INTERNATIONAL STANDARD

ISO/IEC 29146

First edition
2016-06-01

Information technology — Security techniques — A framework for access management

Technologies de l'information — Techniques de sécurité — Cadre pour gestion d'accès

Reference number
ISO/IEC 29146:2016(E)

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

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, *IT Security techniques*.

Introduction

Management of information security is a complex task that is based primarily on risk-based approach and that is supported by several security techniques. The complexity is handled by several supporting systems that can automatically apply a set of rules or policies consistently.

Within the management of information security, access management plays a key role in the administration of the relationships between the accessing party (subjects that can be human or non-human entities) and the information technology resources. With the development of the Internet, information technology resources can be located over distributed networks and the access to them needs to be managed in conformity under a policy and is expected to have common terms and models as a framework on access management.

Identity management is also an important part of access management. Access management is mediated through the identification and authentication of subjects that seek to access information technology resources. This International Standard depends on the existence of an underlying identity management system or an identity management infrastructure (see references in Clause 2).

The framework for access management is one part of an overall identity and access management framework. The other part is the framework for identity management, which is defined in ISO/IEC 24760.

This International Standard describes the concepts, actors, components, reference architecture, functional requirements and practices for access control. Example access control models are included.

It focuses mainly on access control for a single organization, but adds other considerations for access control in collaborative arrangements across multiple organizations.

Information technology — Security techniques — A framework for access management

1 Scope

This International Standard defines and establishes a framework for access management (AM) and the secure management of the process to access information and Information and Communications Technologies (ICT) resources, associated with the accountability of a subject within some context.

This International Standard provides concepts, terms and definitions applicable to distributed access management techniques in network environments.

This International Standard also provides explanations about related architecture, components and management functions.

The subjects involved in access management might be uniquely recognized to access information systems, as defined in ISO/IEC 24760.

The nature and qualities of physical access control involved in access management systems are outside the scope of this International Standard.

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 24760-1:2011, *Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts*

ISO/IEC 24760-2:2015, *Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements*

ISO/IEC 29115:2013, *Information technology — Security techniques — Entity authentication assurance framework*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 24760-1, ISO/IEC 29115, and the following apply.

3.1
access control
granting or denying an operation to be performed on a *resource* (3.14)

Note 1 to entry: A primary purpose of access control is to prevent unauthorized access to information or use of ICT resources based on the business and security requirements; that is, the application of authorization policies to particular access requests.

Note 2 to entry: When an authenticated *subject* (3.15) makes a request, the resource owner will authorize (or not) access in accordance with access policy and subject privileges.