INTERNATIONAL STANDARD

ISO/IEC 24760-3

First edition
2016-08-01

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

Part 3: Practice

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

Partie 3: Mise en oeuvre

This document is a preview generated by EVS

Reference number
ISO/IEC 24760-3:2016(E)

© ISO/IEC 2016

This document is a preview generated by EVS



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, Published in Switzerland

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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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 Mitigating identity related risk in managing identity information ... **2**
5.1 Overview ... 2
5.2 Risk assessment ... 2
5.3 Assurance in identity information ... 3
5.3.1 General ... 3
5.3.2 Identity proofing ... 3
5.3.3 Credentials ... 3
5.3.4 Identity profile ... 3
6 Identity information and identifiers ... **4**
6.1 Overview ... 4
6.2 Policy on accessing identity information ... 4
6.3 Identifiers ... 4
6.3.1 General ... 4
6.3.2 Categorization of identifier by the type of entity to which the identifier is linked 4
6.3.3 Categorization of identifier by the nature of linking ... 5
6.3.4 Categorization of identifier by the grouping of entities ... 6
6.3.5 Management of identifiers ... 6
7 Auditing identity information usage ... **6**
8 Control objectives and controls ... **6**
8.1 General ... 6
8.2 Contextual components for control ... 7
8.2.1 Establishing an identity management system ... 7
8.2.2 Establishing identity information ... 9
8.2.3 Managing identity information ... 10
8.3 Architectural components for control ... 11
8.3.1 Establishing an identity management system ... 11
8.3.2 Controlling an identity management system ... 13
Annex A (normative) **Practice of managing identity information in a federation of identity management systems** ... **15**
Annex B (normative) **Identity management practice using attribute-based credentials to enhance privacy protection** ... **24**
Bibliography ... **31**

This document is a preview generated by EVS

© ISO/IEC 2016 – 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*, SC 27, *IT 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*

This document is a preview generated by EVS

 © ISO/IEC 2016 – All rights reserved

Introduction

Data processing systems commonly gather a range of information on their 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, 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.

This part of 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 presents practices for identity management. These practices cover assurance in controlling identity information use, controlling the access to identity information and other resources based on identity information, and controlling objectives that should be implemented when establishing and maintaining an identity management system.

This part of ISO/IEC 24760 consists of the following parts:

— ISO/IEC 24760-1: Terminology and concepts;

— ISO/IEC 24760-2: Reference architecture and requirements;

— ISO/IEC 24760-3: Practice.

ISO/IEC 24760 is intended to provide foundations for other identity management related International Standards including the following:

— ISO/IEC 29100, Privacy framework;

— ISO/IEC 29101, Privacy reference architecture;

— ISO/IEC 29115, Entity authentication assurance framework;

— ISO/IEC 29146, A framework for access management.

This document is a preview generated by EVS

© ISO/IEC 2016 – All rights reserved

This document is a preview generated by EVS

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

Part 3: Practice

This document is a preview generated by EVS

1 Scope

This part of ISO/IEC 24760 provides guidance for the management of identity information and for ensuring that an identity management system conforms to ISO/IEC 24760-1 and ISO/IEC 24760-2.

This part of ISO/IEC 24760 is applicable to an identity management system where identifiers or PII relating to entities are acquired, processed, stored, transferred or used for the purposes of identifying or authenticating entities and/or for the purpose of decision making using attributes of entities. Practices for identity management can also be addressed in other standards.

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*

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
identity management system
system comprising of policies, procedures, technology and other resources for maintaining identity information including meta data

[SOURCE: ISO/IEC 24760-2:2015, 3.3]

3.2
identity profile
identity containing attributes specified by an identity template

3.3
identity template
definition of a specific set of attributes

Note 1 to entry: Typically, the attributes in a profile are to support a particular technical or business purpose as needed by relying parties.

3.4
identity theft
result of a successful false claim of identity

© ISO/IEC 2016 – All rights reserved