INTERNATIONAL STANDARD

ISO/IEC 24760-2

First edition
2015-06-01

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

Part 2: Reference architecture and requirements

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

Partie 2: Architecture de référence et exigences

ISO/IEC 24760-2:2015 - Preview only Copy via ILNAS e-Shop

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

© ISO/IEC 2015

ISO/IEC 24760-2:2015 - Preview only Copy via ILNAS e-Shop



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015

All rights reserved. Unless otherwise specified, 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
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

© ISO/IEC 2015 – All rights reserved

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols and abbreviated terms ... **2**
5 Reference Architecture ... **2**
5.1 General ... 2
5.2 Architecture elements ... 3
5.2.1 Overview ... 3
5.2.2 Viewpoints ... 3
5.3 Context view ... 4
5.3.1 Stakeholders ... 4
5.3.2 Actors ... 7
5.3.3 Context model ... 12
5.3.4 Use case model ... 13
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 ... 23
5.5 Identity management scenarios ... 23
5.5.1 General ... 23
5.5.2 Enterprise scenario ... 23
5.5.3 Federated scenario ... 23
5.5.4 Service scenario ... 24
5.5.5 Heterogeneous scenario ... 24
6 Requirements for the management of identity information ... **24**
6.1 General ... 24
6.2 Access policy for identity information ... 24
6.3 Functional requirements for management of identity information ... 25
6.3.1 Policy for identity information life cycle ... 25
6.3.2 Conditions and procedure to maintain identity information ... 25
6.3.3 Identity information interface ... 26
6.3.4 Reference identifier ... 26
6.3.5 Identity information quality and compliance ... 27
6.3.6 Archiving information ... 28
6.3.7 Terminating and deleting identity information ... 28
6.4 Non-functional requirements ... 28
Annex A (informative) **Legal and regulatory aspects** ... **30**
Annex B (informative) **Use case model** ... **31**
Annex C (informative) **Component model** ... **34**
Annex D (informative) **Business Process model** ... **37**
Bibliography ... **47**

ISO/IEC 24760-2:2015 - Preview only Copy via ILNAS e-Shop

© ISO/IEC 2015 – All rights reserved

Foreword

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

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

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

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

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

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

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

— *Part 1: Terminology and concepts*

— *Part 2: Reference architecture and requirements*

The following part is under preparation:

— *Part 3: Practice*

Further parts may follow.

ISO/IEC 24760-2:2015 - Preview only Copy via ILNAS e-Shop

 © ISO/IEC 2015 – All rights reserved

Introduction

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

To address the need to efficiently and effectively implement systems that make identity-based decisions, this part of ISO/IEC 24760 specifies a framework for the issuance, administration, and use of data that serves to characterize individuals, organizations, or information technology components, which operate on behalf of individuals or organizations.

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

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

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

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

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

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

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

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

ISO/IEC 24760-2:2015 - Preview only Copy via ILNAS e-Shop

© ISO/IEC 2015 – All rights reserved

ISO/IEC 24760-2:2015 - Preview only Copy via ILNAS e-Shop

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

Part 2: Reference architecture and requirements

1 Scope

This part of ISO/IEC 24760

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

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

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

2 Normative references

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

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

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

3 Terms and definitions

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

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

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

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

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

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

ISO/IEC 24760-2:2015 - Preview only Copy via ILNAS e-Shop

© ISO/IEC 2015 – All rights reserved