



DPC: 14 / 30230396 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: 7 July 2014
Origin: International

Latest date for receipt of comments: 9 September 2014

Project No. 2010/01799

Responsible committee: IST/33 IT - Security techniques

Interested committees:

Title: Draft BS ISO/IEC 24760-2 Information technology - Security techniques - 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 9 September 2014**

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: Ms Anne Cassidy (BSI)
Direct tel: 020 8996 7430
E-mail: anne.cassidy@bsigroup.com

Introduction

This draft standard is based on international discussions in which the UK has taken an active part. Your comments on this draft are welcome and will assist in the preparation of the consequent standard. There is a high probability that this text could be adopted by CENELEC as a reference document for harmonization or as a European Standard. Recipients of this draft are requested to comment on the text bearing in mind this possibility.

UK Vote

Please indicate whether you consider the UK should submit a negative (with reasons) or positive vote on this draft.

BSI Committee Responsibilities

Whether or not the standard is published in its original (international) form, or as a formal British Standard Implementation the BSI committee's responsibilities are to:

- aid enquirers to understand the text;
- present to the responsible international committee any enquiries on interpretation, or proposals for change, and keep UK interests informed;
- monitor related International and European developments and promulgate them in the UK.

Submission of Comments

- The guidance given below is intended to ensure that all comments receive efficient and appropriate attention by the responsible BSI committee. **Annotated drafts are not acceptable and will be rejected.**
- All comments must be submitted, preferably electronically, to the Responsible Committee Secretary at the address given on the front cover. Comments should be compatible with version 6.0 or version 97 of Microsoft Word for Windows, if possible; otherwise comments in ASCII text format are acceptable. **Any comments not submitted electronically should still adhere to these format requirements.**
- All comments submitted should be presented as given in the example below. Further information on submitting comments and how to obtain a blank electronic version of a comment form are available from the BSI website at:
<http://drafts.bsigroup.com/>

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	Comment (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:
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)

Documents
Document Sharing Hub
© 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
Web www.iso.org

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

Violators may be prosecuted.

Contents	Page
Foreword	vi
Introduction.....	vii
1. Scope	1
2. Normative references	1
3. Terms and definitions.....	1
4. Symbols and abbreviated terms	4
5. Reference Architecture.....	5
5.1 General.....	5
5.2 Architecture elements	5
5.2.1 Overview.....	5
5.2.2 Viewpoints	5
5.3 Context view	6
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
5.4 Functional view	16
5.4.1 Component model	16
5.4.2 Processes and services	17
5.4.3 Physical model.....	22
5.5 Identity management scenarios.....	22
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
6. Requirements	23
6.1 General.....	23
6.2 Access policy for identity information	24
6.3 Functional requirements for management of identity information.....	24
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
6.4 Non functional requirements	27
Annex A Legal and regulatory aspects (Informative).....	29
Annex B Use case model (Informative)	30
Annex C Component model (Informative)	33
C.1 Model	33

C.2 UML legend 34

Annex D Business Process model (Informative) 36

D.1 General 36

D.2 Consent management. 36

D.3 Credential lifecycle management.....38

D.4 Configuration Data Management 39

D.5 Policy Management 40

D.6 Principal’s Life Cycle Management.....41

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	<i>Information technology — A framework for identity management — 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