reports on incidents		
	Auditor	Reports on findings. Recommends changes.	Identity management authority	Adjust policies and procedures to implement any recommended changes.
Generating reference identifier	Identity information provider	Requests reference identifier	Reference identifier generator	Generates reference identifier
	Principal	Provides identity information to be used as reference identifier	Reference identifier generator	Validates suitability of provided identity information as reference identifier. Generates reference identifier.
	Reference identifier generator	Provides generated reference identifier.	Identity information provider	Associates reference identifier with other identity information
Identity information invalidation	Auditor	Reports on findings. Recommends change.	Identity management authority	Approves invalidation
	Principals	Identifies error	Identity information provider	Correct information
	Identity information provider	Informs on change	Principals	Confirm and validate change notification
			Relying party	Confirms change notification

5.4.2.3.2 Auditing

Actors and components should be audited over time for their correctness of operating in their role in the identity management framework:

— the identity register and the identity reference generator should be continuously audited for the accuracy of their integrity controls;

— the identity information provider should be audited on a regular basis for the accuracy of their control procedures in providing identity information;

— the identity information authority should be audited on a regular basis for the accuracy of their control procedures in managing identity information.

Auditors should be certified through an accredited control process for their reviews of the identity management framework actors and components.

5.4.2.3.3 Generating reference identifiers

As part of the identity registration a reference identifier is created and associated to the identity information of the related entity. The identity reference generator is invoked with any available identity information needed and it produces an identifier value. The reference identifier is recorded with the other identity information in the identity register.

5.4.2.3.4 Invalidation

The documented design of an identity management system may specify the conditions and procedures for invalidation of identity information.

NOTE Invalidation of identity information implies the invalidation of any provable statements, e.g. with cryptography, on the validity of the identity information that may have been recorded by the user of that information. In practice, deleting the provable statement has the effect of invalidating the information.

The following conditions may be considered:

— identity evidence has been found incorrectly assessed as valid, either fraudulently or by incorrect procedures;

— errors have been found in assigning or recognizing attributes;

— changes occurred to policies for enrolment or identification;

— the principal's identity information has been used by someone else in a manner that requires re-establishment of a new set of identification information.

The invalidation mechanism, if supported, shall be done in accordance with an invalidation policy. This policy should address:

— conditions and mechanisms for provisioning an invalidation;

— the level of assurance for the invalidation message;

— conditions and mechanisms for advising a principal of the invalidation of an attribute in one of its identities;

— mechanisms to respond to requests on the invalidation status of an attribute.

5.4.2.4 Additional functions

5.4.2.4.1 General

The documented design of an identity management system may specify additional functions as described in this clause. These include

— identity information profiling,

— consent,

— identity authority discovery, and

— publication.

Table 3 presents an overview of information exchanged in an identity management system related to the processes described in this clause.

Table 3 — Overview of information exchanged in additional identity management system functions

Process	Actors			
	Source		Recipient	
	Architecture element	Action	Architecture element	Action
Identity information profiling	Identity information provider	Defines profile for entity type	Identity information provider	Implements identity profile
Privacy consent	Principal	Requests identity information attribute to be review or to be hidden	Identity information provider	Verifies policy for request, implement change accordingly, submit information
Identity authority discovery	Identity registration authority	Requests trust establishment with other identity authority	Relying party	Verifies trust request eligibility
	Relying party	Submits trust request	Identity information authority	Validates trust establishment
	Identity information authority	Approves identity information delivery	Identity information provider	Delivers identity information
Publication	Identity management authority	Establishes publication policy	Identity information authority	Validates publication policy
	Identity information provider	Implements validated publication policy	Relying party	Receives published information

5.4.2.4.2 Identity information profile service

An identity information profile service provides an appropriate representation of identity information for entities of a given type, i.e. human, device, and organizational entities. This may involve the definition, maintenance, and use of different identity attributes and identity data formats for the various entity types.

5.4.2.4.3 Consent

A privacy consent process may provide functions:

— to authenticate an entity as a known and authorized principal for access to identity information;

— to present recorded identity information;

— to modify, extend or remove identity information previously provided by the principal;

— to request modification of generated identity information;

— to notify a principal of intended use of identity information.

5.4.2.4.4 Identity information authority discovery

An identity information authority discovery process provides the capability of discovering other identity information authorities and establishing collaboration for identity information access at the required level of assurance.

This service identifies third party identity information authority candidates and conditions the subscription and notification processes with these authorities.

An identity information authority discovery service may provide functions

— to approve another identity information authority to establish trust relationship based on established requirements from the quality and compliance component,

— to accept an entity as an allowed subscriber of identity information,

— to specify the type of identity information needed,

— to specify the required level of assurance in accessing identity information,

— to specify security mechanisms to protect identity information being provided,

— to specify an identifier for which notification of identity information is needed,

— to receive identity information as requested, and

— to receive identity information when such information changes.

The list of functions the discovery service may include depends on the established trust with the other authority and the conditions of that trust.

5.4.2.4.5 Publication

A publication process provides the capability of publishing identity information to service requesters and establishing collaboration for identity information access at the required level of assurance. Subscription and notification services are also part of the publication service.

A publication service may provide functions:

— to publish and modify publication of the service of identity information provisioning and the condition of the access and the use of this information;

— to accept a requester to be provided with identity information based on established requirements from the quality and compliance component;

— to accept an entity as subscriber of identity information;

— to specify the type of identity information to which access is allowed;

— to specify the required level of assurance in accessing identity information;

— to specify security mechanisms to protect identity information being provided;

— to specify an identifier for which notification of identity information is needed;

— to inform on identity information changes when it occurs.

The list of functions the publication service may include depends on the requirements for accessing this information.

5.4.3 Physical model

This view describes the implementation of each of the elements in the identity management systems that provide the functionality to implement the process view. A physical view may present alternative physical implementations, e.g. differing in cost and performance.

This part of ISO/IEC 24760 addresses the physical view only at the level of structural components. Implementation aspects of the physical view are beyond the scope of this part of ISO/IEC 24760.

5.5 Identity management scenarios

5.5.1 General

An identity management system may be deployed according to various scenarios. A deployment scenario impacts governance of the identity management system. The deployment scenario will determine the trust relationships that need to exist between parties involved in operating and governing the identity management system.

A deployment scenario may be chosen when extending an existing identity management system. An extension deployment model may be different from the original deployment model.

The different scenarios that may be used to implement an identity management system include

— the enterprise scenario,

— the federated scenario,

— the service scenario, and

— the heterogeneous scenario.

5.5.2 Enterprise scenario

With an enterprise scenario an identity management system is deployed in the context of a single organization where trust in its operations and governance is inherited from the organization's governance structure and the organisation is responsible for managing the information collected, stored and processed by the system.

An enterprise model is a centralized model (see ISO/IEC 24760-1).

5.5.3 Federated scenario

A federated identity management system comprises multiple subsystems, with independent governance of the sub systems. Trust in operations, and governance of the federation is established through negotiated agreement. Governance may be delegated to an organization with a formal structure or statute, which contains operating rules, responsibilities and defined liabilities for participating members.

When a domain of applicability needs to be extended in order to interface to or collaborate with other domains, a centralized scenario approach would merge the original domains into a single larger domain controlled by a single identity management system. A federated scenario offers an alternative approach

allowing the identity management systems to exchange identity information between domains without requiring the domains to be merged.

NOTE Full system integration imposes an integration of the requirements of the two domains in one new architectural approach, supporting all the different architectural views of the two separated domains. The federated model will instead leave the structure unchanged, but will bring new mechanisms intended to allow the separate structures to communicate with each other.

Mechanisms to support federation shall provide the required level of confidentiality, of integrity, and of trust between separated domains in order for them to exchange identity information, and to use identity information of other domains.

5.5.4 Service scenario

Irrespective of the deployment scenario, enterprise or federated, functional components in an identity management system may be realised as services.

The documented design of an identity management system deployed as service model shall specify the trust and publication components and the mechanisms to ensure that the required level of confidentiality, integrity, and trust is achieved when providing an identity information service.

5.5.5 Heterogeneous scenario

A heterogeneous scenario is one where independent organisations issue identity credentials for principals that conform to a known specification and level of assurance. Relying parties may use the credentials to authenticate principals where the attendant risk is deemed acceptable under their risk management policy.

6 Requirements for the management of identity information

6.1 General

This clause describes the requirements for the management of identity information by an identity management system based upon the reference model and the types of deployment and stakeholders involved. This clause distinguishes *functional requirements* to support actors' interactions with the system, and *non-functional requirements* that pertain to other operational conditions an identity management system may have to respect.

Functional requirements include:

— access policy;

— management conditions;

— maintenance conditions.

The requirements in this clause do not include controls that are part of the practice (see ISO/IEC 24760-3).

6.2 Access policy for identity information

The documented design of an identity management system shall provide an information access policy to specify:

— conditions and mechanisms to access the value of each attribute in the system;

— criteria for authorization of access with appropriate levels of assurance;

— which operations of access to identity information needs to be logged, and with what details;

— how the identity register enforces the protection of identity information it contains;

— duration of retention of records of identity information access.

6.3 Functional requirements for management of identity information

6.3.1 Policy for identity information life cycle

The documented design for an identity management system shall provide a policy for managing the identity information lifecycle, which specifies

— assurance requirements for the accuracy of the identity information required for enrolment,

— conditions and procedure to activate an identity,

— conditions and procedure to maintain an identity for example checking accuracy and correctness of identity information,

— conditions and procedure to perform adjustment of identity information for a principal,

— conditions and procedure to suspend an identity,

— conditions and procedure for identification to reactivate an identity,

— conditions and procedure to delete or archive an identity,

— conditions and procedure for maintaining information,

— conditions and procedure to restore an identity,

— information to archive, and period of archival and conditions of retention for an archived identity, and

— conditions and procedure to terminate or delete an identity.

6.3.2 Conditions and procedure to maintain identity information

The documented design of an identity management system shall specify how the accuracy of the identity information it manages is maintained.

The documented design of an identity management system shall include procedures to monitor the quality of identity information in the identity register in particular for attributes that:

— represent aspects of an entity that may change over time;

— may affect the degree of trust of the recorded information.

The documented design of an identity management system shall provide policies for actions on detecting changes in identity information in particular for attributes that may change in value over time and where the change may affect the level of assurance of the registered identity.

The documented design of an identity management system shall provide policies to maintain the integrity of the identity information and metadata in the identity register. Such policies may specify

— procedures to prevent corruption of registered information,

— procedures to detect corruption of registered information, and

— procedures to correct corruption of registered information.

The documented design of an identity management system shall provide a mechanism for relying parties to report fraudulent or suspicious behaviour to the identity register.

6.3.3 Identity information interface

An identity management system may contain components with a user interface to present identity information. Access to identity information at a user interface shall be governed by a policy specifying

— access control and

— auditing.

The purposes of the information presentation interface include

— presenting identity information,

— presenting identity information metadata,

— presenting information on on-going and past system operations,

— providing controls to process or modify presented information, and

— applying policies of use for the presented information relevant for the actor.

The documented design of an identity management system shall specify the format and conditions for the presentation of identity information in human readable form (see 6.2). Requirements in the documented design on the representation of identity information in human accessible form shall take into account the capabilities and restrictions of the user of the information.

6.3.4 Reference identifier

An identity management system may contain a component to generate a reference identifier. The task of a reference identifier is to assure that a specified identity known in an identity information system is unique.

Access to the value of a reference identifier may be restricted, e.g. exclusively from within the identity management system. The documented design shall specify the access policy for the reference identifier.

NOTE Restricted access to a reference identifier prevents it from being used in other identity management systems.

The documented design of an identity management system shall associate its identity register with a reference-identifier generator. The reference-identifier generator shall generate a unique value for each principal of which identity information is stored in the identity register.

NOTE 1 Typically the reference identifier is generated when an entity enrols with a domain.

NOTE 2 The reference identifier generated may be based on information obtained from the entity, e.g. a chosen pseudonym, which has been checked for uniqueness

NOTE 3 The reference identifier may be generated from identity information for the same principal obtained from another domain in which the principal is enrolled. This may include the reference identifier from the other domain.

While the precise mechanism to generate unique attribute values is beyond the scope of this document, the design of a reference-identifier generator shall specify:

— the algorithm used to generate a unique value together with an argued description of its suitability;

— the interface to obtain a new value for either a new entity or an existing entity, in a way that maintains uniqueness;

— requirements for the input, if any, needed by the algorithm;

— if logging is supported, the requirements for logging the generation of a reference identifier;

— the security measures protecting operations of the (ICT) system that hosts the reference-identifier generator.

NOTE 1 Where there is no connection or reliable communication between domains, each domain will generate its own reference identifier and the probability of the same identifier being generated for the same or a different principal enrolled in multiple domains would be expected to be very small.

NOTE 2 In general the value of an identifier with an originating domain that is unrelated to the identity management system cannot be guaranteed to meet the criteria for a new reference identifier and is unsuitable to be used directly. However, when it is known how the reference identifier in a particular unrelated domain has been constructed, e.g. in accordance with an international standard, such a reference identifier value could be used provided its value can be reliably obtained.

If an identity management system supports logging of the reference identifier generator operations the log entry should contain

— the reference identifier generated,

— the authorization for initiating the generation of the identifier,

— any data provided as input, and

— a time stamp.

A reference-identifier generator may be configured to generate reference identifiers intended for use outside its domain of origin. In this case,

— the value of the reference identifier shall be made available in a manner to assure its integrity,

— if the value of the reference identifier is available in electronic form access to it shall be controlled to protect privacy of the principal,

— care should be given to ensure the uniqueness of this reference identifier for each different entity in the external domains where the reference identifier is also used,

— information should be made available to assess the level of assurance for the uniqueness of the value, and

— care should also be given to the possible restrictions, (e.g. legal and regulatory) and disadvantages of applying to some reference identifier types outside of their domain, such as some state references or privacy related references.

6.3.5 Identity information quality and compliance

The documented design of an identity management system shall specify functional components for quality and compliance that verify that obtained identity information is processed with adequate controls and in compliance with

— applicable policies,

— processes and organisation to keep information updated over time,

— processes for dealing with false positive identification,

— processes for dealing with false negative identification

— business requirements, and

— local, regional, and global regulations.

6.3.6 Archiving information

The documented design of an identity management system shall provide policies to specify the conditions and procedures to archive identity information.

Archived identity information shall be anonymous, either by active anonymizing or by eliminating identifying information.

6.3.7 Terminating and deleting identity information

The documented design of an identity management system shall provide policies to specify the conditions and procedures to initiate deletion of identity information by

— the principal or an entity authorised to act on behalf of the principal,

— the system, after expiration of the retention period for an archived identity, or

— the identity management authority.

The deleted identity information shall be recorded to support appeal and audit. This record shall specify the initiator and reason of deletion and any other metadata specified by the deletion policies. A record of deleted identity information shall be deleted within a period after creation as specified in the deletion policy.

NOTE A typical implementation of deletion involves the archiving of the identity information for a transitional period to allow for the time needed to complete deletion.

Deletion of all identity information for a principal shall expunge any information that can continue to identify the principal and that is under control of the identity management authority, e.g. contained in log files, audit trails or backups, which might also be stored off-site. Deletion should not be considered completed until such additional information has been deleted

In a centralised model, if an identity management system performs automatic provisioning, any relying party that has stored previously received identity information shall be notified of the information deletion. Upon receipt of the information deletion notification the relying party shall remove any information that associates the principal with the notifying domain. In this case the delete life cycle transition shall not be considered complete until confirmation has been received of the removal of the associations.

NOTE A relying party notified of information deletion may retain identity information for the principal it maintains that does not depend on the relation of the principal with the notifying domain.

6.4 Non-functional requirements

Non-functional requirements specify aspects of an identity management system that do not follow directly from functional, logical or physical views. Details of non-functional requirements are beyond the scope of this part of ISO/IEC 24760.

However, meeting one or more of the following non-functional requirements may be essential for most deployed identity management systems:

— availability;

— integrity controls;

— performance;

— privacy assurance;

— usability of access;

— liability and its representation on the technical level;

— time reference controls;

— compliance constraints from contractual, regulatory (local, regional and global), and organizational aspects (see Annex A).

The documented design of an identity management system shall specify how its implementation conforms to ISO/IEC 27002 to meet the availability and response time requirements of the relying parties, protect data integrity and, where required, implement controls to ensure that the confidentiality of sensitive information is protected and privacy requirements are met.

Annex A
(informative)

Legal and regulatory aspects

An identity management system needs to comply with legal requirements. In general such requirements demand that such a system is used for stated and authorized purposes. For example, regulations and laws concerning corporate governance, telecommunications, health care and money laundering may contain requirements affecting identity management.

An identity management authority should keep abreast of regulations and laws that may affect its identity management system requirements.

Regulatory and legal requirements to consider include:

— identification of the entity responsible for specifying identity management requirements;

— specification of identity information and information handling policies (see 6.2);

— specification of purpose for which identity information is permitted to be used;

— domain(s) of applicability outside the domain of origin where specific identity information may be used;

— life cycle management of an identity (see 6.3);

— identification of the identity management authority of the domain of origin where identity information has been established (see 5.3.2.7);

— identity proofing requirements (including protection of information collected in the identity proofing process) and reporting requirements in cases where identity proofing detects invalid identity information;

— identification of the entity responsible for the maintenance of the content of any identity register;

— security aspects of physical credentials, in particular, those intended for use in authentication.

Annex B
(informative)

Use case model

This annex presents a more detailed model with a sample decomposition of the elements of the reference architecture. This decomposition includes the actors described in Table B.1.

Table B.1 — Actors presented in use case diagram

Actor	Details
Identity management system operator	Entity responsible for enforcing identity management policies, managing system-wide configuration data, providing day-to-day operational support. NOTE In an identity federation this role may be called "federation operator".
Identity Assertion Provider	The identity assertion provider has the responsibility to corroborate the authentication and/or attributes. It operates a verifier and may access the identity register. A Relying Party can delegate authentication and/or attribute provisioning to an identity assertion provider. The identity assertion provider authenticates the claimant and/or obtains data from an identity registry to assert identity information. Thereby an identity management system can provide authentication services, attribute services or both to a relying party.
Identity Authority	An actor that can make provable statements on the validity and/or correctness of one or more attribute values in an identity. An identity information authority is typically associated with the domain, for instance the domain of origin, in which the attributes, which the identity authority can make assertions on, have a particular significance. The actor combines an identity information authority and a credential service provider.
Credential Service Provider (CSP)	Trusted actor that issues and/or manages credentials. In this context the role of the CSP is limited to the issuance of credentials to be used for entity authentication.

The purpose of a description of use cases is to represent the contract between an actor and the system, identifying the interactions available to the actor. The actor initiates an interaction with the system to achieve a well-defined goal and each use case describes the system's behaviour in its response.

A use case can also be described using stories, sequence diagrams and other formalised notation, which would allow specifying further details of the interaction with the system. The use case model presented in this annex is a high level presentation that only comprises case diagrams complemented, as an example, with a short formalised description for the "*authenticate entity*" use case.

The description of use cases can be refined to expose further details, typically presented at multiple levels of abstraction. The use case description of a lower level of abstraction may introduce additional actors for subsystems and such actors are inside the system boundary.

The use case shown in Figure B.1 describes two main use cases in an identity management system:

a) access to a protected resource;

b) delivery of a message to be authenticated.

The use case model in Table B.2 describes internal actors of an identity management system in Table B.1 to show use cases with a more detailed granularity.

Table B.2 — Summary definition of uses cases for an identity management system

Use Case	Description
access service	A principal wants access to a resource accessible after entity authentication.
authenticate entity	Activity to authenticate a principal in an on-line transaction.
authenticate message	Activity to authenticate the sender of a message.
consume message	Receiving a message and authenticating the sender.
manage consent	Grant, review and revoke consent to use identity information for authentication for resource access.
manage credential	Activities related to the creation, revocation and renewal of credentials, often includes managing hardware credentials.
manage metadata	Manage configuration data of identity assertion providers and relying parties in a machine readable, trustworthy and interoperable way. This includes technical parameters like addressing and cryptographic keys.
manage principal life cycle	Enrol, update, archive and purge identity information
manage policy	Specify the policy and procedures to operate and maintain the identity management system.
obtain requested attributes	Obtain attributes for an authenticated principal needed to authorize its requested access to a service
provide service	The relying party provides resources that need authorised access.
provision service	Provide a relying party with identity information about principals.
send authenticated message	Send a document, web-service request and the like. There is no direct response in the process or transaction. Examples: a) A company submits a signed document with the balance sheet it is obliged to provide to a bank for keeping up the credit limit. Technically the method uses file upload as anonymous user. Similar business cases are citizens applying from some government action with an electronically signed form. b) A sender delivers asynchronous, signed message, e.g. as specified in SOAP, to a service.

The UML use case notation can be thought as a graphical table of contents for the use case set. Its elements are:

- **Ellipse**: a specific use case
- **Stick figure**: an actor (in the sense of a role, not a specific person)
- **Line** between actor and use case: the „use“ relationship
- (Dashed) **rectangular box**: system boundary
- «Include» **arrow**. A use case includes the behaviour of the pointed-to one, like a program calls a subroutine
- «Extend» **arrow**. The pointed-to use case defines how and when behaviour from another one is included.
- The **arrow** with the **triangle** is pointing from a more specific element (actor, use case) to a more generalized one.
- The **dashed line** with one arrow a general dependency of use cases.

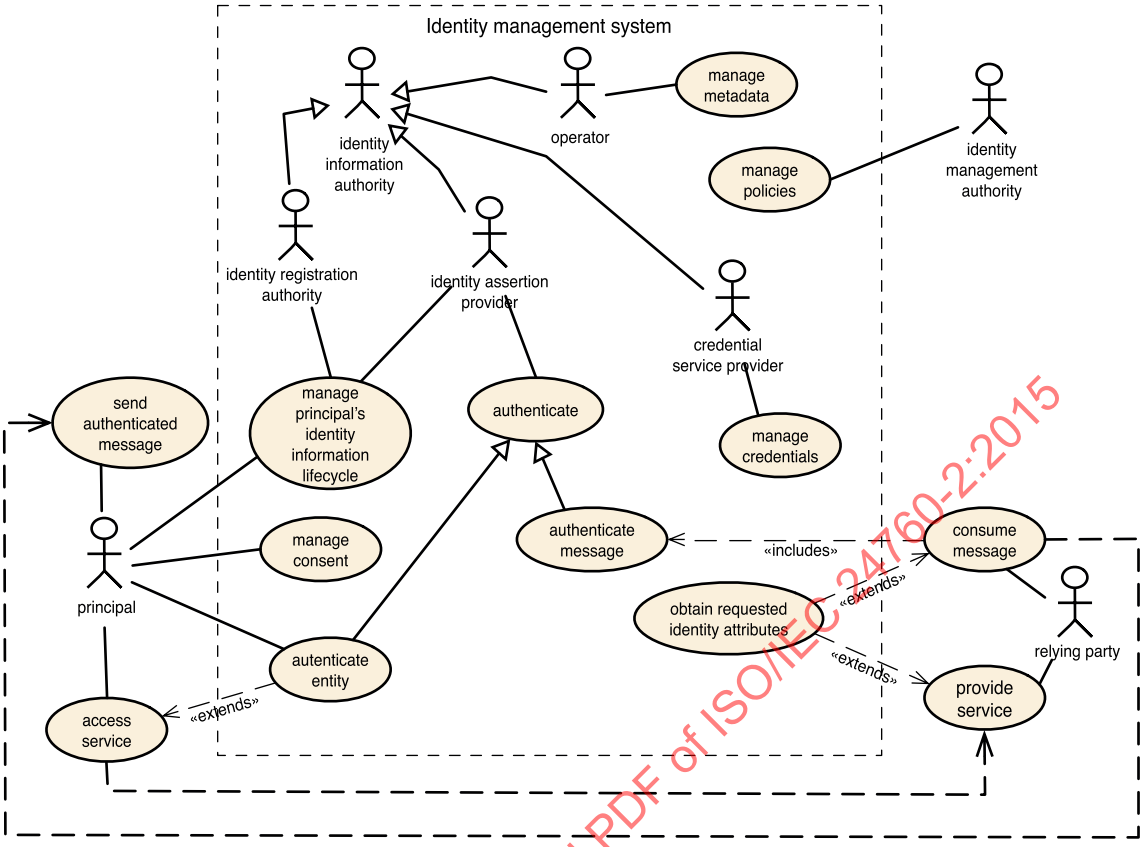

Figure B.1 — Exemplary use case diagram for an identity management system

Use case name: Authenticate Entity

Primary actor: Principal

Scope : Summary

Stakeholders with interests :

- **Principal**—To provide identification data to the service only if the service protects its privacy—to be able to use the service without registration and cumbersome authentication;
- **Relying party**—Provide a low threshold for principals to use the service the first time and the following visits —Obtain sufficient confidence in the principal's right to use the service —comply to laws and regulations;
- **Identity management authority**—supervise the compliance to the system's rules and procedures.

Precondition:

Actor has enrolled in the system and is truly a principal.

Success guarantees: Principal authenticated and the identity assertion is consumed by the relying party.

Trigger: Principal attempts to access service at the relying party and has not yet been authenticated.

Main success scenario :

1. Service access triggers a request for authentication;
2. Principal performs authentication interaction;

Figure B.2 — Example formalized use case description

Annex C
(informative)

Component model

C.1 Model

This Annex further expands the example presented in Annex B and presents, in Figure C.1, functional components of an identity management system. The presented components are sufficient to implement the extended use cases presented in Annex D. The figure uses UML,[3] Section C.2 provides a legend for symbols used in the diagram.

This component diagram shows pieces of the system as organized at runtime. This includes dependencies and interfaces. Table C.1 summarizes the components shown.

Table C.1 — Functional components of an identity management system

Name	Description
Principal and Credential Management	Subsystem to handle the principal and credential management life cycle.
Metadata Management	This component stores metadata and provides facilities to maintain and publish it. It needs to have a security level equal or better that a system using metadata.
Service Provisioning Agent	This component pushes identity information to a service, e.g. relying party.
Relying Service	A service operated provided under control of a relying party. Providing access to services is often the primary objective for an identity management system. Therefore there is a value in specifying interfaces and communicating them early in purchase or development activities for relying services.
Import/Export	This component that can be implemented with source-specific scripts, meta directory software or other interfaces.
Audit Repository	This component stores a log of operational events for auditing. It provides access to the audit log in a controlled manner.
Identity Management System	This component represents the technical infrastructure of an identity management system as a whole.
Identity Register	Repository of consolidated identity information for a domain. This may be a physical storage like a directory, database, or smart card, or a virtual one, like in a virtual directory.
Trust Root	Typically, cryptographic security for information handled in an identity management system use public key protocols based on certificates for public keys used by the system. A public key certificate is provisioned out-of-band.

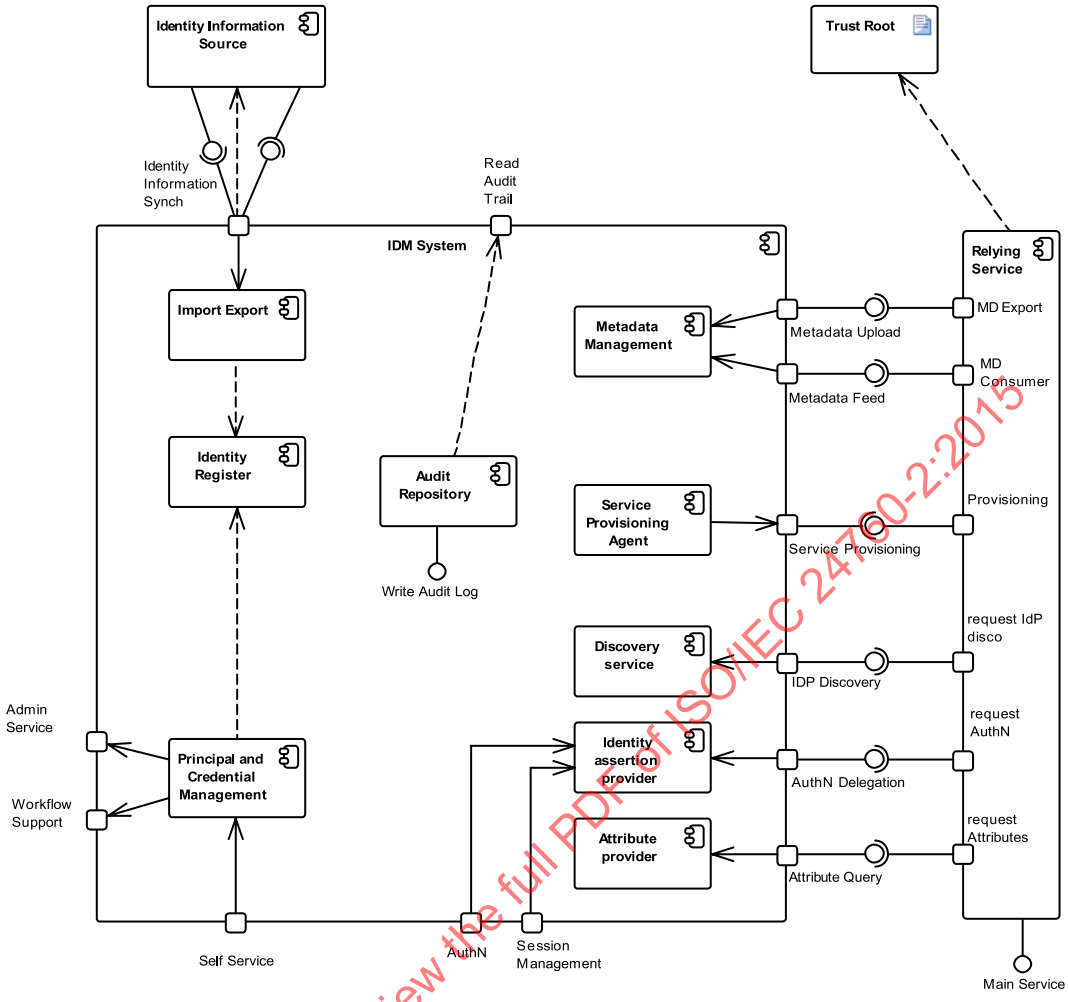

Figure C.1 — Functional components in an identity management system

C.2 UML legend

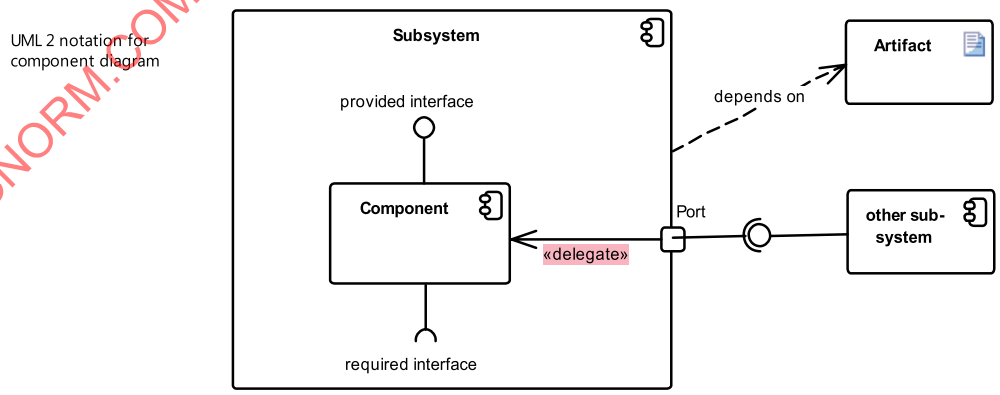

Figure C.2 — Graphical elements in a UML component diagram

Table C.2 — UML component diagram terminology

Symbol	Details
Artefact	An Artefact is any physical piece of information used or produced by a system.
Component	A component represents a modular part of a system that encapsulates its contents and whose manifestation is replaceable within its environment. A component defines its behaviour in terms of provided and required interfaces.
Port	Ports define the interaction between a component and its environment. It can have multiple interfaces controlling this interaction. Ports appear on a boundary of a component.
Provided interface	An interface is a specification of behaviour (or contract) that implementers agree to meet. A component implements behaviour using a provided interface.
Required interface	An interface is a specification of behaviour (or contract) that implementers agree to meet. A component relies on such behaviour using a required interface.
Subsystem	A subsystem is depicted as a component of a larger set of systems.

Annex D
(informative)

Business Process model

D.1 General

This annex further expands the example presented in Annex B with an exemplary description of a business process. A business process is a collection of related, structured activities or tasks that produce a specific service or product (serve a particular goal) for a particular customer or group of customers.

In a documented design a business process model provides descriptions of information and control flows, events, goals and outputs to support detailed description of use cases.

This annex presents business model diagrams using extended UML.[4]

D.2 Consent management

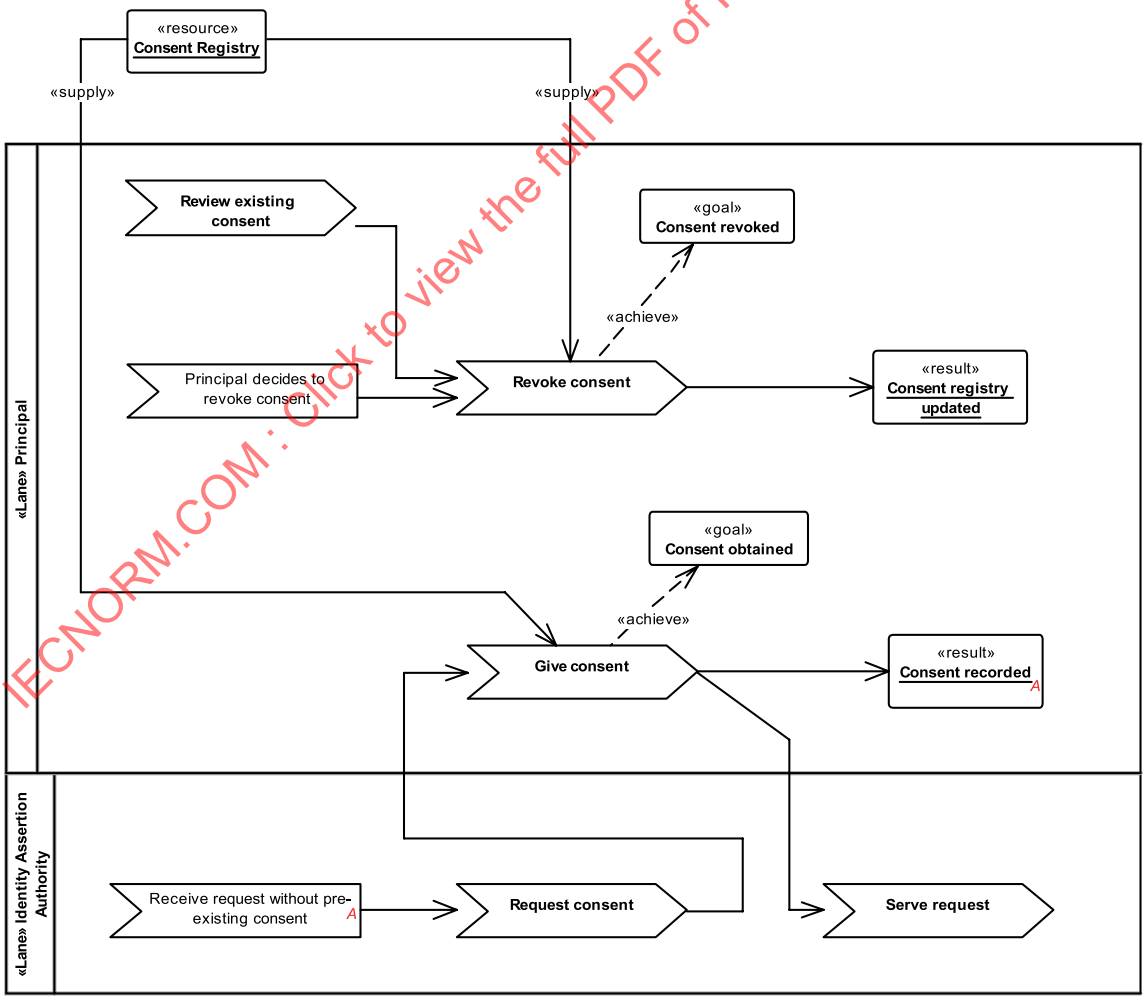

Figure D.1 — Process diagram for consent management