SLOVENSKI STANDARD
SIST EN ISO/IEC 29146:2023

01-julij-2023

Informacijska tehnologija - Varnostne tehnike - Ogrodje za upravljanje dostopa (ISO/IEC 29146:2016, vključno z dopolnilom 1:2022)

Information technology - Security techniques - A framework for access management (ISO/IEC 29146:2016, including Amd 1:2022)

Informationstechnologie - Sicherheitstechniken - Ein Rahmen für die Zugangsverwaltung (ISO/IEC 29146:2016, einschließlich Amd 1:2022)

Technologies de l'information - Techniques de sécurité - Cadre pour gestion d'accès (ISO/IEC 29146:2016, y compris Amd 1:2022)

Ta slovenski standard je istoveten z: **EN ISO/IEC 29146:2023**

ICS:

35.030	Informacijska varnost	IT Security

SIST EN ISO/IEC 29146:2023 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 29146

April 2023

ICS 35.030

English version

Information technology - Security techniques - A framework for access management (ISO/IEC 29146:2016, including Amd 1:2022)

Technologies de l'information - Techniques de sécurité - Cadre pour la gestion de l'accès (ISO/IEC 29146:2016, y compris Amd 1:2022)

Informationstechnologie - Sicherheitstechniken - Ein Rahmen für die Zugangsverwaltung (ISO/IEC 29146:2016, einschließlich Amd 1:2022)

This European Standard was approved by CEN on 24 March 2023.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword

The text of ISO/IEC 29146:2016, including Amd 1:2022 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 29146:2023 by Technical Committee CEN-CENELEC/JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by October 2023, and conflicting national standards shall be withdrawn at the latest by October 2023.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 29146:2016, including Amd 1:2022 has been approved by CEN-CENELEC as EN ISO/IEC 29146:2023 without any modification.

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)

COPYRIGHT PROTECTED DOCUMENT

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.

3.2
access management
set of processes to manage *access control* (3.1) for a set of *resources* (3.14)

3.3
access token
trusted object encapsulating the authority for a *subject* (3.15) to access a *resource* (3.14)

Note 1 to entry: An access token is issued by the policy decision point (PDP) and consumed by the policy enforcement point (PEP) for the resource.

Note 2 to entry: An access token may contain access permission information for a subject to access the resource and identifying information for the authority of the authorization decision.

Note 3 to entry: An access token may contain information that enables its integrity to be validated.

Note 4 to entry: An access token may take a physical or a virtual form.

3.4
attribute
characteristic or property used to describe and to control access to a *resource* (3.14)

Note 1 to entry: The rules for accessing a resource are defined in an *access control* (3.1) policy which specifies the attributes required for the granting of access by a *subject* (3.15) to a resource for a specific operation.

Note 2 to entry: Attributes can include subject attributes, resource attributes, environmental attributes and other attributes used to control access as specified in the access control policy.

3.5
endpoint
location in an *access management* (3.2) system where an *access control* (3.1) function is performed

Note 1 to entry: There can be the following different types of endpoints:

— authentication endpoint, where *subject* (3.15) authentication is performed;

— authorization endpoint, where subject authorization is performed;

— endpoint discovery service, that searches for and locates endpoints;

— initial endpoint discovery service, used at the start of subject interactions with an access management system.

Note 2 to entry: Endpoint discovery services are commonly used in distributed and networked systems.

3.6
enterprise centric implementation
access management (3.2) conducted under the control of a policy decision point

3.7
need-to-know
security objective of keeping the *subject's* (3.15) access to data *resources* (3.14) to the minimum necessary for a requesting user to perform their functions

Note 1 to entry: Need-to-know is authorized at the discretion of the resource owner.

Note 2 to entry: Need-to-have is the security objective of the requester for the fulfilment of specific tasks that may be limited at the resource owner's discretion.

3.8
privilege
access right
permission
authorization to a *subject* (3.15) to access a *resource* (3.14)

Note 1 to entry: Privilege is a necessary but not sufficient condition for access. Access occurs when the access request is granted according to its access control policy. The access control policy is based on privileges and may include other environmental factors (e.g. time-of-day, location, etc.)

Note 2 to entry: Privileges take the form of data presented by a subject or obtained for a subject that is used by a Policy Decision Point in order to grant or deny an operation that a subject is willing to perform on a resource.

Note 3 to entry: A resource may have multiple distinct privileges associated with it which correspond to various defined levels of access. For example, a data resource could have read, write, execute and delete privileges available for assignment to subjects. A request by a subject for access to the resource might be allowed for some levels of access request but disallowed for other levels depending on the level of access requested and the resource privileges that have been assigned to the subject.

3.9
role
name given to a defined set of system functions that may be performed by multiple entities

Note 1 to entry: The name is usually descriptive of the functionality.

Note 2 to entry: Entities can be but are not necessarily human subjects.

Note 3 to entry: Roles are implemented by a set of *privilege* (3.8) attributes to provide the necessary access to data resources or objects.

Note 4 to entry: Subjects assigned to a role inherit the access privileges associated with the role. In operational use, subjects will need to be authenticated as members of the role group before being allowed to perform the functions of the role.

3.10
policy decision point
PDP
service that implements an access control policy to adjudicate requests from entities to access *resources* (3.14) and provide authorization decisions for use by a *policy enforcement point* (3.11)

Note 1 to entry: Authorization decisions are used by a policy enforcement point to control access to a resource. An authorization decision may be communicated through the use of an *access token* (3.3).

Note 2 to entry: PDP also audits the decisions in an audit trail and is able to trigger alarms.

Note 3 to entry: The term corresponds to Access Decision Function (ADF) in ISO 10181-3. It is presumed that this function is located over a network from the *subject* (3.15), and may be located over a network from the corresponding *PEP* (3.11).

3.11
policy enforcement point
PEP
service that enforces the access decision by the *policy decision point* (3.10)

Note 1 to entry: The PEP receives authorization decisions made by the PDP and implements them in order to control access by entities to *resources* (3.14). An authorization decision may be received in the form of an *access token* (3.3) presented by a *subject* (3.15) when an access request is made.

Note 2 to entry: The term corresponds to Access Enforcement Function (AEF) in ISO 10181-3. It is presumed that this function is located over a network from the subject and may be located over a network from the corresponding *PDP* (3.10).