ISO/IEC JTC 1/SC 27

Date: 2022-11-302023-08-22

ISO/IEC /FDIS 29146:2023(E)

ISO/IEC JTC 1/SC 27/WG 5

ISO/IEC JTC 1/SC 27/WG 5

Secretariat:DIN

Information technology — Security techniques — A framework for access management

Information technology — Security techniques — A framework for access management

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

Style Definition: Comment Text
Style Definition: List Continue 5: Font: Indent: Hanging: 20.15 pt, Don't add space between paragraphs of the same style
Style Definition: RefNorm
Style Definition: Base_Text: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left
Style Definition: Body Text_Center
Style Definition: Code: Tab stops: 16.15 pt, Left + 32.6 pt, Left + 48.75 pt, Left + 65.2 pt, Left + 81.35 pt, Left + 97.8 pt, Left + 113.95 pt, Left + 130.4 pt, Left + 146.55 pt, Left + 162.75 pt, Left
Style Definition: Dimension_100
Style Definition: Figure Graphic
Style Definition: Figure subtitle
Style Definition: List Continue 1
Style Definition: List Continue 2 (-): Indent: Left: 19.5 pt, Hanging: 40.5 pt, Space After: 12 pt
Style Definition: List Number 1: Tab stops: Not at 20.15 pt
Style Definition: Example indent 2: Tab stops: 67.7 pt, Left
Style Definition: Note indent 2 continued: Tab stops: 87.9 pt, Left
Style Definition: Note indent 2
Formatted: Font: Bold
Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted: English (United Kingdom)
Formatted: Font: Bold
Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted: French (Switzerland)
Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: English (United Kingdom)

Formatted

Contents

Formatted ... (repeated)
Field Code Changed ... (repeated)

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~~). 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~~). 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.

For an explanation ~~on~~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 ~~the following URL: Foreword – Supplementary information~~www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

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

Formatted: std_publisher

Formatted: std_docNumber

Formatted: Right

Formatted: Left, Space After: 0 pt

Formatted: Font: 10 pt, Spanish (Spain)

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 ~~and the~~. The management of access is expected to ~~them needs~~comply to ~~be managed in conformity under~~ a policy and ~~is expected~~ to have common terms and models ~~as~~defined in 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~~parties that seek to access information technology resources. ~~This International Standard depends~~Access management relies on the existence of an underlying identity management system ~~or an identity management infrastructure (see references in Clause 2).~~

~~The~~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 ~~International Standard~~document describes the concepts, actors, components, reference architecture, functional requirements and ~~practices for~~the practice of an access control ~~. Example access control models are included.~~ framework.

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

Formatted: Left

Formatted: Different first page header

~~Information technology — Security techniques — A framework for access management~~

Information technology — Security techniques — A framework for access management

1 Scope

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

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

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

The subjects involved in access management ~~might~~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 ~~International Standard~~document.

2 Normative references

The following documents~~,~~ are referred to in ~~whole~~the text in such a way that some or ~~in part, are normatively referenced in~~all of their content constitutes requirements of 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~~-1:2019~~-1, *Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts*

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

ISO/IEC ~~24760-2:2015~~29115, *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*~~

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

~~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.

Formatted: Left, Space After: 0 pt

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

Formatted: Font: 10 pt, Spanish (Spain)

- 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.

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

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.

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

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.

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

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:

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

- 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.

Formatted: Left

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~~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).

Formatted: Right, Space After: 0 pt

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

Formatted: Font: 11 pt

Formatted Table

Formatted: Font: 11 pt

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: 11 pt, Not Bold

Formatted: Left, Space After: 0 pt

Formatted: Font: 10 pt, Spanish (Spain)

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~~ 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 ~~*PEP* (3.11).~~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.

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

Note 2 to entry: The term corresponds to ~~Access Enforcement Function~~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 ~~*PDP* (3.10).~~policy decision point.

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.

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

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)

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

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

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.

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

Formatted: Left

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
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

5 Concepts

5.1 A model for controlling access to resources

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.

Formatted: Right, Space After: 0 pt

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted ...

Formatted ...

Formatted ...

Formatted ...

Formatted ...

Formatted ...

Formatted ...

Formatted ...

Formatted ...

Formatted: Tab stops: Not at 18 pt

Formatted ...

Formatted: Font: 11 pt

Formatted Table

Formatted: Font: 11 pt

Formatted ...

Formatted: Font: 11 pt, Not Bold

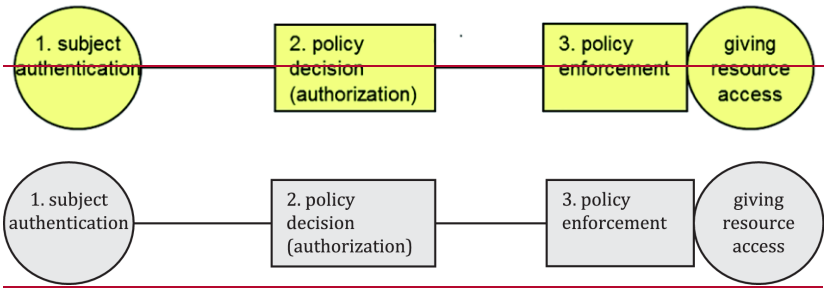

Figure 1 — Access control model sequence

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;
- 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.

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~~,~~:

- 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 ~~(IMS)~~ and an access management system~~ (AMS)~~.

Formatted: Left, Space After: 0 pt

Formatted: Font: 10 pt, Spanish (Spain)

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

Formatted: Left

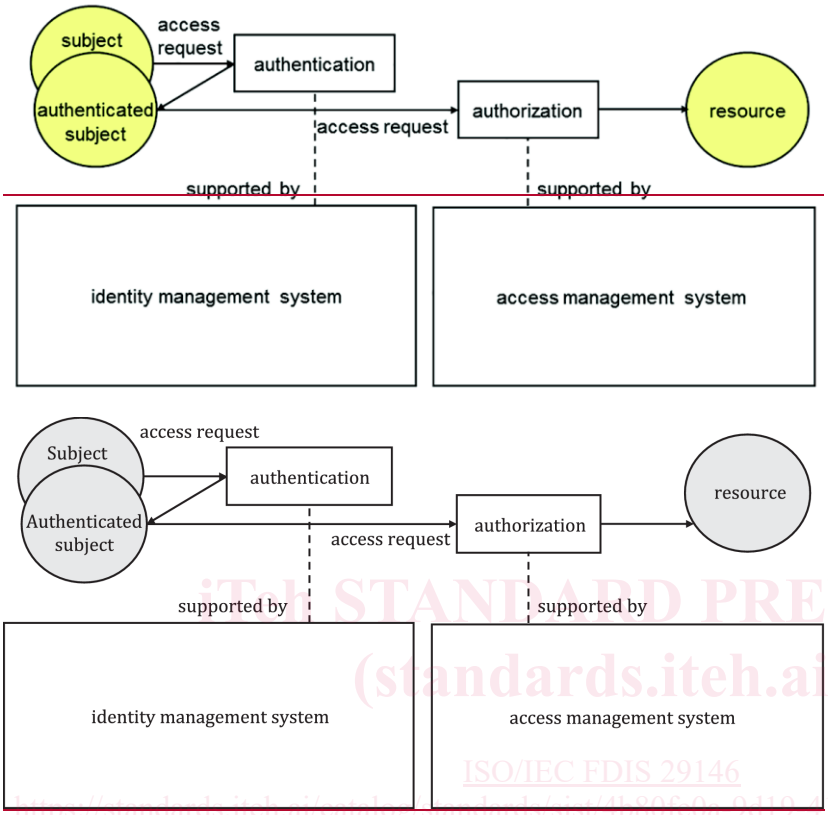

Figure 2 — Identity management system and access management system relationship

Authentication is supported by an identity management system ~~(IMS).~~ 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 ~~may~~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 ~~(AMS)~~ that supports access information management.

Implementation practice for access management systems ~~may~~can vary according to the architecture and the access control model used, ~~e.g.~~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 ~~for a~~that the subject does not ~~to~~ 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.

Formatted: Right, Space After: 0 pt

Formatted: Note, Line spacing: single, Widow/Orphan control, Hyphenate, Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

Formatted: Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

Formatted: Font: 11 pt

Formatted Table

Formatted: Font: 11 pt

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: 11 pt, Not Bold