International Standard

ISO/IEC 29146

Second edition
2024-01

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 29146:2024(en)

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

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.

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).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

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.

This document was prepared by Joint Technical Committee 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.

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 examples of access control models.

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.

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.

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.

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/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.

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)

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

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

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.

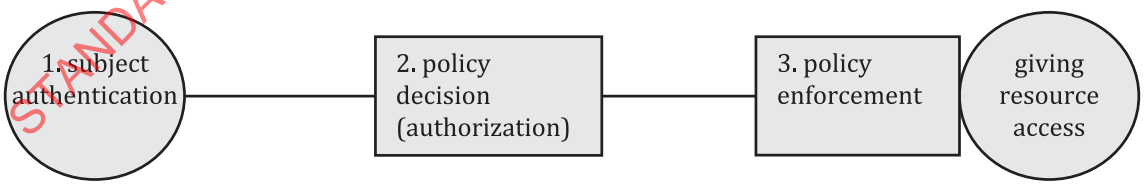

Figure 1 — Access control model sequence

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 and an access management system.

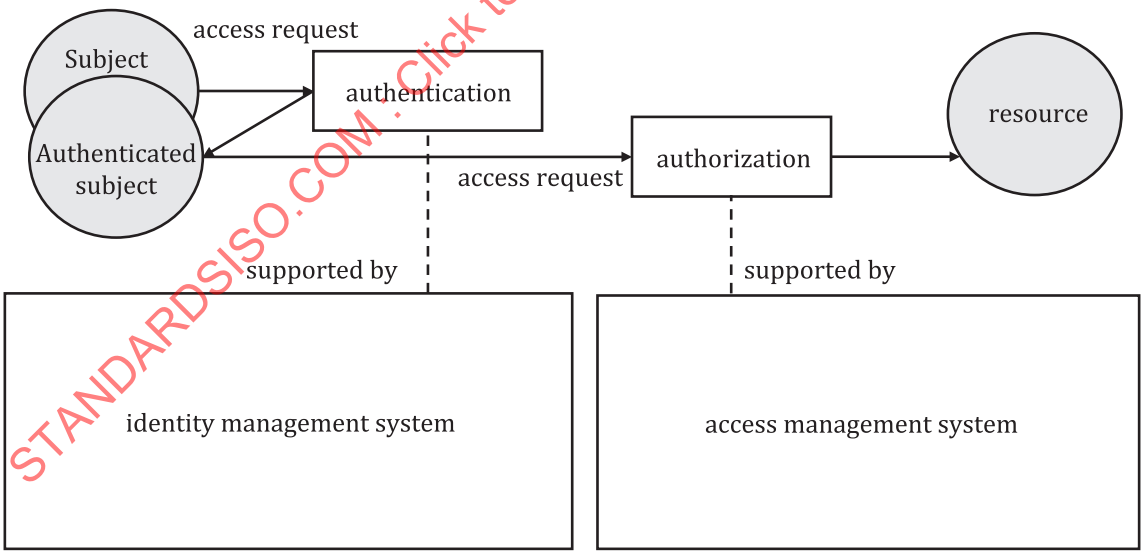

Figure 2 — Identity management system and access management system relationship

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

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.

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.

Logical access to a resource in an enterprise system should be supported by a secure physical infrastructure which provides an effective set of controls and actions that cannot be subverted.

For logical access to a resource hosted by an outsourced service, the outsourced service should be accountable for its physical and logical access control so that it can be trusted by the subject.

5.3 Access management system functions and processes

5.3.1 Overview

An access management system enforces an access control policy and provides two core operational functions:

a) to assign resource access privileges to subjects in advance of operational use; alternatively, to assign access privileges to attributes (as in the ABAC model) and then assign attributes to subjects who inherit the associated access privileges;

b) to use these privileges (together with other information where appropriate) to control subject access to system resources in operational use.

In addition, an AMS provides administrative functions to support the core functions, including:

— policy management;

— policy-related access attribute management;

— monitoring and record keeping management.

Resource access policy should implement the following principles:

a) setting access attributes on a “need-to-know” basis;

b) minimalizing data access in order to restrict access to only strictly required data and minimize data leakage and disclosure risk;

c) segregating and protecting of sensitive data;

d) protecting of PII;

e) using multifactor authentication based on the criticality and sensitivity of resource accessed.

5.3.2 Access control policy

An access management system enforces an access control policy. A number of access control models exist (see Annex A). This document focuses on the following models which are sufficiently flexible to be suitable for use in both centralized and distributed network environments:

— identity-based access control (IBAC) model;

— role-based access control (RBAC) model;

— attribute-based access control (ABAC) model.

Access control policy should be described in natural language or another suitable representation, e.g. a formal language, to express the objectives for the control of access to resources, the methods and processes for exercising the control, and any requirements for monitoring, auditing and other non-core functions.

There may be multiple access control policies within an organization. Typically, a group of resources on one technology may be accessed under the control of a decision point responding to one policy, while access to another group of resources developed with a different technology will be managed under a different decision point responding to a second access control policy. Both decision points may also respond to the same access control policy, which is recommended.

Where multiple access control systems operate within an organization and they are to be integrated into a single system, policy differences should be reconciled and a common access control policy developed and

documented. An alternate approach can be to integrate the systems as an intra-organization federation, in which case, the considerations and requirements described in 5.3.8 shall be applicable.

Access control is provided through mechanisms for granting or denying operations to be performed on resources based on an access control policy.

Authorization decisions are made based on the evaluation of subject privileges and attributes against access rules set out for the relevant resource. Rules can also include environmental attributes such as time of day and location from which the request is made. For example, no operation can be done on the resource between 9:00 p.m. and 7:00 a.m.

If a mandatory access control (MAC) model applies, a rule will necessarily be global to a set of resources. For example, subjects should be cleared to "Top Secret" for any operation that they would like to perform on a given set of resources.

NOTE As multiple rules can be applied sequentially, the order of application can affect the efficiency of the decision process. However, the optimum ordering will depend on the relative likelihood of grant/deny access decisions in operational use.

In general, individual rules may be implemented by means of an access control matrix associated with each resource which contains one or more entries.

Each entry will indicate the condition(s) that a subject shall fulfil in order to perform one or more operations on the resource. The major condition to fulfil is that the subject shall possess some privilege(s).

ABAC is the common situation where access control is based on AMS defined attributes possessed by subjects. IBAC model, a similar IBAC model called pseudonym-based access control (PBAC) model, and RBAC model are particular cases of ABAC where the attributes are, respectively, an identity, a pseudonymous identity, and a role. These four models may be implemented using ACLs.

When the subject presents a capability ticket for authorization (also referred as a capability-based access control (CBAC) model), it is necessary to verify that the capability ticket as an access token is effective for that operation.

In access management systems that embody more than one access model, care should be taken to ensure that policies specifying access to resources by subjects do not result in conflicting access decisions for the same subject via different paths: a policy administration point should be able to manage various models of ABAC, IBAC, PBAC, RBAC, or CBAC.

An access control policy should have the following characteristics:

a) be based on policy requirements common to required models in place, to protect information to meet business requirements and for reasons of legal and regulatory compliance and intellectual property;

b) contain a policy hierarchy, based upon the common policy, from which access control rules applying to individuals with same characteristics may be defined;

c) describe the attributes supporting a defined classification. This categorization will enable policy interoperability and compliance across organizations;

d) describe procedures for the provisioning and management of privileges, the access control process and exception handling.

5.3.3 Privilege management

The requirements for privilege management are defined by the access control policy as mentioned in 5.3.2.

Under identity-based access control policy, privilege management is conducted on the basis of subject identity. IBAC policy employs mechanisms such as access control lists (ACLs) to specify the identities of those allowed to access a resource and the types of operation on the resource that they are allowed to perform. In the IBAC model, the granting of resource access privileges to a subject is made prior to any subject access request, and subject identity and access privileges are added to the relevant resource ACL(s).

If an authenticated subject identity matches an identity recorded in the relevant ACL, the subject is given access to the resource in accordance with its access privileges. Each resource has an associated ACL in which the access privileges for the subjects that are authorized to access the resource are recorded. In the IBAC model, the authorization decisions are made prior to any specific access request and result in the subject and the subject access privileges being added to the relevant resource ACL(s).

In the RBAC model, a role (or roles) is assigned to each subject and is recorded in the account for the subject. Authorization decisions are made based on the access privileges assigned to the relevant role within the access management system. In an RBAC model, the privileges are assigned to roles not subjects. A separate activity assigns roles to subjects. This also affects the authorization process when requesting access to resources that is a two-step process in an RBAC model:

— authorize the access request for the role;

— authenticate the subject to be a member of the role group.

Under the ABAC model, policy-related access attributes are assigned to subjects. Authorization decisions are based on the attributes possessed by subjects.

A subject may access resources as a member of a group, the possessor of attributes or as an individual. Role-based, attribute-based and identity-based access control schemes can exist concurrently in an access control system.

Privilege management comprises the following activities:

a) creating the set of privileges to be used to denote and limit the types of operation that may be performed on resources;

b) establishing the rules specifying the assignment of privileges in accordance with the access control policy and the access control model employed, e.g. assignment to identities, roles, capabilities or other defined attributes;

c) the update and revocation of privileges and identity attributes.

The implementation of access control policy results from the assignment of resource access privileges to subjects, roles, groups, etc. Privileges should be assigned on a “need-to-know” basis, granting the lowest level of privilege consistent with the subject being able to perform the relevant activity.

NOTE Privileges can be assigned to both human subjects and non-human subjects. For example, when a device or a service is added to a network, it can be assigned resource access privileges.

5.3.4 Policy-related attribute information management

Management of information for setting of privileges to attributes is an administrative activity as illustrated in Figure 5.

This kind of information is:

a) obtained from various sources including attribute authorities, resources and the environment;

b) managed through the policy administration point (PAP);

c) stored in the policy information point (PIP).

The resulting information is made available to the policy decision point (PDP) to control access to resources.

Attribute information is managed within an AMS in accordance with the access control policy described previously.

In the case of an ABAC model, the policy is formulated in terms of the attributes that are used to govern access to resources and how the attributes are mapped to resource access privileges. For an RBAC model, the policy specifies how the resource access privileges are assigned to the various roles.

Under a DAC policy, attributes are managed by resource owners, while under a MAC policy, additional attributes are managed by policy officers.

The PBAC model employs mechanisms such as ACLs which contain the pseudonyms of the subjects permitted to access the resource, together with the subject access permissions for the resource. If a subject presents a pseudonym that matches one held in the ACL, the subject may be given the right to perform the operation on the resource, subject to its permissions and any other checks that may apply.

The IBAC model employs a similar mechanism where identities are used rather than pseudonyms.

The RBAC model employs a similar mechanism where roles are used rather than pseudonyms.

The ABAC model employs a similar mechanism where attributes (e.g. group memberships) are used rather than pseudonyms.

The PBAC model, the IBAC model, the RBAC model and the ABAC model may exist concurrently in an access control system.

The CBAC model employs mechanisms where the capability presented by the subject shall first match with the identifier of the resource and with the operation to be performed on the resource. Secondly, the content of the capacity shall also match with the identifier of a recognized authority and with the associated operations granted for this authority. If it is the case, the subject may be given the right to perform the operation on the resource, pending other checks that may apply.

More information on models is provided in Annex A.

5.3.5 Authorization

5.3.5.1 Basic authorization

Authorization happens during the operational phase and is mediated by PDP in accordance with the access control policy. This activity is supported by administrative activity.

5.3.5.2 Authorization of delegate access

Under defined conditions, authorization may be granted to a delegate of a subject. A delegate can be a person or a web server or client application operating under the control of the subject. A delegate will typically inherit the access privileges of the subject. The delegate shall be authenticated in the same or in an equivalent way to the subject of which it was delegated privileges. The delegate scenario is illustrated in Figure 3.

NOTE This is a use case that OAuth technology supports. The authorization decision is made by the resource owner in real time or by pre-registered policy set by the resource owner. If the subject is already a delegate, then the AMS can determine the authorization decision from the credentials the delegate already possesses. If the subject is not already a delegate, the resource owner is expected to be contacted to understand if the unauthorized person is authorized to access the resource.

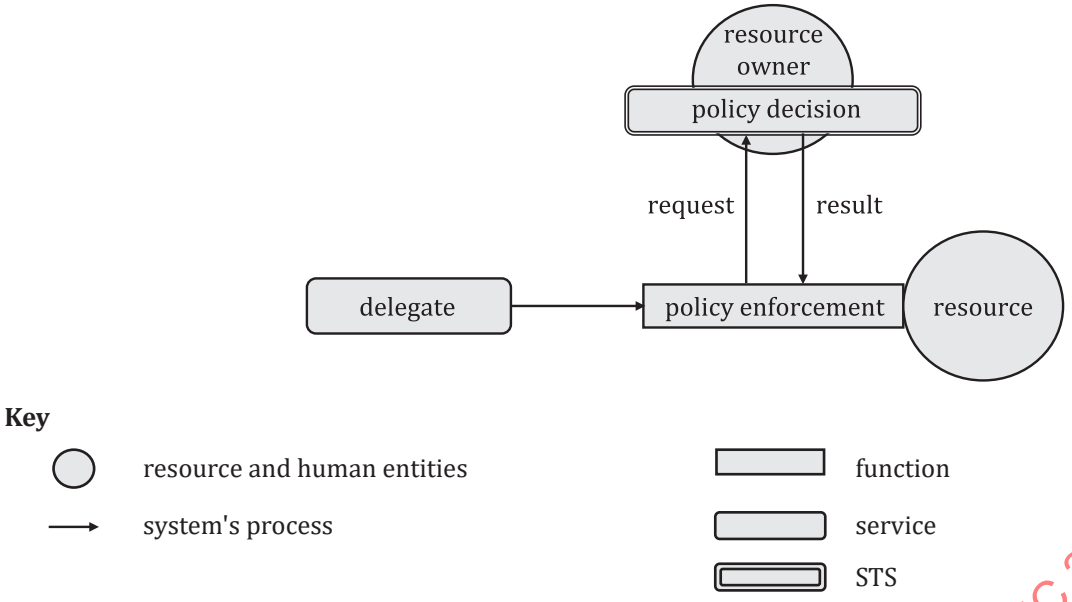

Figure 3 — Authorization of delegate access

5.3.6 Monitoring management

Activities associated with access management should be monitored for compliance and investigative purposes.

The AMS should provide auditable, monitoring and record keeping capabilities, to show compliance with regulatory, liability, and investigation requirements.

An AMS should provide capabilities to monitor the operations attempted by the subjects on the resources and whether these operations have been granted or denied.

The following parameters should be recorded in an audit trail:

a) an identifier of the resource;

b) the operation that the subject requested to perform on the resource;

c) the decision (i.e. grant or deny), together with a reason;

d) the time of access granted or denied;

e) the subject privileges or attributes as appropriate;

f) any information that may directly or indirectly identify the subject.

In addition, the AMS should provide tools to easily build audit reports using filters based on the previous six parameters that may be found in the audit trail.

A resource owner shall specify the access criteria to be used by the policy decision point to enable it to decide whether to grant access to the resource by a subject.

5.3.7 Alarm management

Usually, the purpose of alarms is to alert access management auditors to abnormal operating conditions. Such situations should be defined in the access control policy together with the handling procedures and the handling procedures implemented in monitoring management. Abnormal situations can include, for example, attempts to access resources by unauthorized subjects.

Alarm conditions are defined to enable them to be recognized in operational use and to take appropriate action. When alarm conditions occur, they should be recorded in an audit trail for later analysis.

Alarms may be triggered by single or multiple conditions which may relate to the following:

a) an identifier of the resource;

b) the operation that the subject requested to perform on the resource;

c) the decision (i.e. grant or deny), together with a reason;

d) the time of access granted or denied;

e) privileges or attributes as appropriate;

f) any information that may directly or indirectly identify the subject.

Once an alarm has been triggered, further investigations can be conducted using the audit trail built for monitoring the events.

5.3.8 Federated access control

5.3.8.1 General

Federated identity and access management is required when an authenticated subject from one organization seeks to access a resource in another organization. There are several models for federated identity management, which are described in the ISO/IEC 24760 series. Figure 4 shows an example of a federated access control system. Assuming a subject can authenticate in a federation model, federated access control requirements are implemented by the members of the federation in accordance with a shared trust relationship and common policies agreed by the organizations participating in the community.

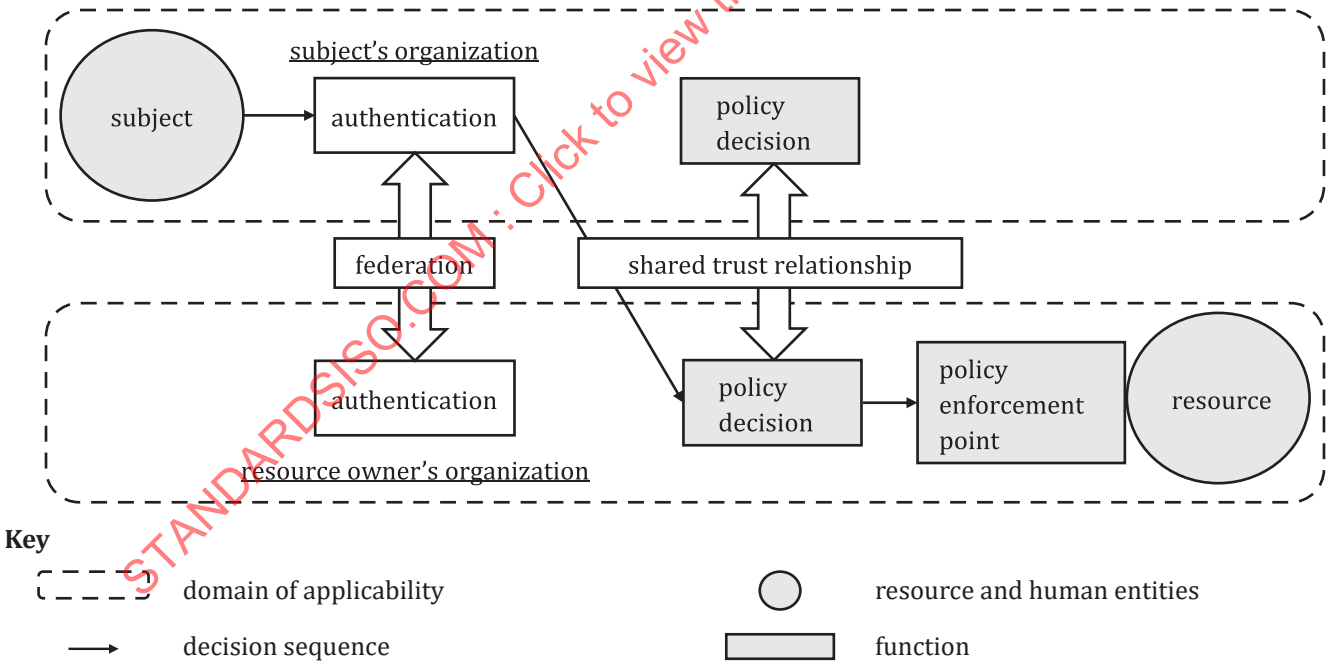

Figure 4 — Federated access control

5.3.8.2 Common access control policies of access control in a federation

Common access control policies of organizations in a federation include:

a) The subject authenticates in his parent organization's source of authority.

b) The subject's organization provides an access control assertion to the resource owner's organization, which confirms the subject's authentication is valid and provides the authentication context and agreed access attributes, including the ABAC or RBAC privileges.

c) The data resource owner's organization accepts the assertion and examines the attributes in relation to the data resources owner's access control policies.

d) The data resource owner authorizes the subject to access the resource or denies access and notifies the subject.

e) All authorities record access control events.

5.3.8.3 Shared trust relationship for access control in a federation

A shared trust relationship for access control within a federation should:

— be based on agreed federation requirements to protect information, for reasons of legal and regulatory compliance and intellectual property,

— contain common policy elements, from which access control rules and implementation categorization can be defined, and

— define access control credentials (attributes, permissions, etc.) that can be adopted across a federation to help facilitate the establishment of trust relationships among federation members.

6 Reference architecture

6.1 Overview

The components presented in Clause 5 establish a reference architecture for an AMS.

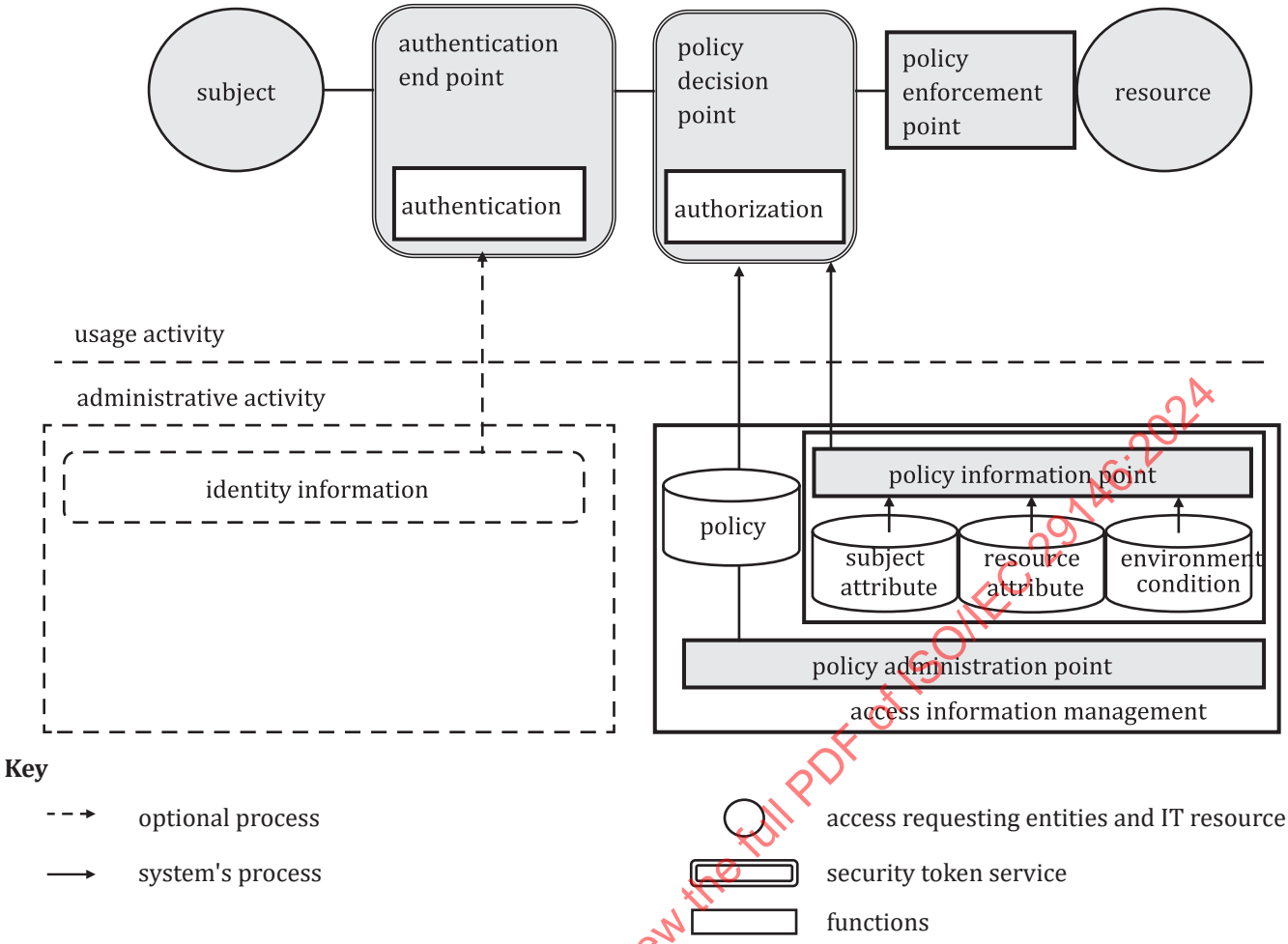

Figure 5 — AMS reference architecture

6.2 Basic components of an access management system

6.2.1 Authentication endpoint

The authentication endpoint provides subject authentication for use by the policy decision point in making decisions on access to resources by subjects.

6.2.2 Policy decision point

The PDP makes authorization decisions to allow or deny access to a resource and conveys the decisions to the PEP for implementation.

The PDP implements the access control policy or policy set for the resource. Based on defined set of policies, the PDP decides whether the subject may access the resource.

In some cases, the policy is created in real-time through an interface to the resource owner. In enterprise centric access control implementations, this service is often called “user authorization endpoint”.

The PDP is supported by the policy information point (PIP).

6.2.3 Policy information point

This component acts as a source of attribute values (e.g. resource, subject, environment condition) that are used by the PDP to make the authorization decision.

6.2.4 Policy administration point

This component provides the interface for administrating the policy set and related information on PIP. The administration of these elements may include configuring, testing, debugging and storing. To administrate access control policy set, an application programmable interface to the PAP is needed.

The policy or policy set may be based on role-based access control (RBAC) or attribute-based access Control (ABAC), or any other model or combination of these.

Natural language policy should be translated into an equivalent digital representation of the policy which the PDP uses to determine its authorization decisions.

6.2.5 Policy enforcement point

The PEP allows authorized access to resources and protects a resource from unauthorized access.

The PEP intercepts the subject's access request to the resource and redirects to the authorization decision, which is made by the PDP.

6.3 Additional service components

6.3.1 General

In implementing the logical view, several services may be additionally introduced.

6.3.2 Subject centric implementation

6.3.2.1 Overview

Figure 6 shows the case where the subject plays a crucial role.

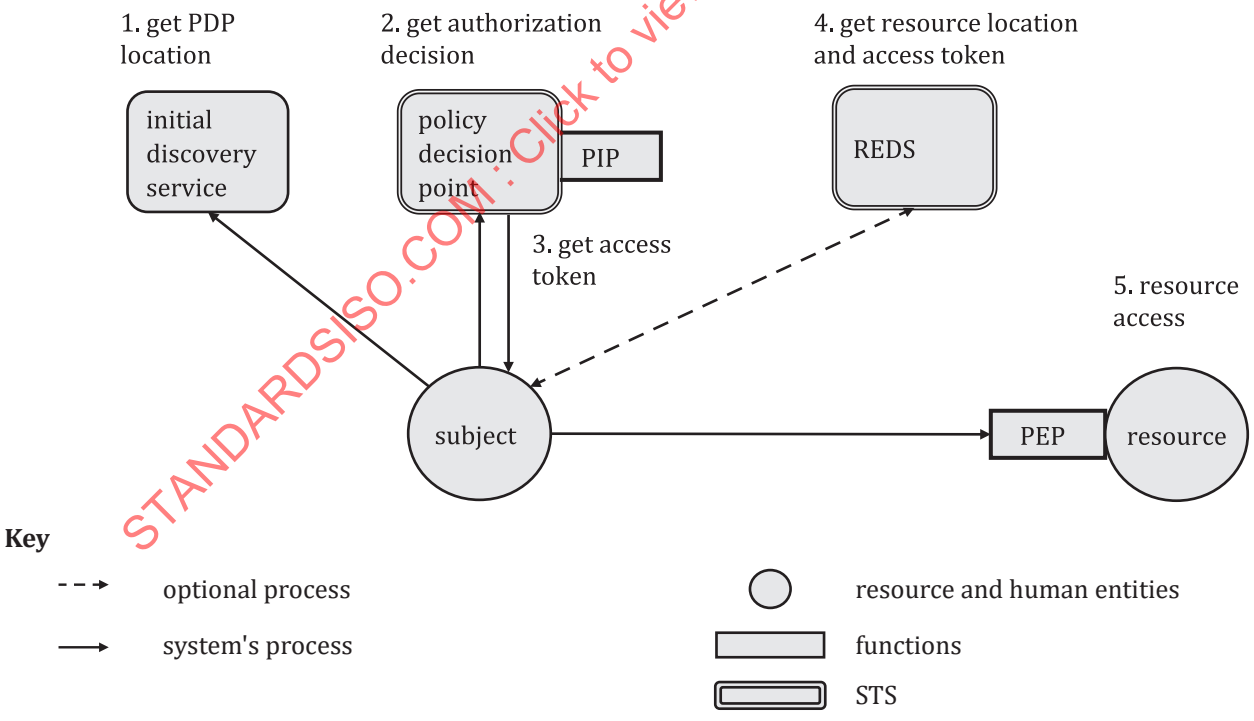

Figure 6 — Components services interactions in subject centric situation

6.3.2.2 Initial endpoint discovery service

In some use cases, a portal service may be implemented such that it undertakes "initial discovery" at the beginning of subject interactions to guide the subject. Usually, the initial endpoint will be the authentication endpoint.

NOTE Subject authentication service is not described here. Refer to ISO/IEC 24760–1, ISO/IEC 24760–2 and ISO/IEC 29115. Sometimes, resource endpoint discovery happens here as well, in some optimizing situations where these are combined and where privacy/data protection is not an issue.

6.3.2.3 Security token service

Based on the decision made by the PDP, a security token service (STS) may build, sign, exchange and issue access tokens.

Access tokens are described in various technical standards. Primary examples are the OAuth access token and the SAML assertion[7]. Refer to the applicable standards for details on these.

An STS can form part of the features of other components of an AMS.

6.3.2.4 Resource discovery service

A resource discovery service (REDS) helps providing information on the location of resources managed by an AMS. A resource discovery service shall itself be a protected resource which requires authorization before it can be accessed. An authorization decision is required to access REDS. However, information that can reveal privacy sensitive information shall also be protected (e.g. the location of a medical record may reveal the nature of the illness.).

NOTE In some situations, the response from the REDS can be uniform across the subjects and stable for prolonged periods. Therefore, the response can be resolved through static metadata, rather than dynamically. Also, in some AMS implementations, a REDS can also function as an STS by providing a resource access token to a subject to replace the token that the subject presented to gain access to the REDS.

6.3.2.5 Steps to access resources

Controlled access to resources may be performed using the following steps.

a) An authenticated subject may start from an initial discovery service from which it finds out the location of the PDP and STS.

b) The subject requests the access authorization to certain resources to the PDP. Based on the policy or policy set provided by the PIP, the PDP determines whether to grant authorization.

c) If access authorization is granted, an access token is generated by the STS component of the PDP and passed to the subject.

d) If the resource location has not been obtained from the initial discovery service, the subject obtains this information from the REDS. At that time, the REDS may accept the subject access token and provide a replacement access token which the subject can use to access the resources.

e) The subject presents the access token to the PEP to gain access to the resource.

NOTE The resource access can be performed in two ways:

— directly to the PEP with the subject accessing the individual resources using the access token;

— indirectly through an interfacing service instead of querying the PEP for each resource needed.

An example of the latter situation is when the subject does not wish to reveal its identity to the resources.

6.3.3 Enterprise centric implementation

6.3.3.1 Overview

Figure 7 shows the situation of enterprise centric access control where PEP plays a crucial role.

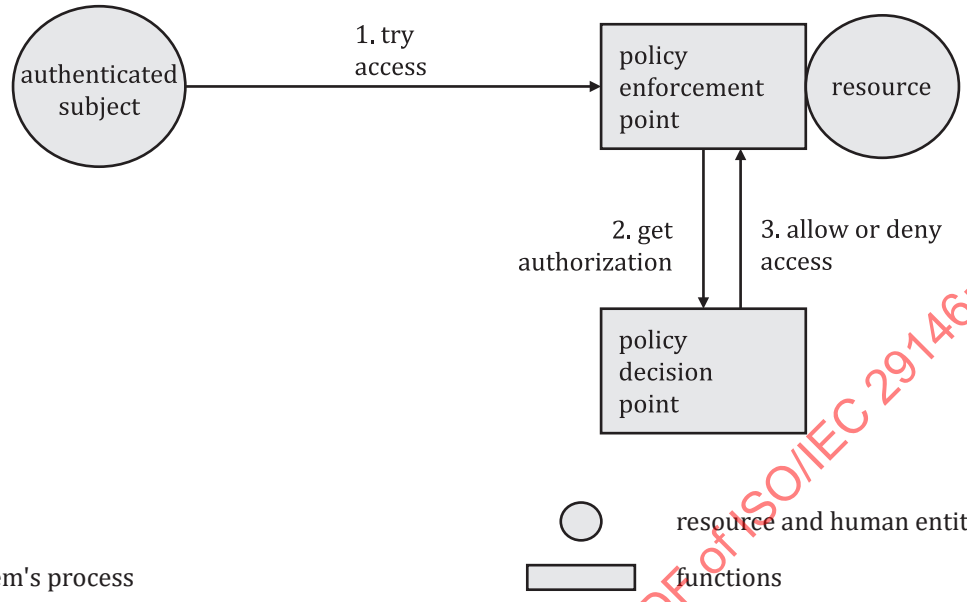

Figure 7 — Components services interactions in enterprise situation

6.3.3.2 Communication between PEP and PDP

Implementing PEP and PDP as independent services can enable flexibility and efficiency in the development of access management systems, particularly where resources are widely distributed.

If the access control policy changes, it is likely that only the PDP will require changing, while the PEP continues to function unchanged.

There should be a trust relationship between the PDP and the PEP.

If the PEP and PDP are not collocated in a secured network, the communication between them should be secured. The PDP and PEP should be able to confirm the authenticity of each other.

6.3.3.3 Steps to access resources

Controlled access to resources may be performed using the following steps.

a) Authenticated subjects make a request to the PEP to access the resource, passing proof of identity with request.

b) The PEP refers access request to the PDP to obtain authorization for the subject to access the resource.

c) The PDP makes an access decision based on subject access privileges and access policy for the resource. It passes the access decision back to the PEP.

d) The PEP enforces the access decision.

7 Additional requirements and concerns

7.1 Access to administrative information

Access to administrative components of access management system (AMS) should be restricted to authorized persons such as administrators, security officers and auditors.

Resource's owners should have the ability to manage the access attributes for the resources they are responsible for.

Access to administrative information is performed via an interface to the policy administration point.

Subjects and attribute information for subjects to access resources are stored in the policy information point.

The design of the access control policy for AMS administration information should specify the following:

a) criteria for authorizing each administrative access to the information;

b) conditions and mechanisms to access the information;

c) conditions of use of the information;

d) which operations of access to information shall be recorded and with what details;

e) the duration of the retention of records such as audit records; alarm records should be determined by the access control policy;

f) the duration and conditions of the AMS highest level system administrator account.

7.2 AMS models and policy issues

7.2.1 Access control models

There are a number of access control models that are suitable for use in a distributed network environment. For managing its resources, an enterprise organization may choose to adopt the following:

a) an identity-based access control (IBAC) model;

b) a role-based access control (RBAC) model;

c) an attribute-based access control (ABAC) model;

d) a capability-based access control (CBAC) model;

e) a pseudonym-based access control (PBAC) model.

The choice between these models is not necessarily exclusive and can be tailored according to different sets of subjects.

NOTE See Annex A for information on access control models.

7.2.2 Policies in access management

AMS policies include policies for controlling access to resources and policies for managing and administering the AMS itself. Policies should be established for these activities together with compliance criteria and means of monitoring and assessing compliance.

The policy will be dependent on the access control model chosen and the details of the implementation while setting up the policy, and its compliance will be dependent on general considerations that may cover the following:

a) matching the access control policy with the access control model employed;

b) determining and setting access control privileges and attributes for subject access and administrative purposes in accordance with the overall access control policy and permitted operations on resources;

c) limiting access to resources to the minimum needed to perform the required operation;

d) requiring the authenticated identity of persons and entities to a given level of assurance prior to authorization considerations;

e) determining the authorization of persons and entities to perform requested access operations on resources;

f) granting or denying access to resources in accordance with authorization criteria and access policy in response to access requests;

g) protecting the privacy of personal data used in the implementation of access control operations;

h) implementing monitoring and recording of access transactions to a sufficient level of granularity to enable auditing of access transactions in order to demonstrate adherence to system and other compliance requirements.

The policy may be documented in natural language (see 6.2.1). Subsequently, the policy should be translated in digital policy. It should be confirmed that the digital policy is equivalent to the natural language policy. Acceptable evidence of conformity to these requirements should be included.

7.3 Legal and regulatory requirements

Relevant legal and regulatory requirements can apply to the implementation of an access management system. These can include:

a) monitoring and recording access events;

b) management of privacy sensitive information.

8 Practice

8.1 Processes

8.1.1 Authorization process

Where authorization is to be implemented as a service, the service interface can utilize an existing standard, e.g. References [12] and [17].

8.1.2 Privilege management process

8.1.2.1 Overview

The privilege management process implements the access control policy for the domain of applicability through the assignment of resource access privileges.

NOTE In the case of the RBAC model, the privilege management process would provide the following function:

a) assigning individuals to roles and setting role privileges that entails;

b) ensuring that individuals are eligible to perform the role and to be assigned the role privileges;

c) assigning the appropriate role name attribute to individuals who will act in that role;

d) assigning the relevant resource access control privileges to the role name.

If the privileges associated with a role are changed, a review of individuals assigned to the role should be undertaken to ensure that they are still eligible to perform the role with the new privileges. If this review is not carried out, the relevant individuals will need to be de-assigned from the role.

8.1.2.2 Availability of privilege information

The subject privilege information needed to control access to protected resources is recorded in the PIP and is made available to the PDP on request.

NOTE Information about subject privileges can be personal or private and can require protection against unauthorized disclosure.

Access control policies should additionally include the following measures.

a) When a subject from a trusted relationship or trusted third party needs to access a resource, the resource should retain its normal access control attribute permissions regardless of whether the resource resides in the original resource owner's organization or in the requester subject organization. The resource should have the ability to authorize access or it should refer back to the resource owner's access regime for a new authorization request as if the data were still in the owning organization.

b) Controls related as enterprise information protection also protect the flow of data between systems and actors, within the resource owner's organization, and externally to other organizations when the resource is accessed from a trusted third party. Such protection is to prevent specific data leaving the organization in any event and particularly if there is an access control failure. This includes, for example, email filters.

8.2 Threats

Referring to Figure 7, the following threats are assumed on request/response communication between PEP and PDP interactions.

a) PDP masquerading

PDP can be a bogus service.

b) Subject identifier capture

An attacker can use a session hijacking attack capture to the subject identifier in access token.

c) Subject identifier manufacture

An attacker can attempt to generate a valid subject identifier for an access token and use it to impersonate a subject.

d) Access token disclosure

Disclosure of access token may make the AMS vulnerable to other types of attacks because it may contain sensitive authorization and attribute information.

e) Access token manufacture/modification

An attacker can generate a bogus access token or modify the access token content.

f) Access token substitution

A subject can attempt to impersonate a more privileged subject by subverting the communication channel between PDP and PEP.

g) Access token reuse

An attacker attempts to use the access token that has already been used with the intended PEP.

h) Access token redirect

An attacker uses the access token to one PEP to obtain unauthorized access to a different resource.

i) Denial of service threat

Accidental or deliberate threat to the operation of an access management system that can result in a denial of service to subjects.

Referring to Figure 6, threats are assumed not only on communication between components services but also on user agent which the subject is using because the sensitive communication goes through the user agent.

Countermeasures and controls to address these threats should be considered. For further guidance on the determination of suitable control objectives and controls, refer to 8.3.

8.3 Control objectives

8.3.1 General

This subclause summarizes objectives and controls to be verified when setting up or reviewing an implementation of an AMS.

a) It first covers objectives to be addressed before establishing the management system.

b) It then covers objectives of the access management system implementation.

c) It eventually covers objectives of operating the access management system.

In addition, general security objectives and controls stated in ISO/IEC 27002 are also relevant for the access management system.

8.3.2 Validating the access management framework

8.3.2.1 Documenting the management framework

8.3.2.1.1 Objective

To establish a management framework to initiate and control the implementation of managing access of subjects.

An access management framework should document, at a minimum: the groups of subjects recognized in the framework, their authentication process, the access control policies with the authorized models, the policy enforcement points (PEP), the means by which each recognized subject may be verified across its lifecycle in the framework and may be provisioned authorizations to access resources, and the possible extensions of the framework in a federation.

8.3.2.1.2 Scope and limits of the management framework

a) Control

The set of attributes used for being authenticated and presented to accessing resources should be clearly defined and documented in a framework for access management.

b) Implementation guidance

The boundaries of a framework for access management should clarify the limits where the subjects can be verified.

The objective, or the legal reason, and the associated liabilities, of the environment where subjects can exist clarify the limits where a framework of access management can apply its control on subjects.

c) Other information

An environment where subjects are defined is made in relation to a particular set of attributes on which an access management system can apply controls.

The scope and boundaries of the framework should also be considered in accordance with the implementation of the ISO/IEC 24760 series.

8.3.2.1.3 Documenting policies

a) Control

A set of policies to support IT strategy on access management should be developed and maintained.[14] These policies should include intent, methods of controls, roles and responsibilities, exception process, compliance approach, and references to procedures, standards and guidelines. Their relevance should be confirmed and approved regularly.

b) Implementation guidance

Policies of an access management framework may vary depending on the chosen implementation. However, a number of general policies and a compliance statement should be set when implementing a management framework, considering the following policies:

1) access control policy, identifying objectives and constrains to be implemented when applying access control in the boundaries of the framework, implementing general considerations made in 7.2.2;

2) compliance policy to the preservation of human privacy in the implementation of access control operations (see also 8.3.2.2);

3) monitoring and tracing (recording) activities of access policy, ensuring a sufficient level of granularity of traces to enable auditing of access transactions in order to demonstrate adherence to system and other compliance requirements.

c) Other information

A framework for access management can be subject-centric, centralized on one policy decision point or enterprise and distributed across multiple PDP. Each implementation aspect leads to different documentation of policies requirements.

The policies may be documented in natural language. However, subsequently, the policies should be translated in digital policy and it should be confirmed that the digital policy is equivalent to the natural language policy. Acceptable evidence of conformity to these requirements should be included.

8.3.2.1.4 Identifying subjects accessing resources in the framework

a) Control

The entities that make control of access to resources to subjects (e.g. PDP and PEP) should be recognized in a framework for access management.

b) Implementation guidance

Entities that can make provable statements on the validity and/or correctness of subject to access resources in the framework (e.g. PDP, PEP), should be recognized in a framework for access management;

Entities endorsing management and regulator responsibilities for the preservation of privilege information should also be identified (e.g. PIP).

c) Other information

An entity can combine the functions of PDP, PDP or PIP.

8.3.2.1.5 Identifying authorities of the management framework

a) Control

Authorities composing the framework for access management, i.e. AMS, IMS, AA, STC, PIP, PDP, PEP, REDS, should be documented and communicated. These entities encompass the PDP, PEP, and the PIP.

b) Implementation guidance

The documentation of the PDP, the PEP, and the PIP should at least encompass the requirements for verifying information privileges, the requirements from the users of information privileges, and the conditions of authorizing and using information privileges.

8.3.2.2 Assuring privacy of subjects when required

a) Control

It is necessary to ensure the privacy of subjects at all times as part of the objectives of establishing a framework for access management, at a level of assurance required by the subjects.

b) Implementation guidance

A framework for access management should establish the necessary controls that guarantee, when required, the preservation of the privacy of the human subjects it interacts with.

A framework for identity management should document any sensitive information it processes about human entities according to ISO/IEC 24760–1.

c) Other information

Requirements for the handling of privacy are given in ISO/IEC 29100 and ISO/IEC 29101.

8.3.2.3 Maintaining the management framework definitions

a) Control

A process should be described that ensures the maintenance of the framework documentation.

b) Implementation guidance

Components of a framework for access management may use over time different structures of privilege information and authorities to support their interactions with entities. Domains may also be created and terminated, or their conditions of usability may change (e.g. change of model).

The verifications of an access management framework should include the governance, policies, processes, data structures, technology, and standards that ensure the control of the lifecycle of key important components, from initial setup to decommissioning and replacement in the framework, reflecting any change in the framework documentation.

8.3.3 Validating the access management system

8.3.3.1 Overview

An access management system implements the controls on a subject when accessing resources within a framework for access management. The AMS operates based on policies, models, scope and constrains

identified at framework level. With reference to ISO/IEC 27001 and/or ISO/IEC 27002, the management of information security within an organization expects all systems should have access controlled under the supervision of an IMS (as defined in the ISO/IEC 24760 series) and an AMS. Compliance to ISO/IEC 27001 and ISO/IEC 27002 control objectives consequently imposes the AMS to comply with a number of additional control objectives:

a) the components and the structure for operating the controls of access should be listed;

b) the used access models should be documented (e.g. IBAC, RBAC, ABAC; CBAC, PBAC);

c) privileges and attributes under specific access models should be defined;

d) the authorization processes should be defined and documented;

e) the risk associated to an AMS should be audited and mitigated.

8.3.3.2 Components of an access management system

8.3.3.2.1 Objective

To ensure a system is implemented and well documented for the management of access to resources.

8.3.3.2.2 Components of an access management system

a) Control

An access management system should include, at a minimum, the following components and all of these components should be properly documented:

1) a central management system, capable of collecting access control information from various validated sources (attributes domains of origins), and deleting the information when the conditions for storing privilege information cease to exist;

2) a repository for privilege information related to the entities types recognized in domains of the relevant framework with different attributes sets, semantic and syntax, identifying privileges and conditions for use;

3) a storage component archiving the information on privileges that ceased to exist;

4) a repository of privilege assignments, within possibly the repository of privilege information, collecting any assignment of privilege reference to any subject reference with the framework for access management;

5) management interfaces for providing access to the need to have privilege information;

6) definitions for PDP, enforcements (PEP), information (PIP), administration (PAP);

7) a generator of unique reference identifiers of privileges to which unique identifiers of users are assigned and reported in the repository of privilege of information.

b) Implementation guidance

Privilege management systems may vary in components depending on the model developed for its implementation. The privilege management system should, however, remain independent as it is required to respond to functional requirements specific and largely different from any other usual IT system.

8.3.3.2.3 Documenting the access models

a) Control

The access models of an access management framework should be documented. The documentation should include:

1) the description of an access right (privilege) to access resources;

2) the rules specifying the method of assigning the privilege to recognized subjects;

3) the authorization process of assigning the privilege to subjects;

4) the update or revocation process of privileges;

5) the verification method of accessing resources.

b) Implementation guidance

A subject can have multiple privilege assignments based on different models in a framework. In a domain of applicability of the framework, a subject can have resources authorized, which are based on a particular model. In another domain of applicability, a subject can become a distinguishing subject with different privileges within that domain. The repository of a framework for access management should be able to gather the various authorizations of the different subjects it recognizes under different models of accesses. Attributes describing a subject in a domain are values on which the repository of the framework may associate different authorized privileges.

Each privilege and associated descriptions should be documented in the framework repository, with details required by the model in order to assign and control the privilege authorized to a subject.

8.3.3.2.4 Communicating between components of an access management system

a) Control

Communications between components composing the framework for access management should be defined and communicated.

b) Implementation guidance

Communications between authorities and systems composing the framework for access management should be defined in conditions, situations and expected results. These communications should be preserved from any leakage to any party outside of the mentioned components.

A procedure should clearly define the condition for communication between the components.

Regular audits should verify that the security of the communications is preserved.

8.3.3.3 Establishing privileges

8.3.3.3.1 Objective

To define, document and communicate on privileged information.

8.3.3.3.2 Privilege representation

a) Control

Access to resources should be defined based on privileges definitions established under the discretion of the information owner and taken into techniques used to control their assignment and their provision when accessing the information.

b) Implementation guidance

Privileges should be defined in each system and application falling into the limits of the framework for access management. Privileges are representations of necessary permissions that users are required to

be assigned and provisioned before accessing the requested information. They represent objectives and controls associated with assignments of subject's access to resources in relation to certain attributes.

The privilege representation should take into account the sensitivity of the information being accessed and the various techniques used to control their provision to a subject when accessing this information. Depending on the sensitivity of the information, a different level of assurance in the subject proofing may be required. At the time of the access, the access verifiers should be informed from the privilege representation of the requirements for accessing this information.

c) Other information

ISO/IEC 27002 provides additional information on controlling the access to the information.

8.3.3.3.3 Privilege information definition

a) Control

Access control to the information and information processing should enforce guidelines specifying requirements for a fixed set of attributes that compose a privilege to access resources. The values of attributes should take into account the sensitivity of the information defined by the information owner, should be validated by the verifiers (PEP), and should be communicated.

b) Implementation guidance

The guidelines should clarify the values for a number of parameters or conditions that should be validated before the privilege can be assigned to an individual.

Access to information, its dissemination and provisioning should only be authorized on "need-to-have" and "need-to-know" principles, and based on information classification. Information asset owners should determine appropriate information classification that would clarify the restrictions for specific privileges and associated user roles, and the controls reflecting the associated information security risks.

8.3.3.3.4 Assurance in collecting information for privilege control

a) Control

All information security responsibilities for the collection and the management of privilege information should be defined and allocated. The collection of privilege information should define levels of assurance to be verified in the identification of the user.

b) Implementation guidance

The level of assurance in the control of the user's access when using a specific privilege should be clarified when defining information for privilege control. Typically, at least two levels of authentication requirements are defined. One is based on user identification, to which a password is associated and shall be verified with some levels of severity. The other is based on two factors, combining the first method with a different element, e.g. a one-time password given by an electronic token.

8.3.3.4 Controlling an access management system

8.3.3.4.1 Objective

To ensure a framework for access management is delivering the intended objectives.

8.3.3.4.2 Administering an access management system

a) Control