



ISO/IEC JTC 1/SC 27 **N14302**

ISO/IEC JTC 1/SC 27WG 5 **N514302**

REPLACES: N14150

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

**Information technology - Security techniques**

**Secretariat: DIN, Germany**

**DOC TYPE:** text for DIS LB

**TITLE:** Text for ISO/IEC DIS 24760-2:2014-07-07(E) – Information technology – Security techniques – A framework for identity management — Part 2: Reference architecture and requirements

**SOURCE:** ITTF

**DATE:** 2014-07-17

**PROJECT:** 1.27.50.02 (24760-2)

**STATUS:** This document is currently undergoing a 3-month DIS letter ballot at the JTC 1 level. The P-members of JTC 1 and SC 27 are kindly requested to submit their votes on ISO/IEC DIS 24760-2:2014-07-07(E) directly to the ISO Central Secretariat via the ISO e-balloting application by 2014-10-07. It is circulated within SC 27 for information.

**ACTION ID:** LB

**DUE DATE:** 2014-10-07

**DISTRIBUTION:** P-, O, and L-Members

L. Rajchel, JTC 1 Secretariat

H. Cuschieri, B. Garcia, ITTF

W. Fumy, SC 27 Chairman

M. De Soete, SC 27 Vice-Chair

E. J. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenber, WG-Convenors

E. de Jong, J. F. Carvajal Vion, Ch. Sténu, Project co-editors, Project co-editors

**MEDIUM:** <http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

**NO. OF PAGES:** 1 + 53 + attachment 1

# DRAFT INTERNATIONAL STANDARD

## ISO/IEC DIS 24760-2

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:  
**2014-07-07**

Voting terminates on:  
**2014-10-07**

---

---

## 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*

ICS: 35.040

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.



---

---

Reference number  
ISO/IEC DIS 24760-2:2014(E)

© ISO/IEC 2014

### **Copyright notice**

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to either ISO at the address below or ISO's member body in the country of the requester.

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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

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

Violators may be prosecuted.

<b>Contents</b>	<b>Page</b>
<b>Foreword .....</b>	<b>vi</b>
<b>Introduction.....</b>	<b>vii</b>
<b>1. Scope .....</b>	<b>1</b>
<b>2. Normative references .....</b>	<b>1</b>
<b>3. Terms and definitions.....</b>	<b>1</b>
<b>4. Symbols and abbreviated terms .....</b>	<b>4</b>
<b>5. Reference Architecture.....</b>	<b>5</b>
<b>5.1 General.....</b>	<b>5</b>
<b>5.2 Architecture elements .....</b>	<b>5</b>
5.2.1 Overview.....	5
5.2.2 Viewpoints .....	5
<b>5.3 Context view .....</b>	<b>6</b>
5.3.1 Stakeholders.....	6
5.3.2 Actors .....	8
5.3.3 Context model.....	13
5.3.4 Use case model.....	14
5.3.5 Compliance and governance model .....	15
<b>5.4 Functional view .....</b>	<b>16</b>
5.4.1 Component model .....	16
5.4.2 Processes and services .....	17
5.4.3 Physical model.....	22
<b>5.5 Identity management scenarios.....</b>	<b>22</b>
5.5.1 General.....	22
5.5.2 Enterprise scenario.....	22
5.5.3 Federated scenario.....	23
5.5.4 Service scenario .....	23
5.5.5 Heterogeneous scenario.....	23
<b>6. Requirements .....</b>	<b>23</b>
<b>6.1 General.....</b>	<b>23</b>
<b>6.2 Access policy for identity information .....</b>	<b>24</b>
<b>6.3 Functional requirements for management of identity information.....</b>	<b>24</b>
6.3.1 Policy for identity information life cycle .....	24
6.3.2 Conditions and procedure to maintain identity information .....	24
6.3.3 Identity information presentation.....	25
6.3.4 Reference identifier.....	25
6.3.5 Identity information quality and compliance .....	26
6.3.6 Archiving information .....	26
6.3.7 Terminating and deleting identity information .....	27
<b>6.4 Non functional requirements .....</b>	<b>27</b>
<b>Annex A Legal and regulatory aspects (Informative).....</b>	<b>29</b>
<b>Annex B Use case model (Informative) .....</b>	<b>30</b>
<b>Annex C Component model (Informative) .....</b>	<b>33</b>
<b>C.1 Model .....</b>	<b>33</b>

<b>C.2</b>	<b>UML legend .....</b>	<b>34</b>
	<b>Annex D Business Process model (Informative) .....</b>	<b>36</b>
<b>D.1</b>	<b>General .....</b>	<b>36</b>
<b>D.2</b>	<b>Consent management. ....</b>	<b>36</b>
<b>D.3</b>	<b>Credential lifecycle management.....</b>	<b>38</b>
<b>D.4</b>	<b>Configuration Data Management .....</b>	<b>39</b>
<b>D.5</b>	<b>Policy Management .....</b>	<b>40</b>
<b>D.6</b>	<b>Principal's Life Cycle Management.....</b>	<b>41</b>

## Figures

Figure 1 Context model for identity management. ....	13
Figure 3 Identity information baseline use case.....	14
Figure 5: Exemplary <i>use case diagram</i> for an identity management system.....	32
Figure 7: Functional components in an identity management system. ....	34
Figure 9: Graphical elements in a UML component diagram.....	34
Figure 10: Process diagram for consent management. ....	36
Figure 11: Process diagram for credential lifecycle management. ....	38
Figure 12: Process diagram for configuration data management .....	39
Figure 13: Process diagram for policy and compliance management. ....	40
Figure 14: Process diagram for principal's lifecycle management. ....	42
Figure 15: Process diagram for adjustment of identity information .....	42
Figure 16: Lifecycle diagram for identity information management life cycle .....	43

## Tables

Table 1: Overview of information exchanged in identity information management processes. ....	18
Table 3: Overview of information exchanged in specific identity management processes. ....	19
Table 4: Overview of information exchanged in additional identity management system functions. ....	21
Table 6: actors presented in use case diagram. ....	30
Table 8: Summary of uses cases for an identity management system. ....	31
Table 10: functional components of an identity management system. ....	33
Table 12 Consent management business process element description. ....	37
Table 13: Credential lifecycle management business process element description. ....	39
Table 14: Configuration management business process element description. ....	40
Table 15: Policy and compliance management business process element description. ....	41
Table 16: Principal's lifecycle business process element description .....	44

## 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 was prepared by Joint Technical Committee 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*
- *Part 3: Practice*

Further Parts may follow.

## Introduction

It is common for computer systems to make automated decisions based on the *identity* of a person, device or service connected to them. Such 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 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 management of identity information needs appropriate measures to manage risk in organizational processes and secure its business operations. For individuals, security aspects of identity management are important to protect their privacy.

This series of International Standard specifies fundamental concepts and operational structures for identity management focussing on processing of identity information with the purpose of realizing information systems that meet business, contractual, regulatory and legal obligations.

This standard 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 standard specifies requirements for the design and implementation of an identity management system so that it may meet objectives of stakeholders involved in the deployment and operation of that system.

This International Standard 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*
- 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 International Standard

- 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 International Standard is applicable to any information system where information relating to identity is processed or stored.

## 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.

ISO/IEC 42010	<i>Systems and software engineering—Architecture description</i>
ISO/IEC 24760-1	Information technology — A framework for identity management — <i>Part 1: Terminology and concepts</i> .
ISO/IEC 27002:2005	<i>Information technology — Security techniques — Code of practice for information security management</i> .
ISO/IEC 29115	<i>Information technology — Security techniques — Entity authentication assurance framework</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.

### 3.1

#### **documented design**

authoritative description of structural, functionality and operational system aspects

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

NOTE 2 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

NOTE 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

#### **principal**

subject

entity to which identity information in an identity management system pertains

NOTE In the context of privacy protection requirements, a principal refers to a person.

### 3.4

#### **invalidation**

process performed in an identity management system when a particular attribute is no longer valid for a particular entity to mark the attribute invalid for future use

NOTE 1 Invalidation of attributes may be part of updating the attribute value, for instance with a change of address,

NOTE 2 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 The term “revocation” is commonly used for invalidation of attributes that are credentials.

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

### 3.5

#### **regulatory body**

body tasked and empowered by law, regulation or agreement, to supervise the operation of identity management systems

### 3.6

#### **stakeholder**

individual, team, organization, or classes thereof, having an interest in a system  
[ISO/IEC 42010]

## **4. Symbols and abbreviated terms**

ICT      Information and Communication Technology

## 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 shall be 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 International Standard. 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 International Standard should use an appropriate architecture description language (**ADL**) and reference architecture components and functions by terms defined in this and other International Standards.

### 5.2 Architecture elements

#### 5.2.1 Overview

Elements in this reference architecture are

- stakeholders (5.2.2),
- actors (5.3.2),
- views (5.3, 5.4),
- models (5.3.3, 5.3.4, 5.3.5),
- 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 focussed. 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 [7].

The documented design of an identity management system shall include a context viewpoint and a functional viewpoint. It may include a physical view.

##### 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.** 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 International Standard recognizes the following direct and indirect stakeholders

- principal,
- identity management authority,
- identity information authority,
- relying party,
- regulatory body
- auditor, and
- consumer representative.

Each stakeholder performs a separate role in the identity management system, which are explained in this clause. These roles possess specific responsibilities and liabilities. With the exception of regulatory bodies and consumer representatives, stakeholders are operationally involved in 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 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 use made of identity information by the identity management system,
- correctness of data analytics used for identification purposes including treatment of false negative and false positive identification,
- transparency of identity data sharing,
- correct representation of the entity by the identity information provided and processed,
- correctness of operations in the delivery of services and the access to resources made available based on the attributes presented in a specific situation,
- equitable treatment in its interactions with the system, and
- an easily understandable, effective, appropriate user interface.

#### **5.3.1.3 Identity management authority**

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

- risk of operating an identity management system;
- 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:

- risk and cost of this particular business;
- 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;
- the level of assurance required for its use of received identity information;
- effective, documented and secure interfaces;
- conformance to regulation applicable to its operations;
- effective mechanism and procedures for auditing; and
- effective operation considering cost, revenue and risk.

#### **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 policies;
- 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 advocate**

Consumer advocates are individuals and groups that frequently have emerged from civil society and try to protect consumers and citizens from surveillance and lobby for improved privacy regulations.

Consumer advocates main concerns are:

- transparency, notification, compliance and protection against complex legal language.
- access of services to disadvantaged populations

#### **5.3.1.8 Consumer (and citizen) representative**

Consumer and citizen representatives are those individuals selected by recognised consumer organisations to act as stakeholder representatives of consumer and public interest concerns.

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

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

#### **5.3.1.9 Auditor**

Concerns of an auditor include:

- clear and attainable criteria for audits.

### **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 specification in a document design of different actors shall comprehensively define all interactions supported by the system.

**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.

The documented design shall describe the interactions of an actor with an identity management system by specifying one or more roles. The documented design shall specify means to authenticate the entity at a level of assurance appropriate for each role.

A documented design may recognize the following actors:

- principal;
- identity management authority;
- identity registration authority
- relying party;
- identity information provider;
- identity information authority;
- verifier; and
- 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 to their identity within identification management processes. The Principal has the following responsibilities:

- as an enrollee when intending to become known in 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 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;
- as the subject of observation and initially anonymous data collection;
- as reviewer, the right to know what identity information pertaining to itself is held in the identity management system and the right for 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.

NOTE An identity management authority use policies to regulate use of registered identity information. Policies may indicate levels of service provide including the level of assurance on identity information that may be provided by the identity management system. Policies may also indicate 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 maintain identity management objectives for an associated domain.

The roles of an identity management authority may be delegated to allow an independent identity management operator with the responsibility is to police the operations of one or more identity managements systems in their associated domains.

Responsibilities of an identity management authority include:

- to initiate regular audits;
- to evaluate audit reports, in particular on the effectiveness of policies;
- to respond to incidents;
- to modify, create 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 and
- to approve changes in the type of information recorded in the repository.

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

NOTE The purpose of a federation 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, each identity management authority

- shall provide a level of assurance in identity information that meets the specified requirement of any other member of the federation,
- shall maintain control over access to the identity information contained in its identity management system,
- shall 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,
- shall provide a level of assurance in identity information,
- should operate with common policies for information sharing,
- shall specify policies to maintain its trust in the level of assurance of identity authentication.

NOTE1 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.

NOTE2 Identity management policies for use in multiple domains of applicability may be established by international standards.

NOTE3 Changes to structure, organisation and extent of a data federation may be subject to external constraints such as legal or regulatory requirements or permission by regulatory bodies.

NOTE4 Members of a federation may agree to delegate operational responsibilities of the identity management authority to a common operator.

#### 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.

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

Responsibilities of an identity management authority include:

- to modify, create or revoke operational policies;
- to approve modification of mechanisms to establish a required level of assurance in entity authentication for access to identity information and system control functions;
- 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 verification identity information for a particular principal. A relying party uses verified information to provide principals 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 in conjunction to identity information. Provided metadata information 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 identity information authority may perform its role as an independent service provider.

**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 International Standard.

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 could 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; and
- 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 information system supports such use, the documented design of an identity management system shall specify policies 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 can provide identity information for a specific entity.

The core responsibilities of an identity information provider are:

- to collect identity attributes from principals;
- 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.

- 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.

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 International Standard.

#### 5.3.2.8 Verifier

A verifier is an actor in an identity management system with the responsibility of establishing 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*,”
- an actor primarily using authoritative identity information provided by an external identity management system should be labelled “*assertion consumer*,”

**NOTE** A 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 examine the operational records of an identity management system in order 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.

Responsibilities of an auditor as actor in an identity management system 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, in reporting 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 non-acting stakeholders and external actors as specified in this International Standard.

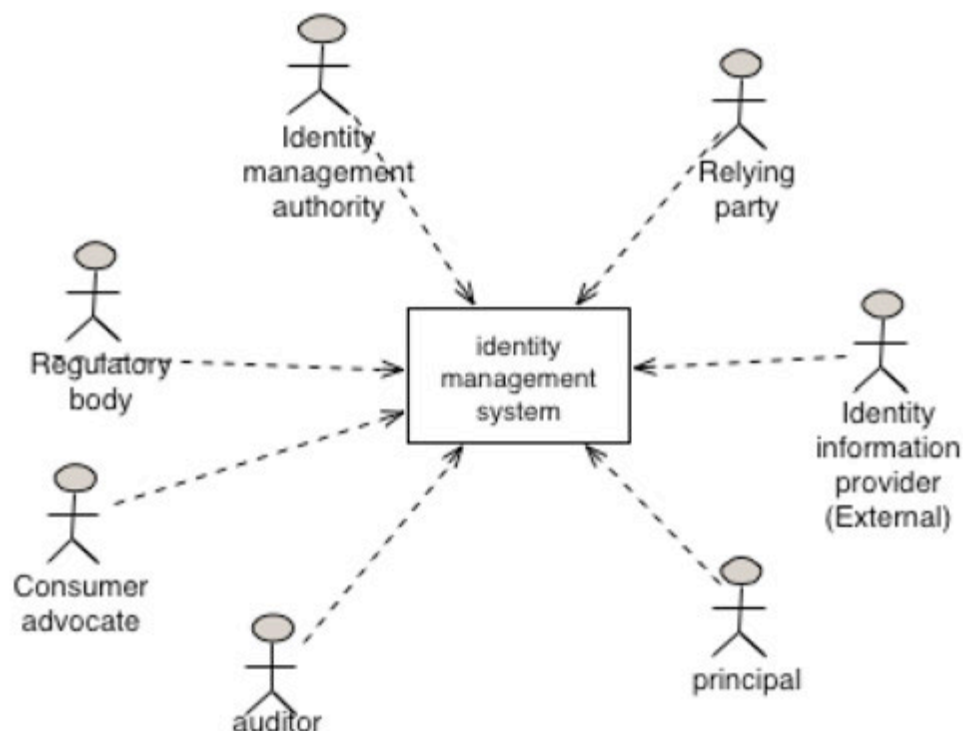


Figure 1 Context model for identity management.

The documented design shall specify concrete representations of the stakeholders and actors in 5.3.1 and 5.3.2, respectively. The documented design may add additional stakeholders or external 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 is 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; and
- a principal accessing a resource under control of a relying party.

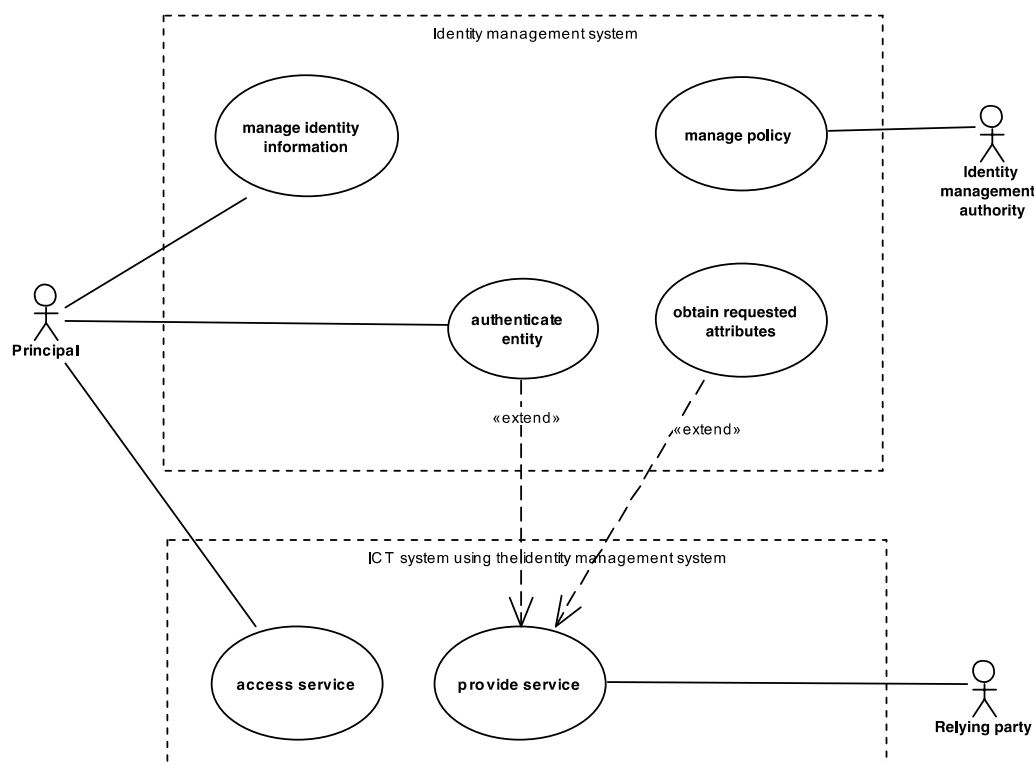


Figure 2 Identity information baseline use case.

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

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 user;
- 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**

As employees, actors mainly use the system as an information retriever, accessing PII of other employees without control of information contained on it self. Consent for information processing and access is implicit.

Based on work duties assigned, this actor mainly expects accurate 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 is an actor with responsibilities to manage components of the system. In interactions with the identity management system, an employer can further be described as an employee. (5.3.4.2)

From an employer point of view, the information should be accurately maintained and used with equal level of semantic, syntax and quality controls, and nothing can pertain to its processing without an approved rationale.

#### **5.3.4.4 Consumer use cases**

In consumer 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 consumer 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 may have been stored in relying parties relating to the re-enrolled entity.

From a consumer 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 the conceptual mechanisms to meet constraints for an identity management system. This includes the following seven concepts, where an identity management system should:

—ensure accuracy of acquired identity information of managed entities with different level of



- assurance not only at initialization but for the whole lifetime of the principal;
- ensure uniqueness of identity information pertaining to a specific principal;
- ensure the identity information is accurately acquired with equal syntax, semantic, and assurance of quality controls;
- ensure the access to different types of identity information is provided to authorized users with different level of assurance;
- ensure auditability of access to identity information.
- 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; and
- comply with local, regional and global regulations, and meet conformance and governance requirement

## 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 to meet the operational requirements for concepts identified in its architecture views.

The documented design of an identity management system shall describe operational structural element of the system, comprising data, functional components and interfaces. In addition to stakeholders and actors more specific data structures should be defined, such as

- metadata of actors to describe cryptographic keys and properties, discovery services, policies and other capabilities and requirements,
- principal data to describe the attribute syntax, semantics and mapping rules to data representation in other systems,
- data structures used in a transaction context, such as authentication requests, assertions and session keys.

#### 5.4.1.2 Deployment

An identity management system may be realized according to either a centralized or decentralized scenario (see ISO/IEC 24760-1). The documented design of an identity management system shall specify its deployment scenario. See 5.5

#### 5.4.1.3 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.

#### 5.4.1.4 Identity register

The purpose of the identity register is to provide consistency of the identity information in the identity management system. An identity register may be implemented in different ways, for instance, centralized, segmented or distributed. Some identity information in an identity register may 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).

An identity may be stored in an identity register in one or 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, and
- differences in storage location, e.g. in a central repository 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 Diagrams

Provides UML diagrams to further describe processes in an identity management system.

A documented design may utilise the diagrams in this International standard as basis.

#### 5.4.2.1 Identity information flow

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

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 the following processes:

- identity information provisioning
- identity information processing; and
- granting identity processing access.

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

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
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.

process	actors			
	source		recipient	
	architecture element	action	architecture element	action
	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

Table 1: Overview of information exchanged in identity information management processes.

**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 roles assigned to the relying party and the permissions associated with these roles.

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

**5.4.2.2.3 Identity information processing**

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 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.

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		

process	actors			
	source		recipient	
	architecture element	action	architecture element	action
	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

Table 2: Overview of information exchanged in specific identity management processes.

**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; and
- 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; or
- 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; and
- 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 for the purpose of a deployment process. These include:

- identity information profile service;
- privacy consent service;
- identity authority discovery service; and
- publication service.

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

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

process	actors			
	source		recipient	
	architecture element	action	architecture element	action
	Identity information provider	Implements validated publication policy	Relying party	Receives published information

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

#### 5.4.2.4.2 Identity information profile service

An identity information profile service provides a canonical representation of identity information for entities of same nature, e.g., a human, a device, an organization. This may require different descriptive format for the purpose of the use of identity information. The definition and maintenance of specific different canonical representation of an identity may be required. The complexity of this approach needs to be balanced with the complexity of the use of identity information when it encloses entities of multiple natures for which different information type may be useful and requested by identity information users.

#### 5.4.2.4.3 Privacy consent service

A privacy consent service 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; and
- to notify a principal of intended use of identity information.

#### 5.4.2.4.4 Identity information authority discovery service

An identity information authority discovery service 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 service

A publication service 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; and
- 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 solutions, e.g. differing in cost and performance.

This International Standard addresses the physical view only at the level of structural components. Implementation aspects of the physical view are beyond the scope of this international standard.

## 5.5 Identity management scenarios

### 5.5.1 General

An identity management system may be deployed according to different scenarios. A deployment scenario impacts governance of the identity management system. A deployment scenario identifies the trust relationships 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.

**NOTE** The users of the identity information are converging on a set of central components, even though the means of access may be distributed. The management of the components, the management of the information, and the management of their respective controls are typically centrally grouped. The information is typically kept on a few storages under one unique management.

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

### 5.5.3 Federated scenario

With a federated scenario an identity management system is deployed that consists of multiple sub systems, with independent governance of the sub systems. Trust in operations, and governance of the deployed system as a whole is established through negotiated agreement. Governance may be delegated to an organization with a formal structure or statute, which contains operating rules, roles, responsibilities and defined liabilities for participating members.

Usually when a domain of applicability needs to be extended in order to integrate another domain or to collaborate with another domain, the centric approach will fuse the two domains into a new one. The federated model offers a flexible exchange of identity information between different, separate domains of applicability without full integration of identity management systems.

**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

Some identity management systems operate where independent organisations issue credentials conforming to a specification to principals and relying parties rely on such credentials provided by principals based upon a commercial risks assessment..

## 6. Requirements

### 6.1 General

This clause describes the requirements for the 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; and
- maintenance conditions.

Requirements 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 different levels of assurance in controlling the access;
- conditions of use to impose on recipients of identity information;
- 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; and
- 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 to govern any supported transitions applied to managing an identity information life cycle management to specify:

- accuracy of the identity information required for enrolment;
- conditions and procedure to perform identity adjustment for an identity;
- 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 be specified to maintain the accuracy of the identity information it manages.

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; and
- 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. Such actions may be:

- updating the recorded value of the changed attribute;
- invalidating identity information; and
- provisioning of the updated information.

The documented design of an identity management system shall provide policies to maintain the integrity of the identity information and meta data 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 presentation

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 under governed of policies to address:

- Access control; and
- Auditing.

The purpose of the information presentation interface include:

- presenting identity information;
- presenting identity information meta data;
- presenting information on on-going and past system operations;
- presenting 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 should take into account the capabilities and restrictions of the indented user of the information.

### 6.3.4 Reference identifier

An identity management system may contain a component to generate a reference. The task of a reference-identifier is to assure that a specified set of attributes for an entity known to an identity information system have a combined value that is different from the value of the same attribute in the identity register for any other entity.

Access to the value of a reference identifier may be restricted, e.g. 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 shall generate a unique reference identifier for each principal of which identity information is stored in the identity register.

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

**NOTE 2** The reference identifier generated may be based on information obtained from the entity, e.g. a chosen pseudonym.

**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; and
- 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 references 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 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 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 should be deleted within a period after creation 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 should 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 International Standard.

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

The documented design of an identity management system should 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.

## **Legal and regulatory aspects (Informative)**

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; and
- security aspects of physical credentials, in particular, those intended for use in authentication.

## Use case model (Informative)

This annex presents a use case model that includes a decomposition of roles for actors in an identity management system. This decomposition of roles includes the actors described in table 4.

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 " <i>federation operator</i> "
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.

Table 4: actors presented in use case diagram.

The use case shown in figure 3, describes two main use cases in an identity management system:

- (1) access to a protected resource,
- (2) delivery of a message to be authenticated.

Table 5 summarises the use cases in this diagram.

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	Enroll, update, archive and purge identity information
manage policy	Specify the policy and procedures to operate and maintain the identity

Use Case	Description
	management system.
obtain requested attributes	Obtain attributes for the authenticated principal for the requested be the service
provide service	The relying party provides resources that need authenticated access.
provision service	Provide a Relying Service with Identity Information about Principals.
send authenticated message	<p>Send a document, web-service request and the like. There is no direct response in the process or transaction. Examples:</p> <p>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.</p> <p>A sender delivers asynchronous, signed message, e.g. as specified in SOAP, to a service.</p>

Table 5: Summary of uses cases for an identity management system.



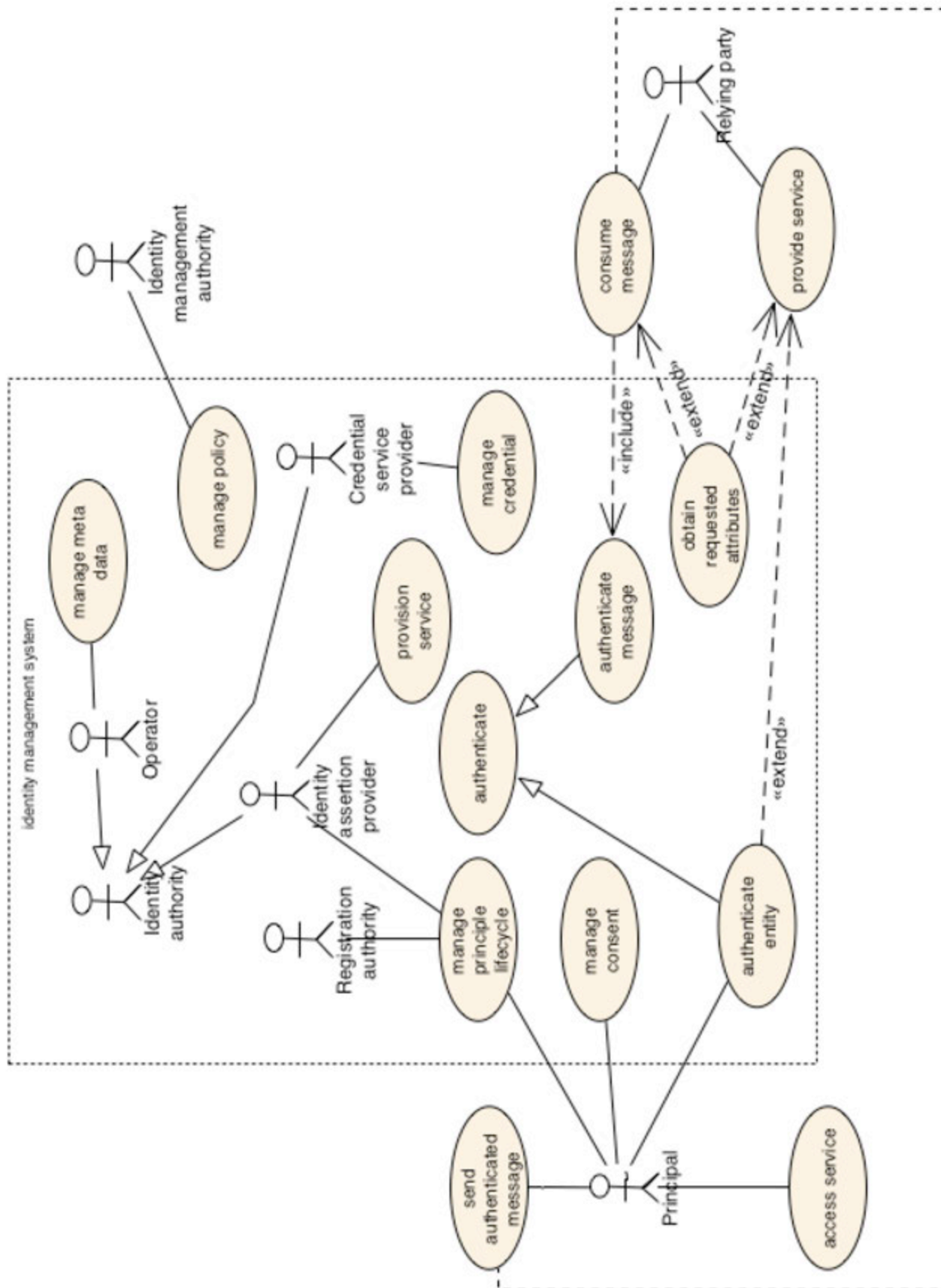


Figure 3: Exemplary *use case diagram* for an identity management system.

## Component model (Informative)

### A.1 Model

This annex presents, in figure 4, 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[14], 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 6 summarizes the components shown.

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 than 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 a certificates for public keys used by the system. A public key certificate is provisioned out-of-band..

Table 6: functional components of an identity management system.

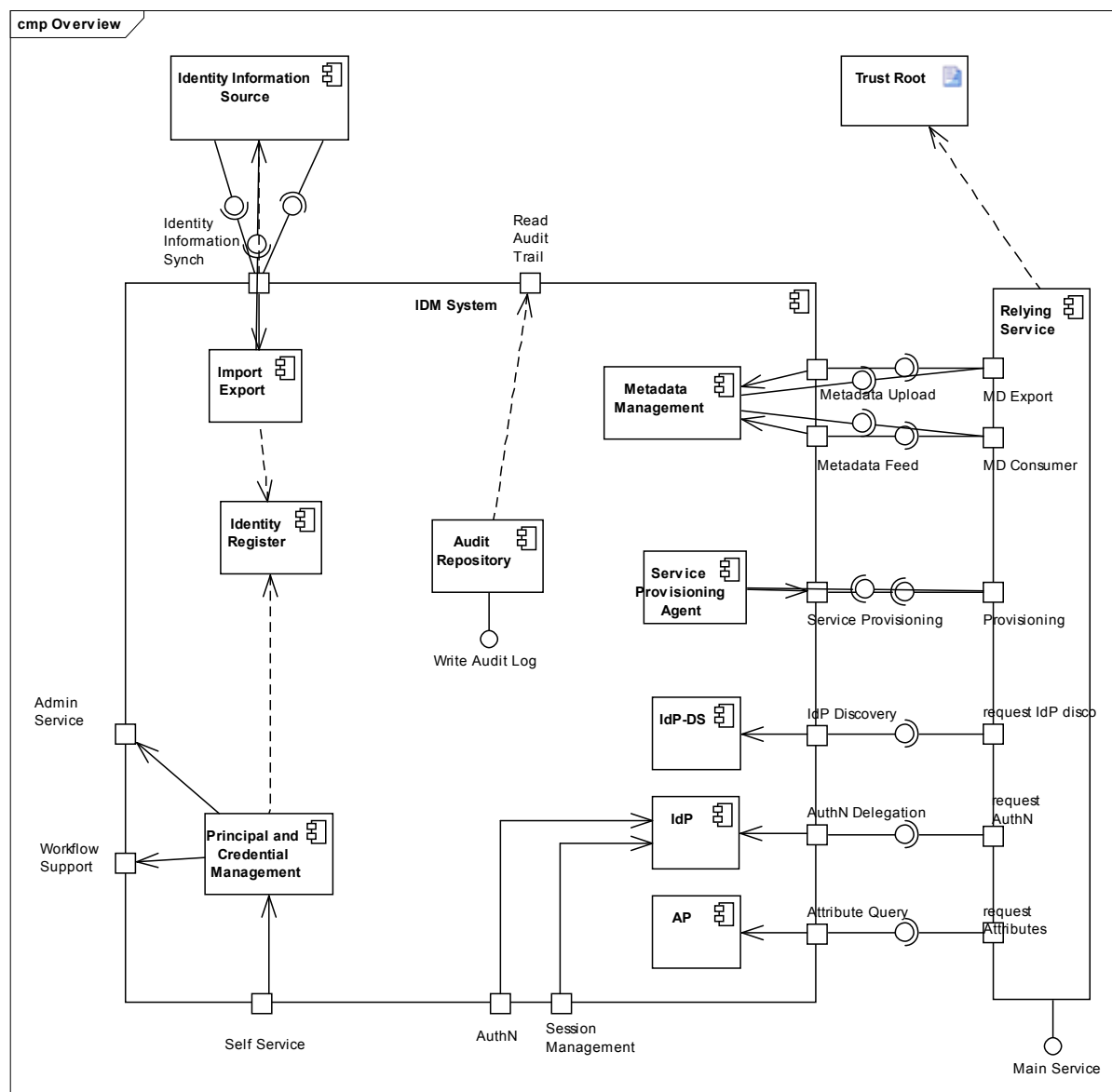


Figure 4: Functional components in an identity management system.

## A.2 UML legend

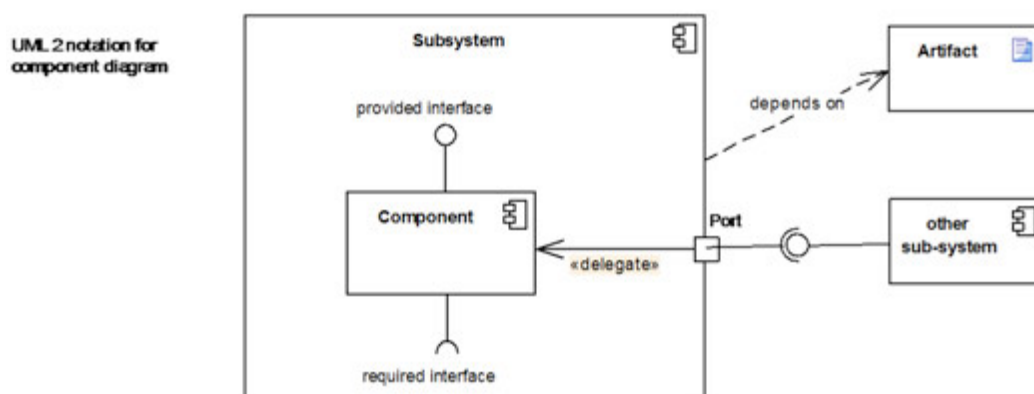


Figure 5: Graphical elements in a UML component diagram.

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.

## Business Process model (Informative)

### A.3 General

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[15].

### A.4 Consent management.

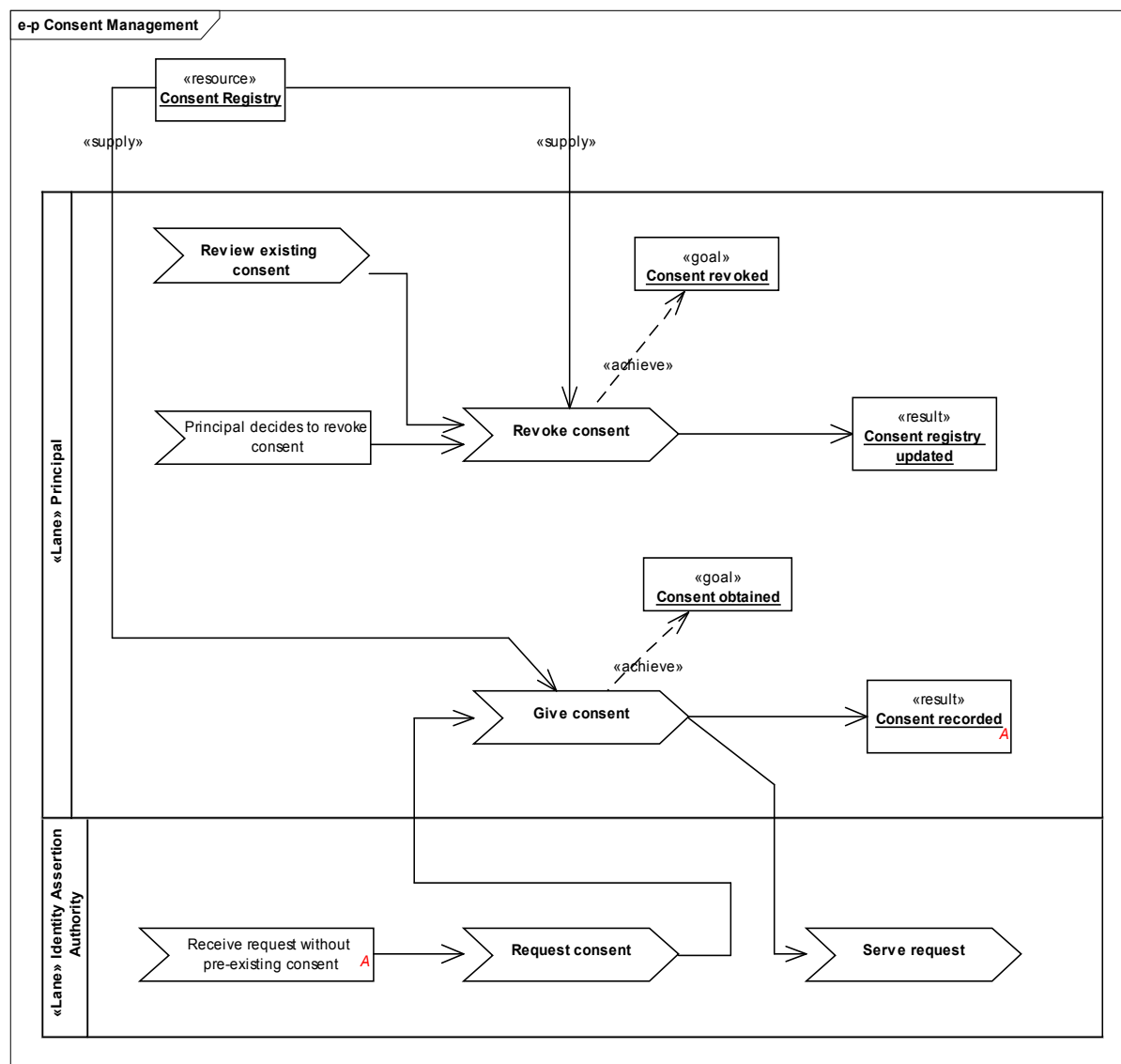


Figure 6: Process diagram for consent management.

Process	Details
Revoke consent	In cases where consent is not implicit the Principal must be provided with an option to revoke previously given consent.
Review existing consent	Users need to have the ability to withdraw a consent given previously.
Give consent	Consent needs to be given according to the privacy policy, e.g.: explicit per business transaction for health data; explicit per relying party for all future transactions for access to a library service for a student; implicit for access of services to a web application to perform official duties for a government employee.

Event	Details
Principal decides to revoke consent	This event implies that the Principal is provided with a facility to revoke consent, be it online, via a call centre or other communication channel.
Receive request without pre-existing consent	Authentication request or attribute query without pre-existing consent. Previous consent does not exist, has expired or is not applicable for the transaction.

Goal	Details
Consent revoked	Consent is revoked. The policy has to decide if this is interpreted as denial or removal. In the latter case the Principal would be asked again to give consent.
Consent obtained	To share Identity information with a relying party the controller has obtained and documented consent in the appropriate manner (per transaction, per relation, etc.)

Resource	Details
Consent Registry	The consent registry stores user consent in a machine-readable format. Unstructured documents may be included for audit purposes. NOTE: The consent registry may be grouped with the identity information provider or other actors.

Result	Details
Consent registry updated	
Consent recorded	Consent decision is recorded. If consent was positive, the authentication and/or attribute request is allowed.

Table 7 Consent management business process element description.

## A.5 Credential lifecycle management

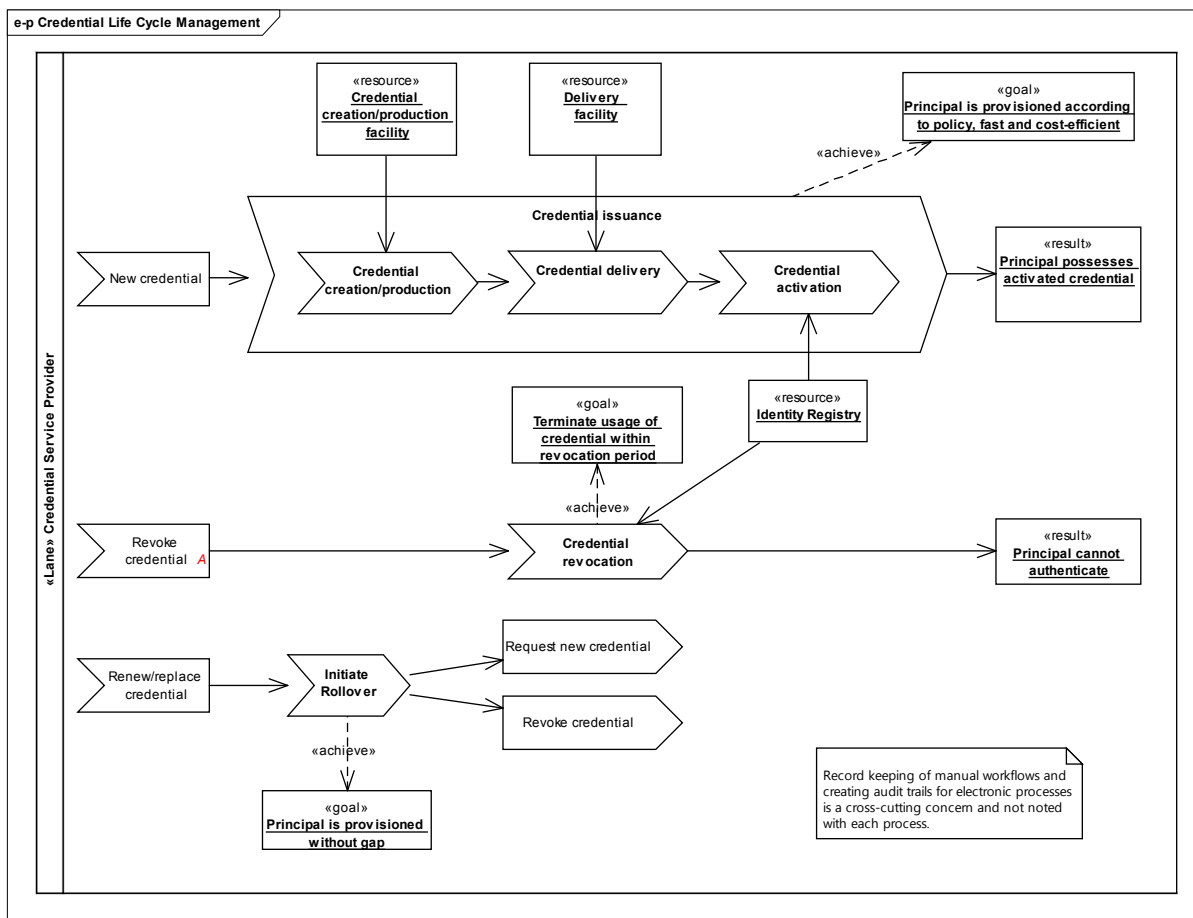


Figure 7: Process diagram for credential lifecycle management.

**NOTE** Suspension of a credential is not supported in this diagram. It was left out to reduce complexity and can be added in a specific architecture where needed.

Process	Details
Credential replacement	Issue a new credential in place of an existing one.
Credential revocation	Update the <b>identity register</b> to reflect the revocation status. The process might also trigger the collection of a physical credential like an OTP token.
Initiate Rollover	Issue a new credential and assure that there is no gap in the transition.
Credential issuance	Provision a Principal with a credential
Credential creation/production	This is a generic placeholder for the simple (e.g. password) or complex (e.g. smartcard, biometrics) process that delivers a credential. NOTE: Although a credential is only data, the process to create it might need to include the production of a physical token containing the credential as well.
Credential delivery	The delivery of the credential (and a belonging physical token as container) may establish or enforce the binding between the credential and the Principal.
Credential activation	<b>Activation</b> is the that enables the entity to access resources using the credential
Event	Details
Renew/replace credential	Replacements might have different reasons, e.g. credential is lost or dysfunctional; an attack on the credential is suspected or known; the credential expired (e.g. a smart card before end of life).
Revoke credential	Revoke old credential in consideration of the rollover period.

Event	Details
New credential	Another process triggered the credential issuance process.
Request new credential	Trigger the process to issue a new credential.
Revoke credential	A process triggered the revocation of a credential.

Resource	Details
Credential creation/production facility	Depending on the type of credential this might just be a password generator or could be e.g. a smartcard production.
Delivery facility	Credentials can be delivered electronically, physically face to face, or via a delivery service.
Identity Registry	Contains the subset of Identity Information that is required for enrolment, authentication and revocation services.

Table 8: Credential lifecycle management business process element description.

## A.6 Configuration Data Management

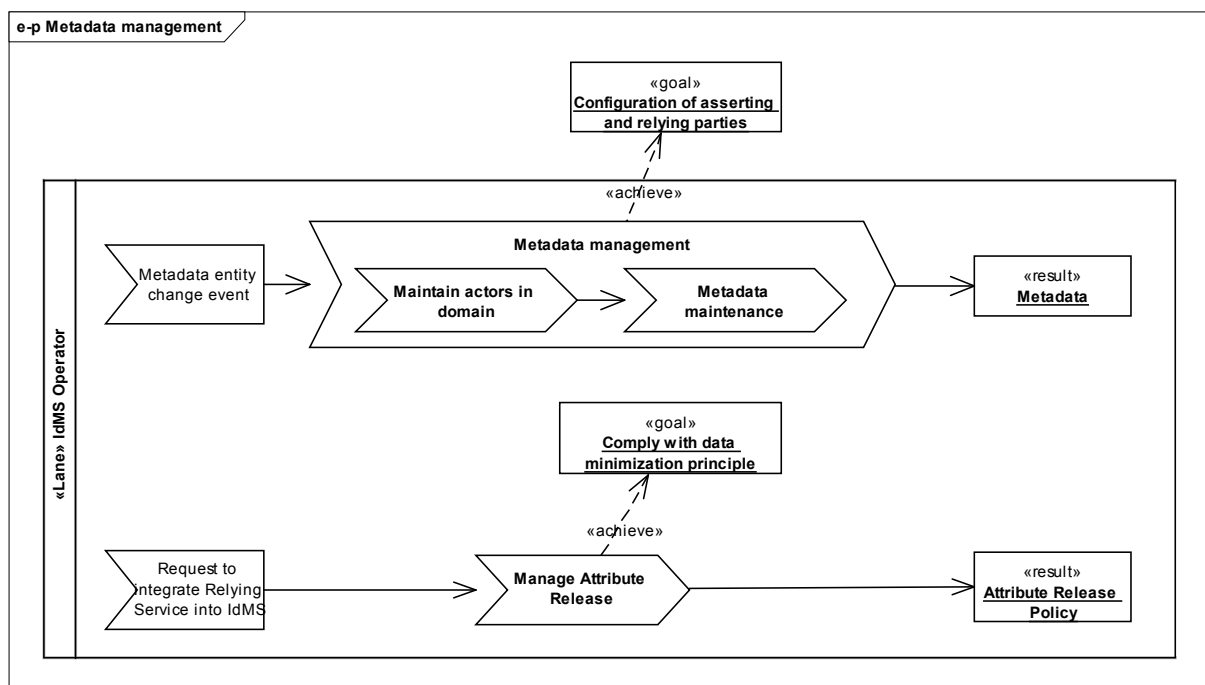


Figure 8: Process diagram for configuration data management

Process	Details
Configuration maintenance data	Create machine-readable configuration or meta data.
Maintain actors in domain	Administration of IMS members on business and technical levels and their properties. This includes the supervision and validation of data self-administered by IMS members.
Manage Attribute Release	When provisioning services only attributes that are required and consented by the user may be released. To achieve this an attribute release policy needs to be defined when boarding a Relying Service to the IMS.

Event	Details
Request to integrate Relying Service into IMS	A Relying Party applies to integrate their service into the IMS.



Goal	Details
Comply with data minimization principle	The Identity Authority must restrict its services to trustworthy Relying Parties, and restrict the release of attributes to what is appropriate for the service and/or consented by the user.
Configuration of asserting and relying parties	Administrative technical data about asserting and relying parties to facilitate their communication and trust relationships.
Result	Details
Attribute Release Policy	

Table 9: Configuration management business process element description.

## A.7 Policy Management

Policy management is concerned with the creation and maintenance of the IMS policy and the associated GRC management.

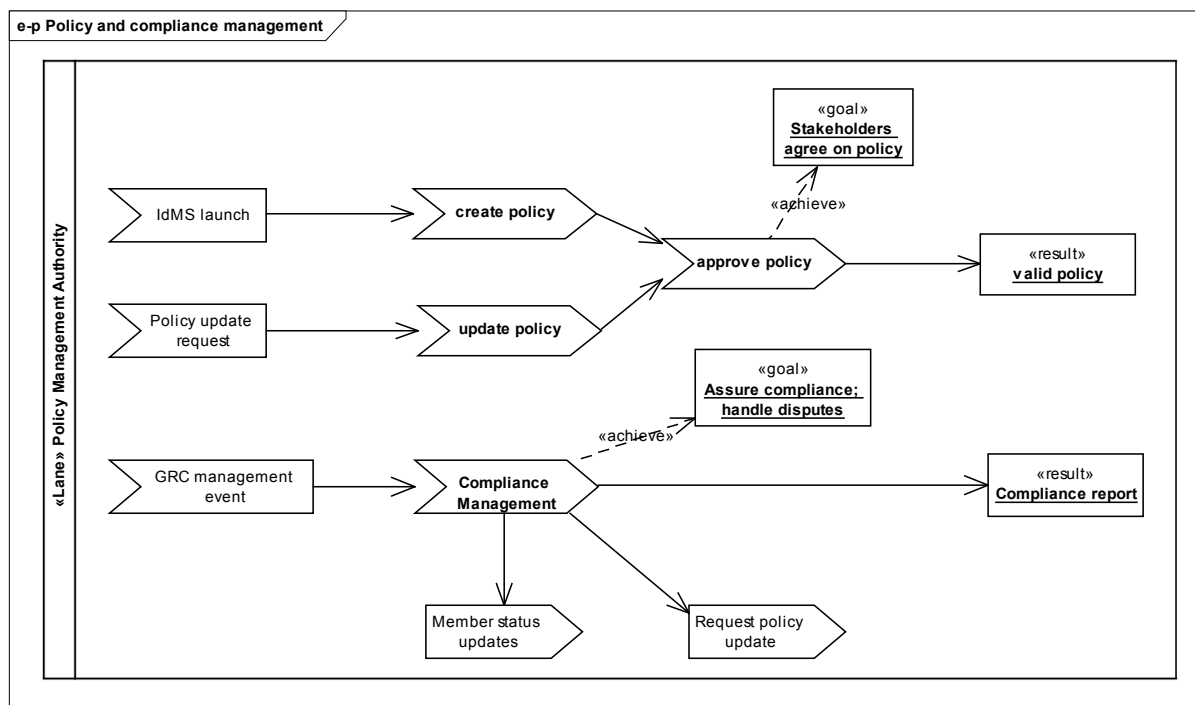


Figure 9: Process diagram for policy and compliance management.

Process	Details
update policy	This is an activity typically performed by a task force or working group.
create policy	This is an activity typically performed by a task force or working group.
approve policy	This is an activity typically performed by a board or general assembly.
Compliance Management	Compliance management comprises executing the management system defined in the IMS policy.

Event	Details
Request policy update	Send request to update policy.
IMS launch	Management of an enterprise, sponsors of a project or founding members of a federation decide to start the development and deployment of an IMS.
GRC management event	The policy defines compliance activities on a scheduled or ad-hoc basis.

Event	Details
Policy update request	Updates may be requested by IMS members, auditors, or in regular intervals for a scheduled review.
Member status updates	Compliance failures are usually handled by the PMA. It can decide to alert, suspend or exclude members from the IMS because of failure to comply.
Goal	Details
Assure compliance; handle disputes	The assurance of compliance should be based on the establishment and maintenance of a management system. Issues that cannot be handled by the management system need to be escalated and resolved by the PMA.
Stakeholders agree on policy	Stakeholders (like representatives of actors or sponsors) agree on rules and procedures to operate the IMS.

Table 10: Policy and compliance management business process element description.

## A.8 Principal's Life Cycle Management

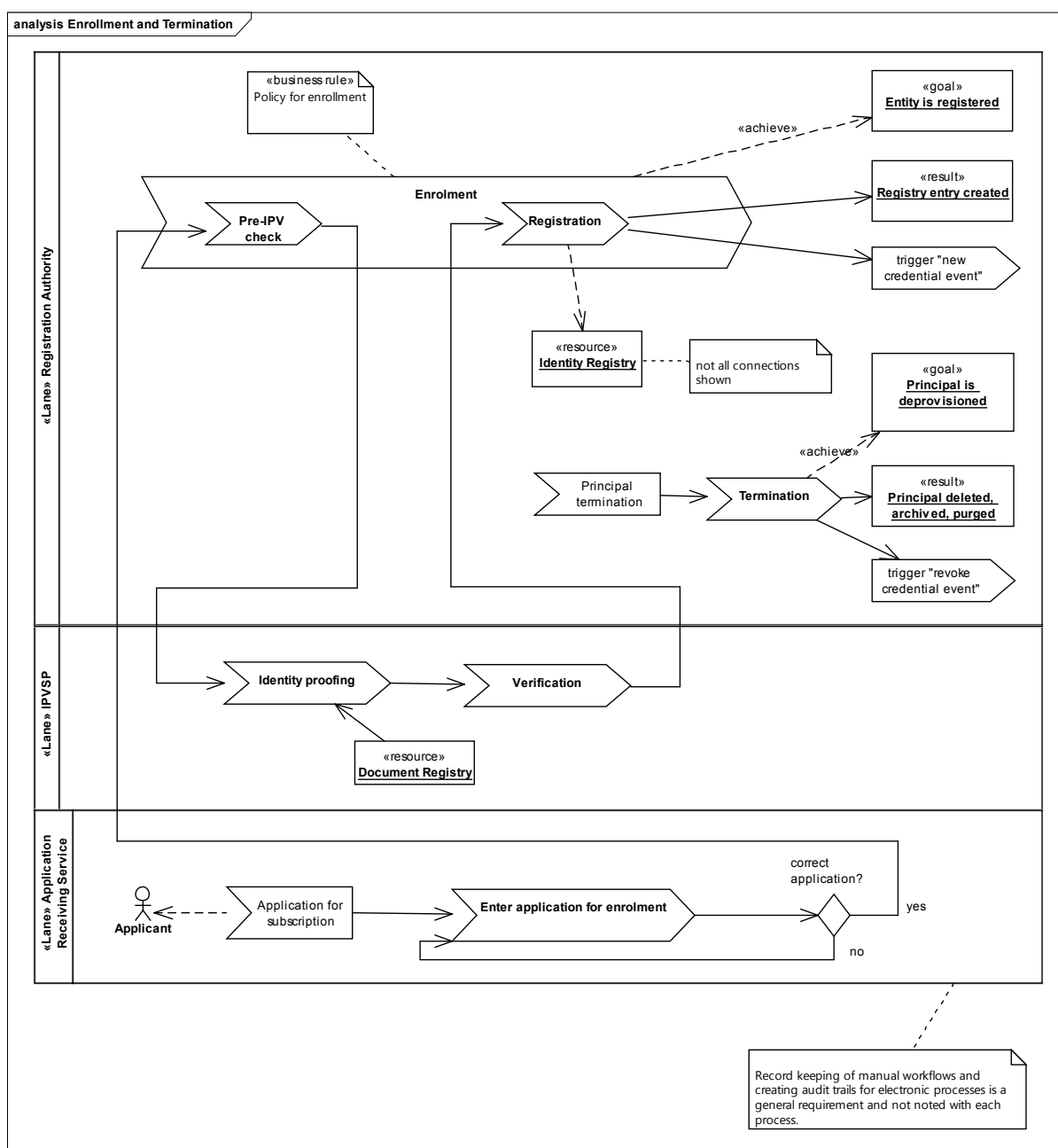


Figure 10: Process diagram for principal's lifecycle management.

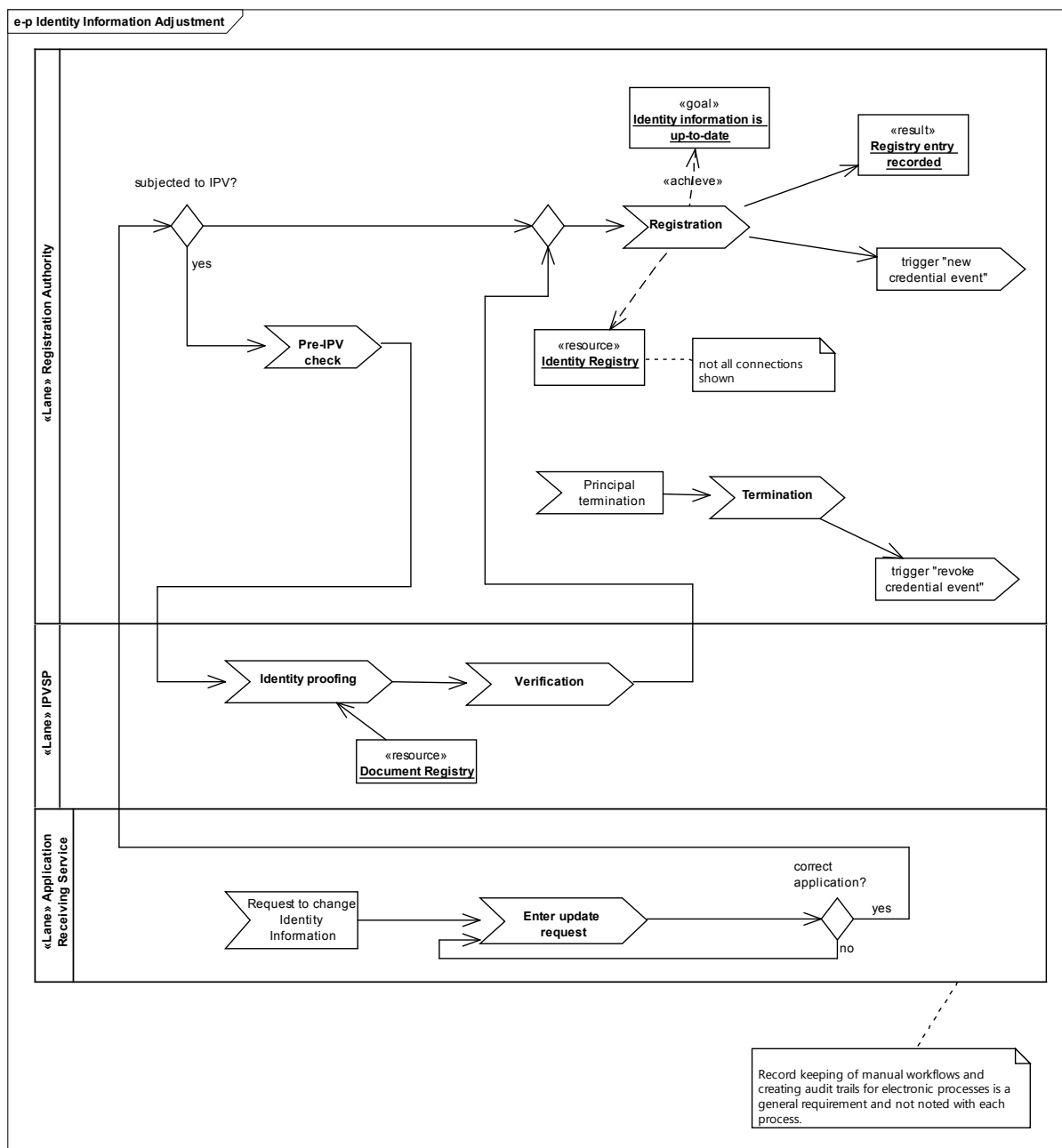


Figure 11: Process diagram for adjustment of identity information

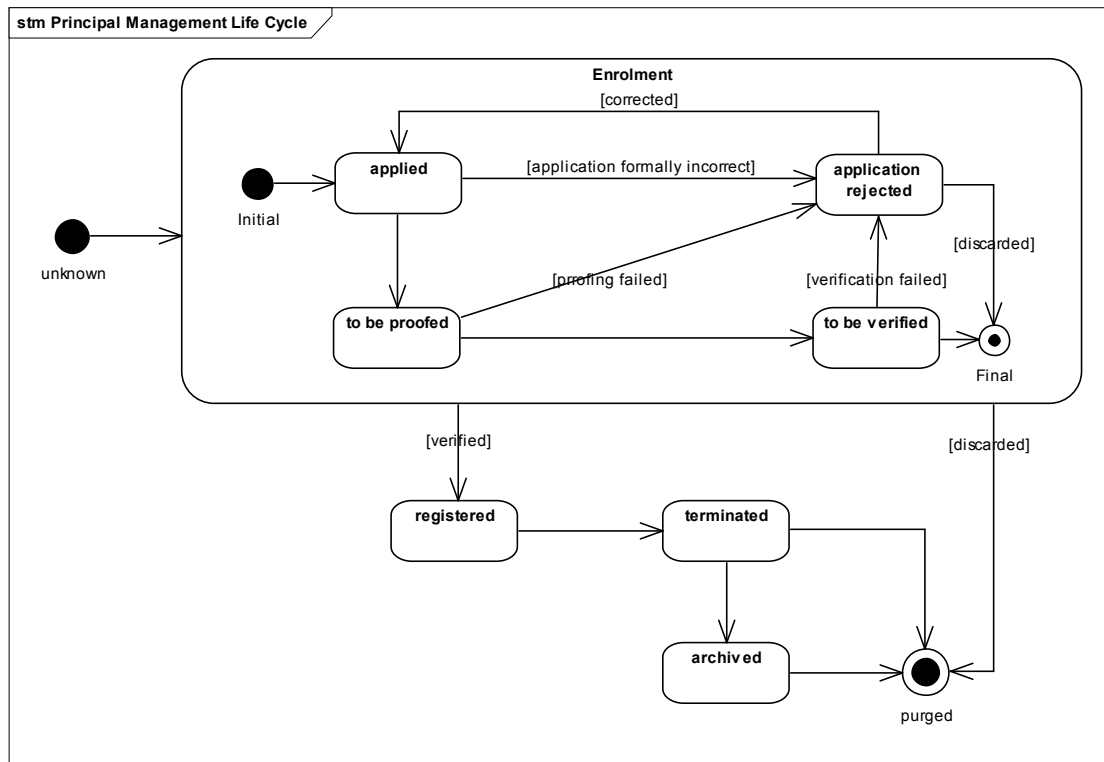


Figure 12: Lifecycle diagram for identity information management life cycle

Process	Details
Enrolment	<p>Process that includes:</p> <ul style="list-style-type: none"> <li>identity proofing (of credentials against tampering);</li> <li>validation (of credentials against issuer's sources);</li> <li>verification of the entities background (credit history, trustworthiness);</li> </ul> <p>assessment of the assurance level; and</p> <ul style="list-style-type: none"> <li>registration of the entity as Principal in the identity registry.</li> </ul> <p>Depending on the required level of assurance some of these steps may be skipped.</p>
Pre-IPV check	Check application for formal criteria like completeness, syntactical correctness and SPAM. Rational: Save cost in the IPV process which might be charged even if the result is negative.
Identity proofing	Process of capturing and verifying sufficient information to identify a Principal to a specified or understood level of assurance.
Verification	<p>Short for Identity Information Verification. Process of checking identity information and credentials against issuers, data sources, or other internal or external resources with respect to authenticity, validity, correctness, and binding to the entity. [ISO/IEC 29115]</p> <p>NOTE: This definition pertains to the enrolment process. A related use is the term verifier, that pertains to the authentication process. This architecture does not use Verification in the context of Authentication.</p>
Enter application for enrolment	The application for enrolment can be provided online by the applicant, or communicated out-of-band, such as on a paper form or a system that is outside the IMS.
Enter update request	The application for a change of identity information can be provided online by the applicant, or communicated out-of-band, such as on a paper form or a system that is outside the IMS.
Registration	<p>The registration process takes identity information that has been proved and verified and writes it to the Identity Registry.</p> <p>NOTE: Technically this information might be stored there already by previous process steps. In this case this process updates the status to "registered". Compare to the state diagram for the principal life cycle management below.</p>

Process	Details
Termination	Termination is a multi-step process: Archive identity information of the Principal; Replace identity information with deletion stubs in identity register; After the expiration of the archiving period purge the archived information including backups.
Event	Details
Application for subscription	Entity applies (self or proxy) to become subscriber at the Identity Management Authority
Principal termination	
trigger "revoke credential event"	
Request to change Identity Information	The request may come from a User Home Organization, Principal, Identity Information Source or other actors.
trigger "new credential event"	
Goal	Details
Identity information is up-to-date	
Entity is registered	The goal of the enrollment process is to register the entity and have its credentials proved, validated and its identity information registered.
Principal is deprovisioned	The goal of the termination process is to deactivate the Principal's credentials within the timeframe specified by the policy, archive the identity information in the specified extend and duration, and purge all identity information after the expiration of the archival period.
Resource	Details
Document Registry	A registry or service that can be used to verify that <ul style="list-style-type: none"> <li>○ a credential presented to establish the identity does exist with the issuing authority, and</li> <li>○ it has not been revoked.</li> </ul>
Document Registry	A registry or service that can be used to verify that <ul style="list-style-type: none"> <li>○ a credential presented to establish the identity does exist with the issuing authority and</li> <li>○ it has not been revoked.</li> </ul>
Result	Details
Principal deleted, archived, purged	These are the activity results related to termination.
Registry entry created	The entity is registered as Principal in the Identity Registry
Registry entry recorded	The entity is registered as Principal in the Identity Information Registry; In the case of an adjustment the identity information is updated.
Registry entry created	The entity is registered as Principal in the Identity Registry

Table 11: Principal's lifecycle business process element description

## Bibliography

- [1] ISO/IEC 12207, "*Information technology — Software life cycle processes.*"
- [2] ISO/IEC 15288, "*Systems engineering — System life cycle processes.*"
- [3] ISO/IEC 29146, "*Information technology — Security techniques — A framework for access management.*"
- [4] ISO/IEC 18014-1, "*Information technology — Security techniques — Time-stamping services — Part 1: Framework.*"
- [5] ISO/IEC 15288 "*Systems engineering—System life cycle processes.*"
- [6] ISO/IEC 12207 "*Information technology—Software life cycle processes.*"
- [7] Rozanski, N., and Woods, E.: "*Software Systems Architecture: Working With Stakeholders Using Viewpoints and Perspectives*", 2011
- [8] NISTIR 7693, "*Specifications for Asset Identification.*"
- [9] IETF SCIM 1.1, "*System for Cross-Domain Identity Management: Core Schema*"
- [10] OASIS SAML 2.0
- [11] W3C RDF/XML, "*syntax specification (revised)*"
- [12] OASIS CIQ 3.0
- [13] IETF RFC 4517 "*LDAP syntax and matching rules.*"
- [14] Fowler, Martin. "*UML distilled: a brief guide to the standard object modeling language.*" Addison-Wesley Professional, 2004.
- [15] Eriksson, Hans-Erik, et al. "*UML 2 toolkit.*" John Wiley & Sons, 2003,


**EXPLANATORY REPORT**  
**RAPPORT EXPLICATIF**
**ISO/IEC CD 24760-2**

ISO/IEC JTC 1/SC 27

Secretariat **DIN**

This form should be sent to the ISO Central Secretariat, together with the English and French versions of the committee draft, by the secretariat of the technical committee or subcommittee

Ce formulaire doit être envoyé au Secrétariat central de l'ISO en même temps que les versions anglaise et française du projet de comité, par le secrétariat du comité technique ou du sous-comité concerné.

The accompanying document is submitted for circulation to member body vote as a DIS, following consensus obtained from the P-members of the committee.

Le document ci-joint est soumis, pour diffusion comme DIS, au vote comité membre, suite au consensus des membres (P) du comité obtenu.

on **2014-04-15**
☒ at the meeting of  
à la réunion du
see resolution No. **2**  
voir résolution n°in  
dans le document **14200**
☐ by postal initiated on  
par un vote par correspondance démarré le

	Number	Countries
P-members in favour: Membres (P) approuvant le projet:	<b>14</b>	<b>Austria, Belgium, China, Germany, Ireland, Jamaica, Korea, Republic of, Mexico, Netherlands, New Zealand, Norway, Singapore, Slovakia, Slovenia</b>
P-members voting against: Membres (P) désapprouvant:	<b>3</b>	<b>Japan, United Kingdom, United States</b>
P-members abstaining: Membres (P) s'abstenant:	<b>27</b>	<b>Argentina, Australia, Brazil, Canada, Chile, Cyprus, Czech Republic, Côte d'Ivoire, Denmark, Finland, France, India, Israel, Italy, Luxembourg, Malaysia, Morocco, Peru, Poland, Romania, Russian Federation, South Africa, Spain, Sweden, Switzerland, Ukraine, United Arab Emirates</b>
P-members who did not vote: Membres (P) n'ayant pas voté:	<b>9</b>	<b>Algeria, Estonia, Kazakhstan, Kenya, Mauritius, Sri Lanka, Thailand, The Former Yugoslav Republic of Macedonia, Uruguay</b>

## Remarks/Remarques

The 3rd CD was circulated as N13375. The summary of voting is presented in N13772. The disposition of comments are shown in N14149. The text for a 3-month DIS balloting is contained in SC 27 N14150.

The negative votes of Japan and United Kingdom have been satisfactorily resolved and changed to APPROVAL.

I hereby confirm that this draft meets the requirements of part 2 of the ISO/IEC Directives  
Je confirme que ce projet satisfait aux prescriptions de la partie 2 des Directives ISO/CEI

Date

Name and signature of the secretary  
Nom et signature du secrétaire**2014-05-01****Passia, Krystyna Mrs**

## Result of voting

Ballot Information	
<b>Ballot reference</b>	ISO/IEC CD 24760-2.3 - ISO-IECJTC1-SC27_N13375
<b>Ballot type</b>	CD
<b>Ballot title</b>	Information Technology -- Security Techniques -- A Framework for Identity Management -- Part 2: Reference architecture and requirements
<b>Opening date</b>	2013-12-18
<b>Closing date</b>	2014-03-18
<b>Note</b>	3rd CD Consideration In accordance with resolution 1 (see SC 27 N13375) of the 16th SC 27/WG 5 Plenary meeting held in Incheon, Republic of Korea, 25th October 2013 the hereby attached document is being circulated for a 3rd Committee Draft (CD) letter ballot closing by 2014-03-18.

Member responses:	
<b>Votes cast (44)</b>	Argentina (IRAM) Australia (SA) Austria (ASI) Belgium (NBN) Brazil (ABNT) Canada (SCC) Chile (INN) China (SAC) Côte d'Ivoire (CODINORM) Cyprus (CYS) Czech Republic (UNMZ) Denmark (DS) Finland (SFS) France (AFNOR) Germany (DIN) India (BIS) Ireland (NSAI) Israel (SII) Italy (UNI) Jamaica (BSJ) Japan (JISC) Korea, Republic of (KATS) Luxembourg (ILNAS) Malaysia (DSM) Mexico (DGN)



	Morocco (IMANOR) Netherlands (NEN) New Zealand (SNZ) Norway (SN) Peru (INDECOPI) Poland (PKN) Romania (ASRO) Russian Federation (GOST R) Singapore (SPRING SG) Slovakia (SUTN) Slovenia (SIST) South Africa (SABS) Spain (AENOR) Sweden (SIS) Switzerland (SNV) Ukraine (DTR) United Arab Emirates (ESMA) United Kingdom (BSI) United States (ANSI)
<b>Comments submitted (0)</b>	
<b>Votes not cast (9)</b>	Algeria (IANOR) Estonia (EVS) Kazakhstan (KAZMEMST) Kenya (KEBS) Mauritius (MSB) Sri Lanka (SLSI) Thailand (TISI) The Former Yugoslav Republic of Macedonia (ISRM) Uruguay (UNIT)

Questions:	
<b>Q.1</b>	"Do you agree with approval of the CD text?"
<b>Q.2</b>	"If you approve the CD text with comments, would you please indicate which type ? (General, Technical or Editorial)"
<b>Q.3</b>	"If you disapprove the draft, would you please indicate if you accept to change your vote to Approval if the reasons and appropriate changes will be accepted?"

Votes by members	Q.1	Q.2	Q.3
<b>Argentina (IRAM)</b>	Abstention	Ignore	Ignore
<b>Australia (SA)</b>	Abstention	Ignore	Ignore
<b>Austria (ASI)</b>	Approval with comments	All	Ignore
<b>Belgium (NBN)</b>	Approval as presented	Ignore	Ignore
<b>Brazil (ABNT)</b>	Abstention	Ignore	Ignore
<b>Canada (SCC)</b>	Abstention	Ignore	Ignore
<b>Chile (INN)</b>	Abstention	Ignore	Ignore

<b>China (SAC)</b>	Approval as presented	Ignore	Ignore
<b>Côte d'Ivoire (CODINORM)</b>	Abstention	Ignore	Ignore
<b>Cyprus (CYS)</b>	Abstention	Ignore	Ignore
<b>Czech Republic (UNMZ)</b>	Abstention	Ignore	Ignore
<b>Denmark (DS)</b>	Abstention	Ignore	Ignore
<b>Finland (SFS)</b>	Abstention	All	Ignore
<b>France (AFNOR)</b>	Abstention	Ignore	Ignore
<b>Germany (DIN)</b>	Approval with comments	All	Ignore
<b>India (BIS)</b>	Abstention	Ignore	Ignore
<b>Ireland (NSAI)</b>	Approval as presented	Ignore	Ignore
<b>Israel (SII)</b>	Abstention	Ignore	Ignore
<b>Italy (UNI)</b>	Abstention	Ignore	Ignore
<b>Jamaica (BSJ)</b>	Approval as presented	Ignore	Ignore
<b>Japan (JISC)</b>	Disapproval of the draft	Ignore	Yes
<b>Korea, Republic of (KATS)</b>	Approval as presented	Ignore	Ignore
<b>Luxembourg (ILNAS)</b>	Abstention	Ignore	Ignore
<b>Malaysia (DSM)</b>	Abstention	Ignore	Ignore
<b>Mexico (DGN)</b>	Approval as presented	Ignore	Ignore
<b>Morocco (IMANOR)</b>	Abstention	Ignore	Ignore
<b>Netherlands (NEN)</b>	Approval as presented	Ignore	Ignore
<b>New Zealand (SNZ)</b>	Approval with comments	Editorial	Ignore
<b>Norway (SN)</b>	Approval as presented	Ignore	Ignore
<b>Peru (INDECOPI)</b>	Abstention	Ignore	Ignore
<b>Poland (PKN)</b>	Abstention	Ignore	Ignore
<b>Romania (ASRO)</b>	Abstention	Ignore	Ignore
<b>Russian Federation (GOST R)</b>	Abstention	Ignore	Ignore
<b>Singapore (SPRING SG)</b>	Approval as presented	Ignore	Ignore

<b>Slovakia (SUTN)</b>	Approval as presented	Ignore	Ignore
<b>Slovenia (SIST)</b>	Approval as presented	Ignore	Ignore
<b>South Africa (SABS)</b>	Abstention	Ignore	Ignore
<b>Spain (AENOR)</b>	Abstention	Ignore	Ignore
<b>Sweden (SIS)</b>	Abstention	Ignore	Ignore
<b>Switzerland (SNV)</b>	Abstention	Ignore	Ignore
<b>Ukraine (DTR)</b>	Abstention	Ignore	Ignore
<b>United Arab Emirates (ESMA)</b>	Abstention	Ignore	Ignore
<b>United Kingdom (BSI)</b>	Disapproval of the draft	Ignore	Yes
<b>United States (ANSI)</b>	Disapproval of the draft	Ignore	Ignore

Answers to Q.1: "Do you agree with approval of the CD text?"		
<b>11 x</b>	<b>Approval as presented</b>	<b>Belgium (NBN)</b> <b>China (SAC)</b> <b>Ireland (NSAI)</b> <b>Jamaica (BSJ)</b> <b>Korea, Republic of (KATS)</b> <b>Mexico (DGN)</b> <b>Netherlands (NEN)</b> <b>Norway (SN)</b> <b>Singapore (SPRING SG)</b> <b>Slovakia (SUTN)</b> <b>Slovenia (SIST)</b>
<b>3 x</b>	<b>Approval with comments</b>	<b>Austria (ASI)</b> <b>Germany (DIN)</b> <b>New Zealand (SNZ)</b>
<b>3 x</b>	<b>Disapproval of the draft</b>	<b>Japan (JISC)</b> <b>United Kingdom (BSI)</b> <b>United States (ANSI)</b>
<b>27 x</b>	<b>Abstention</b>	<b>Argentina (IRAM)</b> <b>Australia (SA)</b> <b>Brazil (ABNT)</b> <b>Canada (SCC)</b> <b>Chile (INN)</b> <b>Cyprus (CYS)</b> <b>Czech Republic (UNMZ)</b> <b>Côte d'Ivoire (CODINORM)</b> <b>Denmark (DS)</b> <b>Finland (SFS)</b> <b>France (AFNOR)</b> <b>India (BIS)</b> <b>Israel (SII)</b> <b>Italy (UNI)</b> <b>Luxembourg (ILNAS)</b>

Malaysia (DSM)  
 Morocco (IMANOR)  
 Peru (INDECOPI)  
 Poland (PKN)  
 Romania (ASRO)  
 Russian Federation (GOST R)  
 South Africa (SABS)  
 Spain (AENOR)  
 Sweden (SIS)  
 Switzerland (SNV)  
 Ukraine (DTR)  
 United Arab Emirates (ESMA)

Answers to Q.2: "If you approve the CD text with comments, would you please indicate which type ? (General, Technical or Editorial)"

0 x      **General**

0 x      **Technical**

1 x      **Editorial**      **New Zealand (SNZ)**

3 x      **All**      **Austria (ASI)**  
**Finland (SFS)**  
**Germany (DIN)**

40 x      **Ignore**      **Argentina (IRAM)**  
**Australia (SA)**  
**Belgium (NBN)**  
**Brazil (ABNT)**  
**Canada (SCC)**  
**Chile (INN)**  
**China (SAC)**  
**Cyprus (CYS)**  
**Czech Republic (UNMZ)**  
**Côte d'Ivoire (CODINORM)**  
**Denmark (DS)**  
**France (AFNOR)**  
**India (BIS)**  
**Ireland (NSAI)**  
**Israel (SII)**  
**Italy (UNI)**  
**Jamaica (BSJ)**  
**Japan (JISC)**  
**Korea, Republic of (KATS)**  
**Luxembourg (ILNAS)**  
**Malaysia (DSM)**  
**Mexico (DGN)**  
**Morocco (IMANOR)**  
**Netherlands (NEN)**  
**Norway (SN)**  
**Peru (INDECOPI)**  
**Poland (PKN)**  
**Romania (ASRO)**  
**Russian Federation (GOST R)**  
**Singapore (SPRING SG)**  
**Slovakia (SUTN)**  
**Slovenia (SIST)**

South Africa (SABS) Spain (AENOR) Sweden (SIS) Switzerland (SNV) Ukraine (DTR) United Arab Emirates (ESMA) United Kingdom (BSI) United States (ANSI)
---

Answers to Q.3: "If you disapprove the draft, would you please indicate if you accept to change your vote to Approval if the reasons and appropriate changes will be accepted?"

2 x	Yes	Japan (JISC) United Kingdom (BSI)
0 x	No	
42 x	Ignore	Argentina (IRAM) Australia (SA) Austria (ASI) Belgium (NBN) Brazil (ABNT) Canada (SCC) Chile (INN) China (SAC) Cyprus (CYS) Czech Republic (UNMZ) Côte d'Ivoire (CODINORM) Denmark (DS) Finland (SFS) France (AFNOR) Germany (DIN) India (BIS) Ireland (NSAI) Israel (SII) Italy (UNI) Jamaica (BSJ) Korea, Republic of (KATS) Luxembourg (ILNAS) Malaysia (DSM) Mexico (DGN) Morocco (IMANOR) Netherlands (NEN) New Zealand (SNZ) Norway (SN) Peru (INDECOPI) Poland (PKN) Romania (ASRO) Russian Federation (GOST R) Singapore (SPRING SG) Slovakia (SUTN) Slovenia (SIST) South Africa (SABS) Spain (AENOR) Sweden (SIS) Switzerland (SNV) Ukraine (DTR)

United Arab Emirates (ESMA)  
United States (ANSI)

Comments from Voters		
Member:	Comment:	Date:
<b>Austria</b> (ASI)	<b><i>Comment File</i></b>	2014-03-05 13:42:21
<b>Germany</b> (DIN)	<b><i>Comment File</i></b>	2014-03-19 11:23:27
<b>Japan</b> (JISC)	<b><i>Comment File</i></b>	2014-03-11 13:45:07
<b>New Zealand</b> (SNZ)	<b><i>Comment File</i></b>	2014-03-19 03:50:27
<b>United Kingdom</b> (BSI)	<b><i>Comment File</i></b>	2014-03-12 11:48:47
<b>United States</b> (ANSI)	<b><i>Comment File</i></b>	2014-02-24 18:26:34

Comments from Commenters		
Member:	Comment:	Date:



ISO/IEC JTC 1/SC 27 **N14149**

ISO/IEC JTC 1/SC 27/WG 5 **N514149**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

**DOC. TYPE:** disposition of comments report

**TITLE:** Dispositions of NB comments in SC 27 N13772 on ISO/IEC 3<sup>rd</sup> CD 24760-2 (N13375) Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements

**SOURCE:** 17<sup>th</sup> SC 27/WG 5 meeting

**DATE:** 2014-05-01

**PROJECT:** 1.27.50.02 (24760-2)

**STATUS:** This document is outcome of the editing session for WG 5 project ISO/IEC 24760-2 held during the 17<sup>th</sup> SC 27/WG 5 Plenary meeting in Hong Kong, China. 7<sup>th</sup> – 11<sup>th</sup> April 2014 It is also circulated within for information.

**ACTION:** FYI

**ACT DUE DATE:**

**DISTRIBUTION:** P-, O- and L-Members  
W. Fumy, SC 27 Chairman  
M. De Soete, SC 27 Vice-Chair  
E. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenber, WG-Convenors  
E. de Jong, J. F. Carvajal Vion, Ch. Sténuit, Project co-editors

**MEDIUM:** <http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

**NO. OF PAGES:** 1 + 43

Secretariat ISO/IEC JTC 1/SC 27 -

DIN Deutsches Institut für Normung e.V., Am DIN-Platz, Burggrafenstr. 6, D-10787 [postal D-10772] Berlin, Germany

Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-4-2652; E-mail: [krystyna.passia@din.de](mailto:krystyna.passia@din.de);

[HTTP://www.jtc1sc27.din.de/en](http://www.jtc1sc27.din.de/en)

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
[AT] 1	general			TE	As mentioned previously there is a general concern with the process for creating an architecture as an IS. The communication intensity and bandwidth is too little given that the contributions did not provide a enough input to restrict work on alignment and improvement.	Future revisions of the IS should require substantial input from NBs.	acknowledged
[AT] 2	general			TE	IMS is a well-established acronym for Information Management System. To avoid confusion, IMS should not be used for Identity Management System.	IMS should be renamed to IDMS.	resolved by deleting the acronym
[AT] 3		5,4		TE	The proposed resolution of GB39 for CD2 (IIA vs. IIP clarification) includes a substantial rearrangement of roles in the system. While the editor accepted the proposed changes they asked for a concrete text proposal. However, such a proposal had been submitted as result of the ad-hoc, so the document might have been lost in email communication.	The proposed text changes are attached to this document for consideration.	resolved with DE2, DE3 and new wording to several clauses
[AT] 4		5,5		TE	Now that an agreement on the architectural viewpoints has been achieved, the structure of the document should be aligned accordingly and all architectural elements presented to stakeholders through views.	See appendix 1 in this document	accepted with editors mandate
[AT] 5		5.5.2.2	Fig. 2	TE	This is the only use case describing which actors use which case cases. Therefore it would be better for the reader to provide an overview of the high-level IDM use cases; The diagram should be extended accordingly.	Replace with figure from appendix 2	resolved with new wording and adding a complementary figure to an annex.
[AT] 6		5,6		TE	“Function viewpoint” is a fact a view, not a viewpoint	Change to “Functional view”	accepted
[AT] 7		5.6.2		TE	The component model diagram suffers from a number of inconsistencies: Principals are actors – why separate, in general actors are not part of a component model, the levels of the components vary from technical to astract, the domain of applicabilty should be a system boundary, if shown at all, and diagrams should use UML or another specified and well-known notation.	Replace with the proposed diagram from appendix 3 in this document.	resolved by adding annex with the proposed figure



NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
[AT] 8		5.6.2.1 and 5.7		TE	Enterprise and federated models are not deployment options and rather not infrastructure models; in contrast these are top-level architectural decisions that pervade all other aspects. A better term for these models is IdP scenarios, which are part of the business level requirements. Figure 4 is not a distribution model.	Remove 5.6.2.1 Deployment. Rename 5.7 to „IDM Scenarios“ and make it a sub-section of requirements, right after „General“. Rephrase „deploy, deployment“ throughout 5.7 (use „organized“, „structured“, or similar terms.) Drop figure 4.	accepted
[AT] 9		5.6.2.2		TE	Domain of applicability is already defined in part 1. It does not make sense to redefine it as a component.	Drop 5.6.2.2	accepted
[AT] 10		5.6.2.4		TE	It is unclear what kind of component an <b>Identity information collector</b> should be in a real-world IDMS. If it is part of the IMS, then it is in conflict with the Identity Information Register, which is filled by „Principal and Credential Management“. If it is part of the Relying Party, then it is out of scope of this standard.	Drop 5.6.2.4	accepted
[AT] 11		5.8.1		TE	An identity cannot be activated, suspended or reactivated. These states would apply to credentials. There was a decision on Sophie Antipolis to exclude the life cycle definition from part 2	Remove the list from 5.8.1	accepted

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
[AT] 12		5.8.1, 5.8.2, 5.8.3, 5.8.4		TE	<p>5.8.1 is an incomplete subset of processes. General should include a balanced set of processes that would allow further decomposition.</p> <p>The description of the processes in 5.8.2 is too general to provide an actual value.</p> <p>The separation between 5.8.2, 5.8.3 and 5.8.4 is not explained and does not make sense when reading. A functional decomposition along the use case overview seems to be more obvious.</p>	<p>Use this decomposition of IMS processes:</p> <ol style="list-style-type: none"> <li>1. Consent Management</li> <li>2. Credential Management</li> <li>3. Entity Authentication</li> <li>4. Message Authentication</li> <li>5. Metadata Management</li> <li>6. Policy Management</li> <li>7. Principal Life Cycle Management</li> <li>8. Service Provisioning</li> </ol> <p>Process descriptions are included in the attached document "BPmodel AT".</p>	Resolved by adding process diagrams in an annex
[AT] 13		5,9		TE	<p>Tables as notation for information flows are very hard to understand and verify if they exceed any trivial size. They should be replaced by a graphical notation like BPMN, UML activity diagram or UML with business extensions. Instead of information/object flow the document should describe control flow, because there is no differentiation in information flow, so the information contents is low.</p>	<p>The process descriptions contained in the attached document „BPmodel AT” propose a notation using extended UML to describe control flows.</p>	Resolved by adding process diagrams in an annex

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
[DE1]		5.4.1		ED	<p>This section does not list the identity-information provider, which is explained in 5.4.6.</p> <p><i>“A reference architecture may recognize the following actors: principal; identity-management authority; relying party;  identity-information authority; verifier; and auditor.”</i></p>	<p>Add the new actor “identity information provider” after the “identity information authority”.</p>	<p>Editors have been given mandate to adopt improve text as commented where still possible</p>
[DE2]		5.4.3	all	TE	<p>Being responsible for setting up and enforcing operational policies for identity management, an identity management authority should not be expected to implement these policies itself by e.g. authorizing individual modifications. Such tasks are to be performed by an <i>identity registration authority</i> being responsible to authorize changes, activations etc. according to the policies set up by the identity management authority.</p> <p>The responsibilities of an identity registration authority are more likely to be combined in one entity with those of an identity information authority than with those of an identity management authority.</p>	<p>1. Add “identify registration authority” as a new actor to clause 5.4 after 5.4.3 with the text in Annex A.</p> <p>2. Modify the first two paragraphs and note of 5.4.3 as described in Annex B.</p> <p>3. Replace the last 4 bullet items in paragraph 6 by:</p> <p><i>-- to approve operational policies</i></p>	

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
[DE3]		5.4.5	I	TE	The function of IIA is not clearly distinguished from the IIP.	<p>Modify the text of paragraph one as follows:</p> <p>An identity-information authority is an actor in an identity- management system with the role as to provide authoritative source status to for identity information provided. An identity-information authority provides identity information on entities known in the domain managed by the system.</p> <p>Operationally an identity- information authority may be a service provider equipped to supply authoritative meta-data in conjunction with identity information. Provided identity information may be complemented with information to establish its reliability, e.g. cryptographic data authentication.</p>	accepted with editorial adjustments

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
[DE4]		5.4.7		TE	<p>The sentence</p> <p><i>“If evidence of identity is provided as a credential, the verifier should interact with the source of the credential to establish the validity of the identity information the credential contains.”</i></p> <p>seems to require an active interaction of the Verifier with the “source” of the credential (the Issuer). This is not always necessary, as it may create some privacy concerns for the Principal (the “source” may profile the Principal’s interactions with Verifiers). There are technologies, such as those based on privacy-enhancing attribute based credentials that avoid such a step. In fact, all a Verifier should check is whether or not the claimed credentials are still valid (i.e. not revoked/invalidated meanwhile). This does not necessarily involve a communication with the source of the credential, but can be outsourced to a different entity for that matter.</p>	<p>To avoid a potentially misleading description of the Verifier, the sentence should be rephrased. We propose the following:</p> <p>“If evidence of identity is provided as a credential, the verifier should interact with the source of the credential to establish the validity of the identity information the credential contains.”</p> <p>To</p> <p>“If evidence of identity is provided as a credential, the verifier must establish the temporal validity of the identity information the credential contains.”</p>	accepted with editorial adjustments
[DE5]		5.5.2.1	Figure 1	TE	Figure 1 does show some but not all stakeholders and actors.	Add verifier and identity information authority to figure.	rejected
[DE6]		5.6		ED	Misaligned chapters: 5.5.1 summarizes the two architecture views, which are then being described in detail in 5.5.2 Context view and 5.6 Functional viewpoint.	label 5.6 as 5.5.3	Editors have been given mandate to adopt improve text as commented where still possible

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
[DE7]		5.6.2.7		TE	<p>Use of identity information cannot be controlled at this point.</p> <p>Recording of access may be restricted by operational policies and/or privacy regulations and thus cannot be mandatory.</p>	<p>“The purpose of the identity information presentation and control component is to provide an interface to present identity information, to control access to <del>and</del> the use of identity information to authorized entities, and <u>–</u> where applicable – to record such access <del>and</del> use for later auditing.”</p>	accepted with editorial adjustments
[DE8]		5.6.2.7		TE	<p><u>The</u> importance of human readable form may not be necessary information needs to be expressed more clearly</p>	<p>Change to: “The documented design of an identity management system shall specify the format and conditions for the presentation of identity information <del>in</del> human readable form (see 6.2).”</p> <p>add text:</p> <p><i>Requirements in the documented design on the representation of identity information in human accessible form should take into account the capabilities and restrictions of the indented user of the information.</i></p>	accepted
[DE9]		5.8.1		TE	<p>Paragraph lacks specification of following processes (according to table 1):</p> <ul style="list-style-type: none"> <li>• Identification</li> <li>• Verification</li> <li>• Authentication</li> </ul>	<p>Add after list of management processes: “Furthermore, it specifies the processes of identification and authentication of a principal already known in the domain as well as verification of identity information.”</p>	resolved by AT11 (deletion)

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- ment2	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
[DE10]		5,9	Ta ble 1	TE	See comment on 5.4.3: Responsibilities moved to identity registration authority.	Replace all occurrences of “identity management authority” by “identity registration authority” In the generic identity management processes and identity information management processes.	resolved by editors mandate

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 1		Title Page		ED	Spurious error message in Dutch language	Suggest correct error or remove message	to be addressed by secretariat using ISO template
GB 2		Introduction	5th paragraph	TE	Missing word “reference” in Introduction	Suggest start sentence with "Defines a reference architecture for an identity management system....."	accepted
GB 3		Scope		GE	A proposed change of scope has been balloted and approved (27N12981) removal of 1st item in scope statement). However this change has not been implemented.	<p>Suggest implement approved scope change which is: This part of ISO/IEC 24760 provides guidelines for the deployment of an identity management system, and specifies the requirements of a framework for an identity management system.</p> <p>This International Standard is applicable to any information system where information relating to identity is processed or stored for the purposes of identifying and/or authenticating an entity.</p> <p>NOTE: This change requires a review of all existing text and alignment to the new scope.</p>	accepted



NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 4		3. Terms and Definitions		TE	Identity Management System (IMS) has not been defined in this part or in ISO 24760 Part 1. The term is used throughout the text in this document and also Figure 1. This definition also needs to align with Clause 5.1.2 in ISO/IEC 2ndCD 29146 Information technology — Security techniques — A framework for access management and ISO/IEC 29115:2012 generally.	Suggest add definition “mechanism comprising of policies, procedures, technology and other resources for maintaining information on digital identities, including attribute data, for the purposes of the identification and authentication of entities and other automated identity based decisions.”	rejected (implicit in definition of constituent terms)
GB 5		3. Terms and Definitions		TE	It would be useful to differentiate between a stakeholder and an actor in this section.	Suggest 'actor' is defined and cross- referenced to 'stakeholder'	acknowledged
GB 6		3.2 and throughout the document		ED	The inclusion of a hyphen in “identity-management authority” and “identity-information authority” is a continuing source of difficulty in this document for the following reasons: 1. The use of hyphenation is inconsistent throughout the document. 2. There is no apparent logic to the use of hyphens, e.g. identity-management authority has a hyphen but identity management system does not? 3. “identity information authority” is defined in 24760-1 without hyphenation but is (inconsistently) used in 24760-2 with hyphenation	Suggest: • Do not use hyphenation for terms defined in this standard. • Check for the consistent use of hyphens in all hyphenated terms in the text.	resolved by removing hyphens

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 7		5,1	Para 3. 2nd & 3rd sentences	ED	The English could be improved by merging the sentences and revising the wording	Suggest replace with: “Actors are stakeholders who interact directly with the identity management system.”	Editors have been given mandate to adopt improve text as commented where still possible
GB 8		5,2	Heading	ED	Number should be in bold	Suggest embolden heading number	Editors have been given mandate to adopt improve text as commented where still possible
GB 9		5.3, 5.4	General	TE	<p>The present description and characteristics of actors (being the subset of stakeholders who interact with an identity management system) is split between clauses 5.3 and 5.4. This split is awkward and unnecessary. The clarity and structure of the document would be improved by including all the descriptive text for each actor in a single place. This could be achieved by merging the current text in clauses 5.3 and 5.4 into a single clause with the “Stakeholder” heading. The various stakeholders could be described in sub-clauses 5.3.x. As the actors are the major stakeholders in an identity management system the ordering should place the actor sub-clauses before the non-interacting stakeholder sub-clauses.</p> <p>Other minor variations are possible, e.g. 5.3 Stakeholders 5.3.1 Actor stakeholders</p>	<p>We recommend that the text in clauses 5.3 and 5.4 is brought together and reorganised into a uniform structure such as that described at left.</p> <p>N.B. Detailed comments on and proposed changes to the current text of 5.3. and 5.4 are given below.</p>	rejected (after discussing documents design choice)

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
					<p>5.3.1.x ..... 5.3.2 Non interactive stakeholders 5.3.2.x ..... The actor sub-clauses would cover:</p> <ul style="list-style-type: none"> <li>• Description of role and function</li> <li>• Discussion of concerns</li> <li>• Description of interactions</li> </ul> <p>The non-interactive stakeholder sub-clauses would cover:</p> <ul style="list-style-type: none"> <li>• Description of role and functions</li> <li>• Discussion of concerns</li> </ul> <p>This simple uniform structure would place all the relevant description for each stakeholder (actor and non-actor) together in one place in the text. It would serve to emphasise that actors are a subset of all stakeholders while at the same time illustrating the interaction distinction between the actors and non-interactive stakeholders. Adopting this structure would aid the clarity and flow of the text in the document.</p>		Editors have been given mandate to adopt improve text as commented where still possible resolved by GB9
GB 10		5,3	Para 1	ED	<p>“. direct and indirect ...” These words are not needed as the distinction between actors and stakeholders is already described in 5,1 para 3 (see earlier GB comment on 5.1)</p>	Suggest delete words “direct and indirect”	
GB 11		5.3.1	Para 1, list of stakeholders	TE	<p>“identity information provider” and “verifier” appear as actors in clause 5.4, which means that they are also stakeholders</p>	Suggest add “identity information provider” and “verifier” to list of stakeholders	

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 12		5.3.1	Para 2, 2nd sentence	ED	Grammar: “by” should not be there	Delete “by”	Editors have been given mandate to adopt improve text as commented where still possible
GB 13		5.3.1	Para 2, 3rd sentence	ED	“a regulatory” This is a reference to item 5 in the previous list which has no indefinite article so the “a” should not be used here “advocates” should be “advocate” (same reason as previously “are operationally involved in” Wording could be improved	Delete “a”  Remove “s” from “advocates” Suggest: “interact operationally with”	Editors have been given mandate to adopt improve text as commented where still possible
GB 14		5.3.2	Principal, list of items	TE	Other concerns of the principal include the minimisation of identity information collected stored and processed and the use to which the identity information will be put by the identity management system.	Suggest add concerns: “- minimisation of identity information collected, processed and stored by the identity management system” and: “ – use made of identity information by the identity management system” “- correctness of data analytics used for identification purposes including treatment of false negative and false positive identification. “- transparency of identity data sharing – who what why and when”	accepted with editorial adjustments
GB 15		5.3.3	List item1	TE	Cost may be a practical concern but surely not one that is addressed by this standard?	Suggest remove cost from the concern list	accepted

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 16		5.3.3	List items 4 & 5	TE	The distinction between these two concerns is not clear. The business objectives for an identity management system would include meeting its business obligations	Suggest merge list items 4 & 5	accepted with editorial adjustments
GB 17		5.3.3	List item 6	ED	The concern could be expressed more clearly and in better English. There are two issues here 1. The information is accurate in that it applies to a real entity 2. The principal is that entity	Suggest: “that the identity information provided by each principal is accurate and pertains to that principal to a known level of assurance”	Editors have been given mandate to adopt improve text as commented where still possible
GB 18		5.3.4	List item 3	TE	“externally mandated criteria” Can this be more specific? Who is the external party? Is it the identity management authority? The relying party?	Suggest state that it is the external party that is referred to here.	accepted with editorial adjustments
GB 19		5.3.4	List items 3 & 5	TE	The distinction between these two concerns is not clear. The business objectives would include meeting externally mandated criteria. <del>Also what is the entity deploying the relying party? Is it not just the relying party that is meant here?</del>	Suggest clarify the distinction between list items 3 & 5 or merge the two concerns and identify the relying party as the source of the “externally mandated criteria”. (see also GB18)	resolved with GB18
GB 19		5.3.4	List items 3 & 5	TE	<del>The distinction between these two concerns is not clear. The business objectives would include meeting externally mandated criteria.</del> Also what is the entity deploying the relying party? Is it not just the relying party that is meant here?	Suggest clarify the distinction between list items 3 & 5 or merge the two concerns and identify the relying party as the source of the “externally mandated criteria”. (see also GB18)	accepted by removing bullet item

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 20		5.3.5	List of concerns	TE	The replying party also has a concern that the identity information and authenticated identity that is supplied to it by the identity management system meets its identity and authentication assurance criteria.	Suggest add this concern to the list of concerns.	resolved with new wording
GB 21		5.3.6	List item 1	ED	“description” Policy would normally imply documentation which would be a better word here than “description”.	Suggest change “description” to “documentation”	Editors have been given mandate to adopt improve text as commented where still possible
GB 22		5.3.6	List of concerns	TE	There are other concerns including: a. Compliance of operational policy and operational practice with legal and regulatory requirements b. Proper accountability and audit of system operations	Suggest add these two concerns	resolved with new wording
GB 23		5,4	General	TE	This clause describes actors who are distinguished from non-interacting stakeholders by their interactions with the identity management system. However currently these interactions are not described. See also 5.4.1 Note	Suggest describe the actor interactions with the identity management system, in a generic form even though all possible variations cannot be foreseen.	Acknowledged

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 24		5.4.1	Para 3	ED	“A reference architecture may recognize the following actors:” As this standard is titled “Reference architecture and requirements” it is this reference architecture that is being referred to here so the indefinite article “A” should be the definite article “The”. Similarly the actors referred to are the actors described in this standard so “may” is not the right word.	Suggest change wording to: “The reference architecture recognizes the following actors.”	Editors have been given mandate to adopt improve text as commented where still possible accepted
GB 25		5.4.1	Para 3, list of actors	TE	identity information provider does not appear in the list but is described in 5.4.6	Suggest add identity information provider to list of actors	
GB 26		5.4.1	Para 4, last sentence	ED	“Access management may be implemented as specified in ISO/IEC 29146” Is this a recommendation or merely a statement of fact?	Suggest that if this is intended to be a recommendation, change “may” to “should”	Editors have been given mandate to adopt improve text as commented where still possible
GB 27		5.4.3	Paras 1-3	ED	The information in these paragraphs is not presented in the right order. The first paragraph should describe the basic role and functions of the identity management authority. This is currently split across paragraph 1 and paragraph 3. The issue of domain of applicability (should this be authority?) should follow the core description.	Suggest reorder the information in paras 1-3 as indicated at left.	

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 28		5.4.3	Para 4 and associated Notes 1 & 2	TE	“An identity management authority may be a group of entities;” Unclear what this means or what entities are referred to “each possibly assigned one ore (sic) more of the operational responsibilities” Also unclear what this means. N.B. The actual meaning of the paragraph appears to be contained in Notes 1 and 2.	Suggest delete para 4. Promote the notes to paragraphs in the main body of the text.	resolved by replacing the text of the paragraph by note 2.
GB 29		5.4.3	Para 5, list of IMA responsibilities	TE	Missing responsibility: to ensure legal and regulatory compliance of the policies and operation of the identity management system	Suggest add missing responsibility as per comments	accepted
GB 30		5.4.3	Para 5, list item 5	TE	“to authorize modification ....” The IMA may also be responsible for requiring the modification in discharge of its duties to monitor the operations of the IMS and ensure compliance to policy, regulation etc.	Suggest change wording to: “to require and authorize modification ....”	accepted with editorial adjustments
GB 31		5.4.3	Para 5, last list item	TE	“to authorize modification of identity information recorded in the repository” Unclear what kind of modification this refers to. The IMA cannot be called on to authorize every detailed change of data for any principal whose identity information is held in the repository, e.g. change of address? Presumably this is intended to relate to fundamental changes such as new kinds of identity information to be collected and stored, new uses to be made of identity information etc? However this is already covered by the previous item in the list	Suggest clarify intended meaning and scope of modifications of identity information that lie within this responsibility. Alternatively if this is already covered by the previous list item, delete the last item.	resolved by deleting the last bullet.



NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 32		5.4.3	Para 6	TE	<p>This paragraph describes a particular model of a federated IDMS which is certainly not the only possible model and may not be typical. The model assumes that the IMA for a particular IMS is the initiator of the federation and will effectively become the IMA for the federation.</p> <p>In reality each existing IMS that is a putative member of the future federation will have its own IMA. The IMA could be part of the organisation operating the IMS or alternatively a separate independent body. An important issue concerning a federated IMS (which is not currently addressed by this document) is whether a federated IMS should/shall be responsible to a single federation IMA. The answer to this question will inform the content and requirements of this standard.</p>	Suggest for discussion in Hong Kong	resolved with new wording

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 33		5.4.3	Para 6, list item 1	ED	<p>“shall provide a level of assurance in identity information that meets the minimum requirement of any other member of the federation.</p> <p>It is difficult to be sure about how this would operate in practice but a likely scenario is that of a group of members wishing to form a federation who would agree amongst themselves on a common assurance level of identity information for the federation, in accordance with their business requirements. The role of the federation IMA would be to ensure that the policies and procedures of the federation members meet the legal and regulatory requirements associated with the defined level of assurance. In this scenario the IMA would be unlikely to “provide” the level of assurance; rather to monitor its correct implementation and operation.</p>	Suggest change “minimum” to “specified” Change “any other member” to “members”	Editors have been given mandate to adopt improve text as commented where still possible
GB 34		5.4.3	Last para, Note 4	ED	Missing word “identity” before “management”	Suggest insert “identity” before “management on last line of Note 4	Editors have been given mandate to adopt improve text as commented where still possible

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 36		5.4.6	Para 2	TE	<p>The descriptions in this list are difficult to understand and to reconcile with the collection, storage, maintenance and provision functions described in the previous GB comment.</p> <p>Does the “observer” responsibility correspond to the “collection” function?</p> <p>Does the “encoder” responsibility correspond to the “storage” and “maintenance” functions?</p> <p>Unclear what the “information generator” responsibility refers to.</p> <p>Does the “provider” responsibility correspond to the “provision” function”?</p>	<p>Suggest replacing text of para 2 with:</p> <p>“The core responsibilities of an identity information provider are:</p> <ul style="list-style-type: none"> <li>! to collect identity attributes from principals;</li> <li>! to assemble the requisite identity attributes into identity information that is used by the identity management system to identify principals;</li> <li>! to format the identity information into an identity record and to store the record in the identity register of the identity management system;</li> <li>! to maintain identity information in the identity register to reflect changes that may occur in the identity attributes of principals;</li> <li>! to extract identity information from the identity register and provide it to relying parties.</li> <li>! 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.</li> </ul>	accepted

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 38		5.4.6	Para 4	TE	<p>The wording should be revised to aid clarity</p> <p>N.B. “a description of the process used in establishing the value, or a reference to such a description” Unclear what this means. Is it a reference to identity proofing data and its validation associated with identity information?</p>	<p>Suggested change “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; formatted versions of identity 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 records; date and time of expiration of validity of identity attributes and identity information records; references to the source of identity information; cryptographic data used to protect the confidentiality and integrity of stored and communicated identity information and any associated metadata.” Clarify meaning of list item 4.</p>	accepted with editorial adjustments

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 39		5.4.6	Para 5	ED	Wording could be improved	Suggested change “An identity information provider may create a credential containing identity information that can be used to authenticate a principal. The credential may be cryptographically signed by the identity information authority to validate its authenticity. A credential is typically a physical token that is machine and human readable.”	Editors have been given mandate to adopt improve text as commented where still possible resolved by DE2
GB 40		5.4.7	Title	TE	The verifier is responsible for the identity proofing function but that is not obvious from the name	Suggest change name to “identity proofer” or “identity information proofer”	
GB 41		5.4.7	Para 2	TE	“An identity management system may contain multiple complementary verifiers .....” This paragraph seems to be an unnecessary complication. Para 1 already states that identity evidence may include previously issued identity credentials (in fact it can be argued that all items of identity evidence are identity credentials in that they provide credence of identity - e.g. a utility bill). It is difficult to understand the purpose of introducing the new terms “ <i>authentication verifier</i> ” and “ <i>assertion consumer</i> ”, which do not appear elsewhere in the standard? Note 1 says what needs to be said	Suggest delete para 2 and elevate Note 1 to become para 2.	resolved with NZ16 and new wording

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 42		5.4.8		TE	The clause should begin with a brief description of the role of the auditor	Suggested change “The role of the auditor is to examine the operational records of an identity management system in order 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.”	accepted
GB 43		5.5, 5.6	Structure and title of clauses	Ed	Sub-clause 5.5.1 describes two viewpoints, the context viewpoint and the functional viewpoint. 5.5.2 describes the context view. Logically then 5.5.3 would be expected to describe the functional view. However the functional view appears in clause 5.6 where it is incorrectly titled “viewpoint”	Suggest correct the structural and title issues. This could be accomplished in a number of ways, e.g.: a. Renumber 5.6 and its sub-clauses as 5.5.3 + 5.5.3.x sub-clauses and change subsequent clause numbers in document - OR b. Retitle 5.5 as “Architectural viewpoints and renumber 5.5.1.1 – 5.5.1.3 as 5.5.1 – 5.5.3. Follow with 5.6 Context view and 5.7 Functional view. Update subsequent clause numbers accordingly.	Editors have been given mandate to adopt improve text as commented where still possible

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 44		5.5.1.1	General	TE	<p>The 1st line is not appropriate to the introduction</p> <p>Notes 1 &amp; 2 are at the start of the clause and form its main part. This is not an appropriate status for Notes.</p> <p>The normative requirement includes “may” in the 2nd sentence. Is this intended to be a recommendation or merely a statement of fact?</p>	<p>Suggest delete 1st line</p> <p>Suggest reorganise the content of the clause as follows:</p> <p>! Brief introduction to the subject of viewpoints</p> <p>! Content of Notes 1 &amp; 2 elevated to the main body of the text (N.B.</p> <p>In Note 1, 1st sentence the clause referred to is not literally “this clause”. It is “the following clauses”)</p> <p>! Statement of normative requirement</p> <p>! Recommendation or statement of fact in a new paragraph</p>	<p>accepted with editorial adjustments</p> <p>acknowledged</p>
GB 45		5.5.1.2, 5.5.1.3	General	TE	<p>These clauses do not seem to contain information specific to an identity management system architecture. It looks like the content may have been simply copied from ref [7]?</p>	<p>Suggest clarify if the content of 5.5.1.2 and 5.5.1.3 is copied from ref [7]. If so, state it explicitly at the start of each clause (and confirm that permission to use has been granted).</p>	

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment2	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 46		5.5.2.1	Figure 1	TE	<p>“Figure 1 shows the context model for an identity management system, showing non-acting stakeholders and external actors as specified in this International Standard”</p> <p>In Figure 1 the only stakeholders listed in 5.3 and not shown are: “identity information authority” and “verifier”</p> <p>The text above Figure 1 implies by omission that only internal actors are not shown, which means that “identity information authority” and “verifier” are the only stakeholders classed as internal actors (as they are not shown).</p> <p>It is not clear how the internal/external classification was determined for each actor. Why is the identity management authority (shown) classed as an external actor whereas the identity information authority (not shown) is classed as an internal actor? Similarly for the “verifier”. There is no apparent logic in this classification.</p>	<p>Suggest abandon the internal/external classification scheme. Show all the stakeholders (actors and non-actors) in Figure1. Connect the interacting stakeholders (actors) with solid lines to the IDMS and the non-interacting stakeholders with dashed lines (or no lines at all). Add a key to explain the two line types.</p>	rejected



NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 47		5.5.2.2	General	TE	It is difficult to reconcile the interactions listed in para 2 with the interaction lines shown in Figure 2. A cursory inspection suggest that there is no close correspondence and there may be some inconsistencies, e.g. 2nd list item: “ a principal providing identity information to a relying party in order to obtain access to a resource” There is no line in Figure 2 connecting the principal to the relying party. Similarly with other list items	Validate the descriptions against the Figure. Suggest label each line relevant to the description in Figure 2. In the description of each interaction, state the line label in Figure 2 corresponding to each significant step in the description. Doing this will have the twin benefits of helping the reader to understand the use-case transactions described in the standard and helping the editor to validate the descriptions against the Figure.	resolved with AT3 and new wording to several clauses
GB 48		5.5.2.2	Para 3, (under Figure 2), 1st sentence	ED	Wording could be improved	Suggested change “The example use case diagram in the figure shows both administrative activity (Manage Identity Information) and online activity including authentication.”	Editors have been given mandate to adopt improve text as commented where still possible
GB 49		5.5.2.2	Para 4?	ED	“To facilitate ....” Is this the start of a new paragraph?	If it is a new paragraph, suggest include correct paragraph spacing. If not, flow the text from the previous line.	Editors have been given mandate to adopt improve text as commented where still possible

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 50		5.5.2.2	Para 4?	TE	Communities: what are organisational users and non-organisational users? Are organisational users, persons employed by the organisation that operates the identity management system to operate the system? Are non-organisational users the principals?	Suggest add an explanation of the meaning of organisational and non-organisational users. Also note that 'organizational' uses a 'z'	acknowledged
GB 51		5.5.2.2	Last para	TE	This sentence does not follow well from the earlier text in the clause because it refers specifically to authentication whereas the earlier description concerns an access request which involves more aspects of identity management than authentication.	Suggest revise the wording to tie in better with earlier content of the clause, e.g. “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”	accepted
GB 52		5.5.2.3 – 5.5.2.8	General	TE	The reader of this document will find much of the content of these clauses is incomprehensible. From: <a href="http://en.wikipedia.org/wiki/Use_case">http://en.wikipedia.org/wiki/Use_case</a> “In <u>software</u> and <u>systems engineering</u> , a <b>use case</b> is a list of steps, typically defining interactions between a role (known in <u>Unified Modeling Language</u> (UML) as an " <u>actor</u> ") and a system, to achieve a goal”	Suggest that the descriptions and figures should be remodelled to show the steps defining the relevant actor interactions for each goal of the use case as described and illustrated in the Wiki article.	resolved by adding diagrams to an annex
GB 53		5,6	Title	TE	The title of the clause is “Function viewpoint” but the content of the sub-clauses is not about viewpoints but describes various views.	Suggest change title to “Functional view” – see also earlier GB comment on structure of clauses 5.5 and 5.6	resolved with AT6

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 54		5.6.1, 5.6.2	General	TE	It would be better to describe the component view before the physical view. The component view describes the logical constructs (e.g. interfaces, databases, data structures, functions, operations etc.) that are needed to provide the functionality of the IDMS. The physical view describes the practical implementation of the IDMS in terms of its architecture and hardware (e.g. physical interfaces, computers, data stores, networks, communications channels etc.). They should be described in that order because the physical realisation is derived from the functionality (plus external drivers – cost, environment etc.) and not the other way round.	Suggest reverse the order of the component view and the physical view	accepted
GB 55		5.6.2	Para 2, list item 1	TE	“communications addresses” Unclear what this means	Request an explanation of the meaning of “communication addresses” and its significance in the architectural view	accepted by removing the words "communication address"
GB 56		5.6.2	Para 2, 3rd list item	ED	“like”; - “such as” would be better “tickets”; - Unclear what these are. Should it be “credentials”?	Suggest replace “like with “such as” Explain meaning of “tickets”. Change to “credentials” if that is what is meant.	Editors have been given mandate to adopt improve text as commented where still possible

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 57		5.6.2	Figure 3	TE	<p>1. Names in boxes in figure do not exactly correspond to the names in the item list preceding the figure</p> <p>2. “Principals” and “Actors” are shown as distinct entities but Principals are Actors. [we appreciate the wish to separate Principals from other Actors here because of their special significance in the functional view but it would be better to acknowledge that they are nonetheless Actors.</p> <p>3. Except for Principals, the actors are not distinguished in Figure 3. It is unclear why it was not felt necessary to provide this distinction</p> <p>4. “Domain of applicability”. The Principal does not interact with the Domain of applicability as shown in the figure. Rather the IDMS, its principals and other actors and stakeholders operate within the domain of applicability.</p>	<p>Use consistent names</p> <p>Suggest either:</p> <p>a. Use a single icon for all Actors but split internally to separate principals from other Actors, OR</p> <p>b. Label the icons: “Principal Actors” and “Other Actors” (but also see following comment)</p> <p>c. Consider whether it would be beneficial to distinguish all Actors in Figure 3</p> <p>d. Remove the internal icon labelled “Domain of applicability”. Add an enclosing box around Figure 3 labelled “Domain of applicability”</p>	resolved with AT7
GB 58		5.6.2.2 and Figure 3	Para 1	TE	<p>The domain of applicability is not a component of the IDMS. It is the context within which the IDMS and its stakeholders and actors operate and which defines the boundary for the architectural description of the IDMS. The reference to: ”services and resources available to the principal” suggests that the description here is in fact referring to “Relying party” described in 5.3.5 and 5.4.4</p>	<p>Suggest rename 5.6.2.2 to “Relying party”. Replace “Domain of applicability” box in Figure 3 with “Relying Party” box. (see also related comment 4 and proposed change (d) on Figure 3)</p>	resolved with AT9

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 59		5.3.7		TE	<p>Distinguish between Consumer Advocates and Consumer Representatives as they are significantly different roles ( see attached annex to this comments document )</p> <p>Then the documents needs to be adjusted to use the role Consumer and citizen representative rather than consumer advocate.</p>	<p>Suggest add: “Consumer ( and citizen ) Representatives</p> <p>Consumer and citizen representatives are those individuals selected by recognised consumer organisations to act as stakeholder representatives of consumer and public interest concerns.</p> <p>Consumer and citizen representatives participate in recognised multi- stakeholder societal processes such as governance and establishing good practice and requirements to be met by those providing goods and services to consumers and citizens.</p> <p>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.”</p>	accepted
GB 60		5.4.2		TE	The definition of a Principal needs to include that part of the role where identifiable data is	Suggested change:	accepted

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
					<p>collected by automatic means and auto-identification occurs as part of the processes for which that data is processed. <i>See last bullet in the proposed change</i></p> <p>The proposed change also tidies up and changes some English terms and usage to be clearer.</p>	<p>“5.4.2 Principal A principal is an actor who provides identification information to establish and validate to their identity within identification management processes. The Principal has the following responsibilities: - as an enrollee when intending to become known in 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 information in the identity management system and to be authorized for access to services or use of resources available in the domain of applicability associated with the identity management system _ - as reviewer, the right to know what identity information pertaining to itself is held in the identity management system and the right for 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. - As the subject of observation and initially anonymous data</p>	

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
						collection”	
GB 61		5.5.2.5 and 5.5.2.6 5.5.2.2 and 5.8.3.4		TE	<p>Consumer Cases.</p> <p>It is important that a consumer/citizen case is included for the situation where someone’s identity has been ‘stolen’ and they need to re-establish their credentials.</p> <p>In a real life example stolen personal information has been used to impersonate and individual in a mobile phone outlet claiming a lost ‘sim’ card for a phone with mobile banking where the phone’s details ( based on the sim card ) were used to access the bank accounts of the individual. The accounts were ‘cleared out’ i.e. £30,000 stolen and the individual then had to re-establish their identity with the bank concerned and then a process to pass the revised validation data out to other systems and parties to whom the pervious and now invalid identity data had been passed so it could be replaced.</p>	Suggest add a consumer case for re-establishing identity after the original information has been lost or stolen. The case to include both re-establishing the identity information data set of the for the original identity data collection party but also the subsequent tracing of who else had the ‘old’ data and ensuring that they are updated accurately with the new data.	accepted with editorial adjustments

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 62		5.6.2.4 and also relevant to 5.6.2.7 and 5.8.2.3		TE	<p>5.6.2.4 Identity information collector This description needs to cover the issue of pervasive sensing where data collected from many sources may be processed using data analytics to identify individuals. As an example cameras are a major source of such data which may be shared with many parties who then apply with biometrics algorithms to undertake identification.</p> <p>Such identification technology and processes require good governance to like the identification by analysis with the purpose of the identification to ensure identification only occurs when legal within properly governed processes.</p> <p>This aspect of identity management is of particular concern for the Internet of Things and linked to that Smart Cities.</p>	Suggest add a sub section to deal with identification by processing ( data analytics ) of sensor data, remembering that such sensor data may be accessed by many parties for many reasons and that identification occurs after data analytics have been undertaken.	resolved with AT10
GB 63		5.6.2.8		TE	<p>5.6.2.8 Identity information quality and compliance add a further bullet points to cover the inaccuracy of identification issues</p>	Suggest add bullets “- processes for dealing with false positive identification - processes for dealing with false negative identification”	accepted



NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
GB 64		5.7.5		TE	Delete text as it is incorrect	Suggest use text provided in previous GB comments. Using the issuance of ePassports and the inspection of ePassports. Proposed text. "Some identity management systems operate where independent organisations issue credentials conforming to a specification to principals and relying parties rely on such credentials provided by principals based upon a commercial risks assessment. "	accepted
GB 65		5.8.3.4	1st para after Note	TE	Invalidation The consumer significant case of your identity information having been invalidated by a 3rd party needs to be included. Add extra bullet points	Suggested addition "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."	accepted

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- ment2	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
[JP]1		5.4.6	Text	TE	<p>There was a discussion about Registration Authority (RA) functionality based on JP14 at Korea meeting. To reflect the discussion, the functionality should be written somewhere in Identity-information provider.</p> <p>The place may be around:</p> <ul style="list-style-type: none"> <li>- as observer,</li> <li>- as information generator,</li> <li>- as provider, ...</li> </ul> <p>Current explanation is not sufficient.</p> <p>We still think that “as Registration Authority (RA)” is the most comprehensive and direct expression. However, there may be alternative expression.</p> <p>At least, a reference to 29003 is necessary, although its title change is also discussed. (Current 29003 title is “Identity Proofing”)</p>	<p>Suggest a proposed text like following:</p> <ul style="list-style-type: none"> <li>- as information generator, the quality of identity information must be kept. (See, ISO/IEC 29003)</li> </ul> <p>Request to discuss at the meeting.</p>	resolved with DE2 and new wording.
[JP] 2		5.4.8	text	TE	<p>The expression of “Responsibility of ...include: ” is logically not correct. Not all the elements; reporter, monitor, advisor and supervisor are included at the same time.</p>	<p>Suggest a proposed text like following:</p> <ul style="list-style-type: none"> <li>- as reporter,</li> <li>- as monitor,</li> <li>- as advisor,</li> <li>- as supervisor,</li> </ul> <p>Other logical expression may be possible.</p>	accepted

[JP] 3		5.5.2.2	Figure 2	ED	This figure is not comprehensive.	Suggest dividing usage activity and administrative activity Cleary in the figure.
--------	--	---------	----------	----	-----------------------------------	--

Editors have been given  
mandate to adopt improve  
text as commented where  
still possible

NB1					Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- ment2	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
US1	ALL						TE	Since the terminology and concepts in ISO 24760-2 are not aligned with ISO 29115, and thus cause confusion with the lack of harmonization between the Identity related standards substantial progress needs to be made on aligning the terminology and concepts. The misalignment of terminology and concepts with ISO 29115 and ITU-T X.1252, (a joint ITU-T/ISO/IEC project) is a major concern to us as it will bring into question the credibility/viability of ISO 24760-2.	Align the terminology and concepts between 24760-2 and 29115	acknowledged (no technical changes proposed)

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- mentz	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
NZ 1				GE	Terminology used in 24760 differs from terminology emerging in operational standards such as 29115 and 29003	Terminology set prior to the establishment of practice is bound to require refining.  Schedule a review for all 24760 standards once practice is accepted.	acknowledged
NZ 2		Introduct ion	1	TE	“...make decisions based on the identity of a ....”  Decisions are rarely if ever made based on identity alone but also require input from other aspects such as eligibility and authority.	Decide if the topic is Identity Management or Identity Information Management or Personal Information Management or Access Management or a combination. This document weaves between all and is clear about none.	acknowledged (no technical changes proposed)
NZ 3		1	1	TE	‘identity information’ as defined by Part 1 is all information relating to an entity, potentially restricted by domain. This is too wide a definition for a single life cycle model. Different information will have different life cycles.	Decide what types of information are explicitly included in the identity management system.  Reword “- describes the life cycle models of identity information”	resolved by GB3
NZ 4		3,3		ED	The way ‘Principal’ is used in this standard is sometimes ‘entity type’ and ‘subject’ as used in other standards. The note relates to its use as the former.	Reuse existing terminology where possible or add ‘subject’ and ‘entity type’ as synonyms and add a note to explain its use as the entity of focus in a transaction e.g. verification check	resolved by adding synonym
NZ 5		5.3.1		ED	No hyphen in identity information authority	Remove the hyphen from identity information authority  And throughout rest of document	Editors have been given mandate to adopt improve text as commented where still possible
NZ 6	3rd bullet	5.3.2	1	ED	Typo – should be identity	Change identify to identity	Editors have been given mandate to adopt improve text as commented where still possible
NZ 7	6th bullet	5.3.3	1	ED	Grammar – what is ‘it’?	Reword for clarity	Editors have been given mandate to adopt improve text as commented where still possible

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- mentz	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
NZ 8		5.4.1	3	ED	"The documented design shall specify means to authenticate...." This should include 'identify'	Change "...means to identify and authenticate..."	Editors have been given mandate to adopt improve text as commented where still possible
NZ 9	2nd bullet	5.4.2		ED	Inconsistent font	Correct font	Editors have been given mandate to adopt improve text as commented where still possible
NZ 10		5.4.3	5	ED	Typo "...assigned one ore more..."	Remove 'e' from 'ore'	Editors have been given mandate to adopt improve text as commented where still possible
NZ 11		5.4.3	Note 2	ED	Typo extra word 'is'	Remove 'is'	Editors have been given mandate to adopt improve text as commented where still possible
NZ 12		5.4.3	Note 2	ED	Typo "...more identity managements systems..."	Remove 's' from 'managements'	Editors have been given mandate to adopt improve text as commented where still possible
NZ 13		5.4.4		TE	This use of Relying Party differs from the definition given in 24760-1	Use correctly or rename	resolved with new wording
NZ 14		5.4.5	3	ED	List should include credential strength	Level of assurance policy also needs to apply to the strength of the credential, not just identity and provisioning.	Editors have been given mandate to adopt improve text as commented where still possible
NZ 15		5.4.6		TE	How is the identity information provider different from the identity information authority	Clarify the difference	resolved with DE3

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
NZ 16		5.4.7	3	TE	Establishing that an entity is the principal is identity proofing not authentication. Use the term defined by 29003 for this role.  'assertion consumer' as defined in this paragraph appears to be 'Relying Party' as defined in 24760-1	Change 'authentication verifier' to 'Identity proofing and verification service provider (IPVSP)'  Use 'Relying Party' as this has already been defined.  In either case if a new term is being established then they should be described in the definitions and reused within the document otherwise what is the point of naming them at all.	resolved with new wording
NZ 17		5.5.1.1	Note 2	ED	Unnecessary comma	Remove the comma after '...should be focussed.'	Editors have been given mandate to adopt improve text as commented where still possible
NZ 18		5.5.2.1	Fig 1	ED	Should not have roles or actors that have not been defined or described	Redo diagram to only use terms that have been described or defined.	Editors have been given mandate to adopt improve text as commented where still possible
NZ 19		5.5.2.2		TE	Unable to translate this into an operational context.	Suggest this may need to be informed by operational standards	acknowledged
NZ 20		5.5.2.3	1	TE	What is meant by ...the actual person not as an individual'?	Clarify	resolved by deleteing the sentence
NZ 21		5.5.2.5		TE	In a pure identity context the fact of citizenship is not relevant. For a start it does not apply to all entity types and it is usually a factor of eligibility which is different from identity.	Remove use case	accpeted

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- mentz	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
NZ 22	3rd bullet	5.5.2.8		ED	Typo – should be an 's' on the end of 'type'	Change to '...to different types...'	Editors have been given mandate to adopt improve text as commented where still possible
NZ 23	5th bullet	5.5.2.8		ED	New term 'owner' and typo	Change to '...without the principal's consent...'  Or define 'owner'	Editors have been given mandate to adopt improve text as commented where still possible
NZ 24		5.6.2	Fig 3	ED	New term 'Identity Information Collector'	Use existing term/s.	Editors have been given mandate to adopt improve text as commented where still possible
NZ 25		5.6.2.6	1	TE	Implies that the identifier must be a single attribute where it can be a combination of attributes. Some jurisdictions have restrictions on the exchange of unique identifiers.	Reword last sentence to allow for a set of attributes for a principal that when combined is distinct from the same set of attribute for any other principal	resolved with new wording
NZ 26		5.6.2.6	2	TE	While it is administratively efficient to assign a unique identifier it should be noted that these identifiers may be private to the system or even subparts of the system.	Make it clear that assigned identifiers may not be able to be used outside the register.	accepted with new wording
NZ 27		5.6.2.6	Note 3	ED	Should include a sub note that this may only be done where legislation and or privacy allow.		Editors have been given mandate to adopt improve text as commented where still possible
NZ 28	1st bullet	5.6.2.6	3	ED	Typo '...together with an justification...'	Remove 'n' from 'an'	Editors have been given mandate to adopt improve text as commented where still possible



NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- mentz	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
NZ 29		5.8.1		TE	<p>The list of processes assumes a specific focus of what identity is, which is unclear. See NZ 3</p> <p>These processes do not apply to identity as defined by 24760-1 which implies that identity is all information in a domain relating to the entity.</p> <p>These processes do not align with the processes / transitions outlined in 24760-1</p>	<p>Define what identity actually is.</p> <p>Determine if the processes apply to all aspects of identity</p> <p>Or at least align with the context set in 24760-1 Section 7.</p>	resolved by AT11 (deletion)
NZ 30		5.8.2.2		TE	<p>First line ignores that it has already been determined there is an enrolment point. Ergo there must be a point at which information is provided where no information currently exists.</p> <p>Provisioning has a very specific meaning in relation to identity systems and this not it.</p>	Rename Identity information maintenance	accpeted
NZ 31		5.8.2.4		ED	Extra full stops at start of title and text	Remove unnecessary full stops	Editors have been given mandate to adopt improve text as commented where still possible
NZ 32		5.8.3.3		ED	Inconsistent use of the terms reference identifier and unique identifier	Use terms consistently throughout the document	Editors have been given mandate to adopt improve text as commented where still possible
NZ 33		5,9	Tabl e 1	TE	<p>This table is difficult to understand due to:</p> <p>a) the scope of identity not being sufficiently established b) the first section refers to 5.8.1 but then has different processes than were listed, likewise the second section</p> <p>c) assumes that the principal is not able to make choices on their own i.e. participate in certain processes</p> <p>d) should be able to be mapped to</p>	Needs rework	resolved with AT4, AT13

NB1		Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of commentz	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
					one or more of the diagrams		
NZ 34		6		TE	This section does not appear to align with 24760-1		resolved with new wording
NZ 35		6.3.3		ED	With only two inactive statuses – Suspended and Archived, neither allow for the ongoing reference to an identity by entities other than the principal entity who/which not longer exists.  The second sentence is illogical – making identity information anonymous means it ceases to be identity information and becomes something else	This means that either another lifecycle stage is required or it can not be a 'shall' requirement for archived identities to be made anonymous.	Editors have been given mandate to adopt improve text as commented where still possible
NZ 36		Annex A		ED	This section has not been titled Annex A	Add reference to Annex A to the title	Editors have been given mandate to adopt improve text as commented where still possible
NZ 37		Annex A		ED	Typo – 'An identity Management needs...'	Change to 'An identity management system needs...'	Editors have been given mandate to adopt improve text as commented where still possible