FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
29146**

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2023-09-05

Voting terminates on:
2023-10-31

Information technology — Security techniques — A framework for access management

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC FDIS 29146
https://standards.iteh.ai/catalog/standards/sist/4b80fe0a-9d19-4144-aa69-9ef336b91bcf/iso-iec-fdis-29146

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.

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.

Reference number
ISO/IEC FDIS 29146:2023(E)

© ISO/IEC 2023

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC FDIS 29146
https://standards.iteh.ai/catalog/standards/sist/4b80fe0a-9d19-4144-aa69-9ef336b91bcf/iso-iec-fdis-29146

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2023 – All rights reserved

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC FDIS 29146
https://standards.iteh.ai/catalog/standards/sist/4b09e0af-9ff9-4144-aa69-9ef336b91bef/iso-iec-fdis-29146

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC FDIS 29146
https://standards.iteh.ai/catalog/standards/sist/4b80fe0a-9d19-4144-aa69-9ef336b91bcf/iso-iec-fdis-29146

© ISO/IEC 2023 – 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.

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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

ISO/IEC FDIS 29146
https://standards.iteh.ai/catalog/standards/sist/4b80fe0a-9119-4144-aa69-9ef336b91bcf/iso-iec-fdis-29146

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 29146:2016), of which it constitutes a minor revision. It also incorporates the Amendment ISO/IEC 29146:2016/Amd 1:2022. The changes are as follows:

— the text has been editorially revised and normative references updated.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2023 – All rights reserved

Introduction

Management of information security is a complex task that is based primarily on a 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 also be located over distributed networks. The management of access is expected to comply to a policy and to have common terms and models defined in a framework.

Identity management is also an important part of access management. Access management is mediated through the identification and authentication of parties that seek to access information technology resources. Access management relies on the existence of an underlying identity management system.

A 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 the ISO/IEC 24760 series.

This document describes the concepts, actors, components, reference architecture, functional requirements and the practice of an access control framework.

The document focuses mainly on the access control for a single organization. It provides additional considerations for access control in collaborative arrangements across multiple organizations. The document includes eventually examples of access control models.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC FDIS 29146
https://standards.iteh.ai/catalog/standards/sist/4b80fe0a-9d19-4144-aa69-9ef336b91bcf/iso-iec-fdis-29146

© ISO/IEC 2023 – All rights reserved

Information technology — Security techniques — A framework for access management

1 Scope

This document 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 contexts.

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

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

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

https://standards.iteh.ai/catalog/standards/sist/4b80fe0a-9d19-4144-aa69-9ef336b91bcf/iso-

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, ISO/IEC 29115, and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

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.

© ISO/IEC 2023 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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:

ISO/IEC FDIS 29146:2023
https://standards.iteh.ai/catalog/standards/sist/4b80fe0a-9d19-4144-aa69-9ef336b91bcf/iso-iec-fdis-29146

— 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.

© ISO/IEC 2023 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC FDIS 29146
https://standards.iteh.ai/catalog/standards/sist/4b80fe0a-9d19-4144-aa69-9ef336b91bcf/iso-iec-fdis-29146

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/IEC 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 policy enforcement point.

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/IEC 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 policy decision point.

© ISO/IEC 2023 – All rights reserved

3.12
policy administration point
PAP
service that administers access authorization policy

3.13
policy information point
PIP
service that acts as the source of *attributes* (3.4) that are used by a *policy decision point* (3.10) to make authorization decisions

Note 1 to entry: Attributes can include *resource* (3.14), *subject* (3.15) and environment *privileges* (3.8)/ permissions.

3.14
resource
object
physical, network, or any information asset that can be accessed for use by a *subject* (3.15)

3.15
subject
entity requesting access to a *resource* (3.14) controlled by an *access control* (3.1) system

3.16
security token service
STS
service that builds, signs, exchanges and issues *access tokens* (3.3) based on decision made by a *policy decision point* (3.10)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Note 1 to entry: This service may be split into separate components.

ISO/IEC FDIS 29146
atalog/standards/sist/4b80fe0a-9d19-4144-aa69-9ef336b91bcf/iso-

3.17
subject centric implementation
access management (3.2) implemented as component services that are called by a *subject* (3.15) to acquire the means recognized by the *policy enforcement point* (3.11) for accessing a *resource* (3.14)

Note 1 to entry: Component services may include policy decision point service, policy enforcement point service and associated discovery services that enable the subject to locate and contact the *access control* (3.1) services.

4 Abbreviated terms

AA	attribute authority
ABAC	attribute-based access control
ACL	access control list
AM	access management
AMS	access management system
CBAC	capabilities-based access control
DAC	discretionary access control
IBAC	identity-based access control
ICT	information and communication technology
IMS	identity management system

© ISO/IEC 2023 – All rights reserved

IT	information technology
MAC	mandatory access control
PBAC	pseudonym-based access control
PAP	policy administration point
PEP	policy enforcement point
PDP	policy decision point
PII	personally identifiable information
PIP	policy information point
RBAC	role-based access control
REDS	resource endpoint discovery service
STS	security token service
TLS	transport layer security
XACML	extensible access control markup language

iTeh STANDARD PREVIEW
(standards.iteh.ai)

5 Concepts

5.1 A model for controlling access to resources

ISO/IEC FDIS 29146
https://standards.iteh.ai/catalog/standards/sist/4b80fe0a-9d19-4144-aa69-9ef336b91bcf/iso-iec-fdis-29146

5.1.1 Overview

The conceptual sequence in giving access to a resource is as follows.

a) Subject authentication is needed before giving access to a resource. However, authentication is a separate function that is typically implemented on a session basis rather than for each access request.

b) Authorization decision to allow or deny access to the resource is made based on a policy, and an access token is issued to convey the result of the decision.

c) Authorization enforcement is conducted on the resource based on the decision result and resource access will be given.

Figure 1 shows this decision sequence.

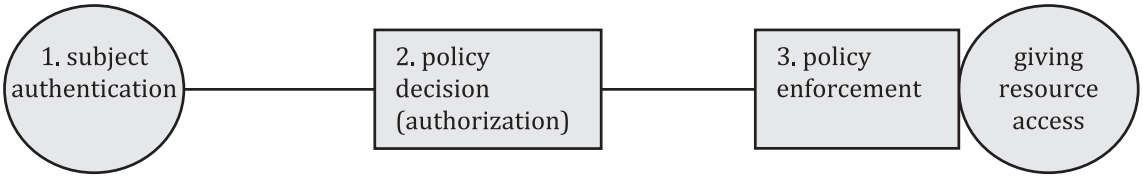

Figure 1 — Access control model sequence

Subject and resource are depicted as balloons while conceptual functions are depicted as rectangles.

For the purpose of being accessed, a resource is characterized by the following:

— an identifier, either for a specific resource or for a resource class;

© ISO/IEC 2023 – All rights reserved

— one or more modes of access;

— a set of attributes associated with the modes of access and other access criteria as specified in the access control policy.

An access management system is responsible for the administration and operation of authorizations to access. Authorizations are supported by administrative activity which assigns and maintains resource attributes and subject privileges in accordance with the access management policy.

Resources in IT systems are typically dynamic. They run a lifecycle from creation to destruction and this is a continuous process.

a) Resources have a life-cycle which runs from creation to destruction.

b) Resources are continually being created, updated and destroyed.

c) Resources need to be assigned access attributes (usually at the time of creation) which will be used by the access management system to control access by subjects to the resources. [Typically this is done by pre-defining recognized resource types with associated access attribute templates. When a resource of a known type is created, it inherits the access attributes of the corresponding template].

d) Resources are owned by a party which might be a person or an organization. The owner is often the creator of the resource but not always and the ownership may change during the life of the resource.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

5.1.2 Relationship between identity management system and access management system

In the model described here, the subject is authenticated using an identity management system (IMS), as described in ISO/IEC 24760-2. The authenticated subject then requests access using the access management system (AMS). The access management system determines whether or not to authorize the subject request to access the resource. Subject authorization comprises two distinct activities:

https://standards.iteh.ai/catalog/standards/sist/4b80fe0a-9d19-4144-aa69-9ef336b91bcf/iso-

— the pre-assignment of resource access privileges to subjects, and

— the granting of access to resources by subjects in operational use.

Figure 2 shows the relationship between an identity management system and an access management system.

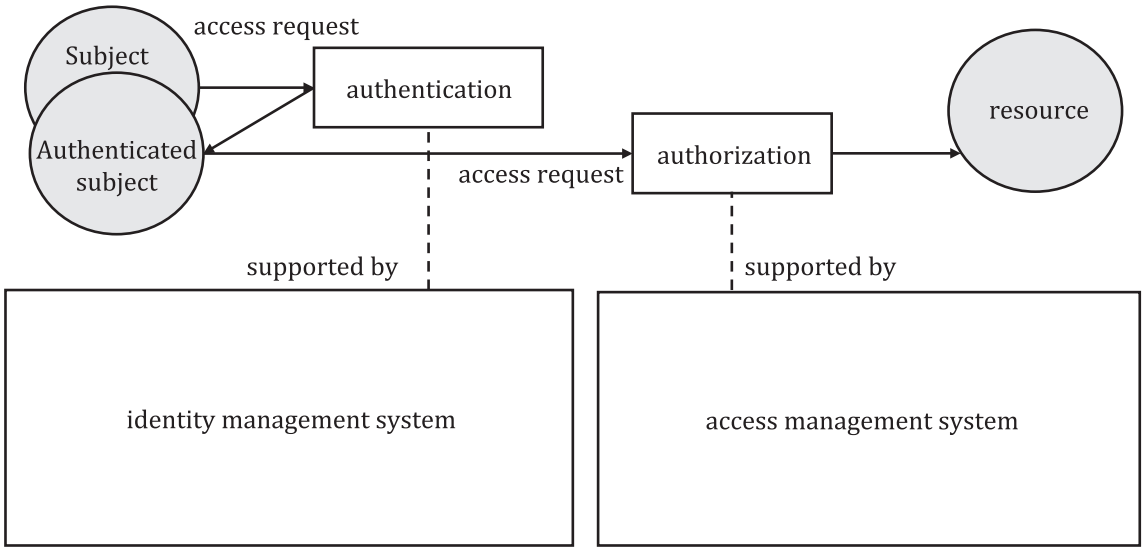

Figure 2 — Identity management system and access management system relationship

© ISO/IEC 2023 – All rights reserved

Authentication is supported by an identity management system. In an access management system using the IBAC model, identity is the basis for the assignment of resource access privileges to subjects and for the authorization of resource access requests by subjects in operational use.

NOTE Granting access to a resource can require a minimum stated level of authentication assurance for the subject which depends on the risk profile of resource. The required level depends on the identity-related risk pertaining to the resource to be accessed. For further information on authentication level of assurance, see ISO/IEC 29115.

Authorization is provided by the access management system that supports access information management.

Implementation practice for access management systems can vary according to the architecture and the access control model used, for example:

a) when an AMS is implemented as a Web service system, a subject may request access to a resource without first being authenticated. In this case, the AMS will direct the subject to request the IMS to provide authentication, and

b) when an ABAC model is adopted, there is a possibility that the subject does not require any authentication. In this case, an anonymous entity may be allowed to go directly to the AMS, and an authorization decision will be made based on a credential that can be validated to prove that the subject possesses the asserted attributes.

5.1.3 Security characteristics of the access method

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Consideration should be given to address the security aspects of access control systems implementation and processes, particularly where federated architectures are employed.

For security reasons, the integrity of the access request may first require validation before it is further processed by the access management system.

ISO/IEC FDIS 29146

Where communication channels can be trusted, such as for private connections within an organization, additional protection may not be needed. However, where communication channels run across public networks or other unprotected channels, measures to protect the integrity and confidentiality of access requests and associated data should be provided for both the access request itself (privileges, subject authentication data, resource, requested operation, etc.) and the data sent to or received from the resource during the period of access.

There are two approaches to establish a secure communication channel between the subject and the access management system. The following approaches consider the time at which that secure communication channel will be established:

a) a secure communication channel may be established before the transmission of the privileges or of the data that will be used to obtain the privileges [e.g. by the construction of a Transport Layer Security (TLS) session with the server supporting the resource];

b) a secure communication channel may be established after the successful transmission of the privileges or of the data that has been used to authenticate an identifier of the subject.

In the latter case, the secure communication channel is established either after a successful authentication exchange or after the successful acceptance of an access token; the integrity and the confidentiality keys are derived from the authentication exchange or derived from information contained in the access token or from information linked to the access token. Then, the transmission of the operation requested on the resource can be made through that secure communication channel.

5.2 Relationships between logical and physical access control

This document mainly focuses on logical access control. Logical access control is supported by physical access control.

© ISO/IEC 2023 – All rights reserved