



DPC: 23 / 30429577 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 24 January 2023

Origin: International

Latest date for receipt of comments: 11 March 2023

Project No. 2020/03003

Responsible committee: IST/33/5 Identity Management and Privacy Technologies

Interested committees:

Title: BS ISO/IEC 24760-2 IT Security and Privacy - A framework for identity management

Part 2: Reference architecture and requirements

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 11 March 2023**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: **Mr Delme Stephenson (BSI)**Direct tel: **020 8996 7213**E-mail: delme.stephenson@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 24760-2

ISO/IEC JTC 1/SC 27

Secretariat: DIN

Voting begins on:
2023-01-16

Voting terminates on:
2023-04-10

IT Security and Privacy — A framework for identity management —

Part 2: Reference architecture and requirements

*Sécurité IT et confidentialité — Cadre pour la gestion de l'identité —
Partie 2: Architecture de référence et exigences*

ICS: 35.030

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.

This document is circulated as received from the committee secretariat.



Reference number
ISO/IEC DIS 24760-2:2023(E)
Documents
AVA Document Sharing Hub
© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	2
5 Reference Architecture	3
5.1 General	3
5.2 Deployment scenarios	3
5.3 Stakeholders	4
5.3.1 General	4
5.3.2 Principal	4
5.3.3 Identity management authority	5
5.3.4 Identity information authority	5
5.3.5 Relying party	6
5.3.6 Regulatory body	6
5.3.7 Consumer/citizen representative or advocate	6
5.4 Actors	7
5.4.1 General	7
5.4.2 Principal	7
5.4.3 Identity management authority	8
5.4.4 Identity registration authority	9
5.4.5 Relying party	10
5.4.6 Identity information authority	10
5.4.7 Identity information provider	11
5.4.8 Verifier	12
5.4.9 Auditor	13
5.5 Processes and Services	13
5.5.1 Documentation	13
5.5.2 Identity information management processes	14
5.5.3 Specific identity information management processes	15
5.5.4 Additional functions	18
5.6 Viewpoints	20
5.6.1 General	20
5.6.2 Context viewpoint	20
5.6.3 Functional viewpoint	21
5.7 Use cases	21
5.7.1 General	21
5.7.2 Principal use cases	22
5.8 Components	23
5.8.1 General	23
5.8.2 Principal	23
5.8.3 Identity register	23
5.9 Compliance and governance	24
5.10 Physical model	24
6 Architecture for managing internal identities	24
6.1 Deployment scenario	24
6.2 Context	24
6.3 Stakeholders & Concerns	25
6.4 Use cases	26
6.4.1 Employee use cases	26
6.4.2 Employer use cases	26

7	Architecture for managing external identities	27
7.1	Deployment scenarios	27
7.1.1	Service scenario	27
7.1.2	Federated scenario	27
7.1.3	Federated scenario as applied to services	27
7.2	Context	27
7.3	Stakeholders & Concerns	28
7.4	Use cases	29
7.4.1	Device use cases	29
7.4.2	Sharing use cases	29
8	Requirements for the management of identity information	30
8.1	General	30
8.2	Access policy for identity information	30
8.3	Functional requirements for management of identity information	30
8.3.1	Policy for identity information life cycle	30
8.3.2	Conditions and procedure to maintain identity information	31
8.3.3	Identity information interface	31
8.3.4	Reference identifier	31
8.3.5	Identity information quality and compliance	33
8.3.6	Archiving information	33
8.3.7	Terminating and deleting identity information	33
8.4	Non-functional requirements	34
	Annex A (informative) Legal and regulatory aspects	35
	Annex B (informative) Use case model	36
	Annex C (informative) Component model	39
	Annex D (informative) Business Process model	42
	Bibliography	47

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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

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

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1 *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 24760-2:2015), which has been technically revised.

The main changes compared to the previous edition are as follows:

- The leading parts of the title have been adapted to the new convention in ISO/IEC JTC 1/SC 27.
- In [Clause 3](#) the definitions of terms that have been moved in the second edition of ISO/IEC 24760-1:2019, have been removed;
- To address the emerging concept of mobile identity, the term “*principal’s private IMS*” with acronym “PPI” has been added as terminology item [3.1](#), which is further described in [5.4.2](#), [5.4.3](#) and [5.4.6](#);
- The structure of [clause 5](#) has been flattened with part of the content placed in new [clauses 6](#) and [7](#);
- Ambiguous references to (sub)clauses in the documents have been resolved;
- The document has been brought to better conformance with the ISO/IEC directives;
- The readability of figures in the annexes has been improved.

A list of all parts in the ISO/IEC 24760 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

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

To address the need to efficiently and effectively implement systems that make identity-based decisions, this document specifies a framework for the issuance, administration, and use of data that serves to characterize individuals, organizations, or information technology components, which operate on behalf of individuals or organizations.

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

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

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

This document 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 29101:2018, *Information technology — Security techniques — Privacy architecture framework*,
- ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*, and
- ISO/IEC 29146, *Information technology — Security techniques — A framework for access management*.

IT Security and Privacy — A framework for identity management —

Part 2: Reference architecture and requirements

1 Scope

This document

- 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 document is applicable to any information system where information relating to identity is processed or stored. This document is not a management system standard (MSS)

2 Normative references

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

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

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

ISO/IEC/IEEE 42010, *Software, systems and enterprise — Architecture description*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 24760-1:2019 and the following apply.

Note a cross reference for terms defined in all parts in the ISO/IEC 24760 series of standards is available in ISO/IEC 24760-1:2019 or in any accepted amendments.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1

documented design

authoritative description of structural, functional, and operational system aspects

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

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

3.2

identity management authority

entity responsible for setting and enforcing operational policies for an *identity management system*

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

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

3.3

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

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

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

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

3.4

regulatory body

formally recognized organization tasked and empowered by law, regulation, or agreement to supervise the operation of *identity management systems*

3.5

stakeholder

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

[SOURCE: ISO/IEC 42010:2011, 3.10]

3.6

principal's private IMS

PPI

identity management system holding identity information for a single principal, operated by, or under exclusive control of, this principal

Note 1 to entry: Note to entry: The wording “mobile identity” has been used to, among other concepts, refer to a principal's private IMS, e.g. as implemented on a mobile phone or as a dedicated processing token.

4 Symbols and abbreviated terms

ICT	Information and Communication Technology
IMS	Identity management system
PII	Personal identifiable information
PPI	principal's private identity management system

5 Reference Architecture

5.1 General

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

The documented design for the architecture of an identity management system should be based on ISO/IEC/IEEE 42010:2011 and address the primary concerns of this system, which can be one, or both, of:

- i) managing identity information for the members of an organisation, ([clause 6](#)) and
- ii) managing identity information for entities outside an organisation ([clause 7](#)).

NOTE 1 The reference architecture and architecture description specified in this document are based on ISO/IEC/IEEE 42010:2011

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 document. 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 document should use an appropriate architecture description language and reference architecture components and functions by terms defined in ISO/IEC 24760 (all parts).

This clause provides an overview of the components that may be present in one or more of the architectural views that can be specified in a documented design including:

- Stakeholders ([5.2](#)),
- Actors ([5.4](#)), and
- Processes and services ([5.5](#)).

[Clause 5.6](#) presents two commonly present viewpoints in an identity management system.

5.2 Deployment scenarios

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

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

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

- the enterprise scenario ([6.1](#)),
- the federated scenario ([7.1.2](#)),
- the service scenario ([7.1.1](#)), and
- the “federated scenario as applied to services” ([7.1.3](#)).

5.3 Stakeholders

5.3.1 General

The documented design may recognize the following direct and indirect stakeholders:

- principal,
- identity management authority,
- identity information authority,
- relying party,
- regulatory body,
- auditor,
- assessor,
- cloud service provider, and
- consumer/citizen representative or advocate.

Each stakeholder performs a separate function in the identity management system. These functions imply specific responsibilities and liabilities.

NOTE 2 The purpose of the deployment of an identity management system, and the regulatory environment of that deployment, indicates the involvement of stakeholders.

Stakeholders in a particular identity management system may be affiliated with different commercial or public organisations with their interests in the system shaped by this affiliation. As the information about the system available to different stakeholders may be different, interactions between stakeholders should be based on explicitly established trust relations.

The documented design shall specify concrete representations of its stakeholders and actors as defined in [5.3](#) and [5.4](#), respectively. The documented design may add additional stakeholders or actors. It may also specify the stakeholders and actors identified in [5.3](#) and [5.4](#) with multiple distinct representations.

Stakeholders as specified in this document can also be an actor; non-actor stakeholders are a *regulatory body* and a *consumer/citizen representative or advocate*.

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

NOTE 3 The text in bold after each description of a concern is used as a reference in [clauses 6](#) and [7](#). It can also be used as a reference in the documented design.

5.3.2 Principal

Concerns of a principal in an identity management system include

- correctness of identity information collected, processed and stored [**Data correctness**],
- protection of privacy [**Privacy**],
- minimisation of identity information collected, processed and stored by the identity management system [**Data minimisation**],
- minimisation of identity information usage by the identity management system in its domain of applicability [**Information sharing minimisation**],

- ability of different relying parties to correlate identity information for a single principal [**Principal correlation**]
- ability of a relying party to positively link the principal with their recorded identity information received to identity information it has already stored, e.g. a user account [**Correct authentication**],
- errors in identification including false negative and false positive identification and the detection and handling of errors [**Correct identification**],
- knowledge of and consent to, identity information sharing with third parties [**Information & consent**],
- being correctly represented by identity information captured, processed or stored [**Representative information**],
- correctness of operations in the delivery of services and the access to resources made available based on the attributes presented in a specific situation [**Correct operation**],
- collecting, processing and storage of identity information only occurs with its informed consent [**Processing consent**],
- equitable treatment in its interactions with the system [**Equitable**], and
- an easily understandable, effective, appropriate user interface [**Understandable**].

NOTE 4 A concern of a principal about how a third-party service uses identity information obtained from the identity management system is not a concern about the identity management system itself. Therefore such a concern need not be addressed explicitly in the documented design.

5.3.3 Identity management authority

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

- definition of identity management objectives for the domain(s) served by the identity management system [**Defined objectives**],
- specification of policies to maintain identity management objectives for the domain(s) served by the identity management system [**Policies specified**],
- that the business objectives of the identity management system with respect to principals and users of identity information are fulfilled [**Meeting user objectives**],
- that the business objectives of relationships with other identity management systems are fulfilled [**Meeting third party objectives**],
- that the identity information provided by each principal is accurate and pertains to that principal to a specific level of assurance [**Correct information**], and
- compliance with regulation [**Compliance**].

5.3.4 Identity information authority

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

- completeness, correctness and freshness of identity information [**Data quality**],
- meeting requirements from relying parties [**Meeting needs of relying parties**],
- effectiveness of cryptographic methods to assert identity information [**Appropriate assertions**],
- effectiveness of cryptographic methods to deidentify identity information [**Effective deidentification**],

- compliance with regulation [**Compliance**], and
- meeting business obligations with principals [**Meeting principal objectives**].

5.3.5 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 [**Required identity information**],
- provisioning of accurate identity information pertaining to relevant principals at the required level of assurance [**Quality of information**],
- effective, documented and secure interfaces [**Usable interfaces**],
- conformance to regulation applicable to its operations [**Compliance**], and
- effective mechanism and procedures for auditing [**Auditing**].

5.3.6 Regulatory body

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

- the proper documentation of operating policies [**Documented policies**],
- correctness of operation, in particular, in applying operational policies [**Correct operation**],
- proper accountability and audit of system operations [**Accountability**],
- compliance of operational policy and operational practice with legal and regulatory requirements [**Compliance**],
- effective reporting on system operations, including control effectiveness, incidents, and actions taken in overcoming incidents [**Effective reporting**], and
- effective response to incidents that violate, or have a potential to violate privacy protection [**Incident responsiveness**].

NOTE 5 Effectively, auditors, as actors in an identity management system (see 5.4.9), in inspecting the operations of an identity management system (see 5.5) may represent the interests of regulatory bodies.

5.3.7 Consumer/citizen representative or advocate

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

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

Consumer/citizen representative and advocates' main concerns are

- transparency, notification, compliance and protection against complex legal language [**Clear language**],
- availability of procedures to exercise the rights of consumer/citizen [**Accessible procedures**], and
- access of services to disadvantaged populations [**Accessible services**].

NOTE 6 Consumer and citizen representatives participate in recognised multi-stakeholder societal processes such as governance and establish good practices and requirements to be met by those providing goods and services to consumers and citizens.

NOTE 7 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.

5.4 Actors

5.4.1 General

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

NOTE 8 Actors could be directly related to the domain that uses an IMS or they can be third parties, which could be another IMS.

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

NOTE 9 One purpose of specifying actors in the design of an identity management system is to be able to describe all intended interactions with the system.

A documented design may recognize the following actors:

- principal;
- identity management authority;
- identity registration authority
- relying party;
- identity information provider;
- identity information authority;
- verifier;
- auditor.

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

5.4.2 Principal

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

- as an entity when applying to become registered in a domain of applicability, to provide accurate identity information for enrolment as a new principal,
- as system user once enrolled, to request to be recognized by the identity management system and to be approved for access to services or use of resources available in the domain of applicability associated with the identity management system, and
- as the subject of observation to obtain identity information, to facilitate the observation.

NOTE 10 As a subject of observation the identity information obtained is anonymous, until its relation to the principal has been established.

For a PPI, the Principal makes available a suitable hardware platform for the identity register and the execution environment for implementing IMS Functions. A PPI hardware platform may be provided by a domain where the principal is known or by a third party. Requirement for this hardware platform and its operations including issuance and data provisioning are beyond the scope of this document.

NOTE 11 The hardware platform can be a mobile phone in which case the IMS can be an implementation installed on the phone.

A principal can use an identity management system to

- request to be recognized by information in the identity management system and to be approved for access to services or use of resources available in the domain of applicability associated with the identity management system, and
- be informed, as human, of the identity information pertaining to itself is held in the identity management system and to request any errors in the identity information to be corrected

NOTE 12 In appropriately defined circumstances, a legally authorised representative may act on behalf of a principal.

5.4.3 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 13 A Chief Information Officer (CIO) in an organisation that uses an IMS typically acts as identity registration authority that person. In practice this actor may be realised by a compliance team

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

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

Responsibilities of an identity management authority include:

- to create, modify or revoke operational policies,
- to ensure legal and regulatory compliance of the policies and operation of the identity management system,
- to require and approve modification of mechanisms to establish a required level of assurance in entity authentication for access to identity information and system control functions
- to respond to incidents,
- to approve changes in the type of information recorded in the identity register
- to initiate regular audits, and
- to evaluate audit reports, in particular on the effectiveness of policies,

For a PPI the identity management authority is shared between the principal and an external party that has provided the implementation of the IMS, e.g. as an installable application. After deploying the IMS application, a principal can act in operational configuration enabled through a user interface provided

by the external party. After installation of an IMS application the identity management may be involved in supporting security to an engagement of one or more identity information providers or identity information authorities to be used by the IMS.

NOTE 14 The provider of the IMS application could support operational configuration by the principal with a number of menus to select from pre-configured options and policies.

An identity management authority may establish a business relationship with another identity management authority in order to share identity information and identity management operations, in particular authentication. Such a business relationship may be characterised as a federation if it involves multiple parties that share a common agreement. A business relationship that involves sharing of identity information shall be based on a formal agreement specifying methods to protect privacy, e.g. by using specific mechanisms of deidentification.

NOTE 15 The purpose of the business relationship is to extend the domain of applicability for principals with the other domains of applicability in a federation. This extension is achieved with strictly controlled sharing of identity information.

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

- to provide a level of assurance of identity information that meets the specified requirement of any other member of the federation,
- to maintain control over access to the identity information contained in its identity management system,
- to ascertain that the level of assurance realized by any other member of the federation in authorizing access to identity information in the federated identity management systems meets its requirements for access to its own identity information,
- to operate with common policies for information sharing, and
- to specify policies to maintain its trust in the level of assurance of authentication.

NOTE 16 Typically, in a federation, some of the identity management policies, in particular on authorization for access, will be part of an agreement between the identity management authorities involved in the domains.

NOTE 17 Identity management policies for use in multiple domains of applicability could be the subject of standardization.

NOTE 18 Changes to structure, organisation and extent of a data federation may be subject to external constraints such as legal or regulatory requirements or the granting of permission by regulatory bodies.

NOTE 19 Members of a federation may agree to delegate operational responsibilities of the identity management authority to a common operator, designated as the “federation authority”.

5.4.4 Identity registration authority

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

For a Principal's Personal IMS (PPI), an identity registration authority is a party external to that IMS, which the principal engages to obtain a specific level of assurance for the identity information registered in the IMS.

NOTE 20 The Principal can engage multiple distinct identity registration authorities for different, or the same, attributes.