INTERNATIONAL STANDARD

ISO/IEC 29146

First edition
2016-06-01

Information technology — Security techniques — A framework for access management

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

Reference number
ISO/IEC 29146:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

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

Introduction

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

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

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

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

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

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

Information technology — Security techniques — A framework for access management

1 Scope

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

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

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

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

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

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

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

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

3 Terms and definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

— authorization endpoint, where subject authorization is performed;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

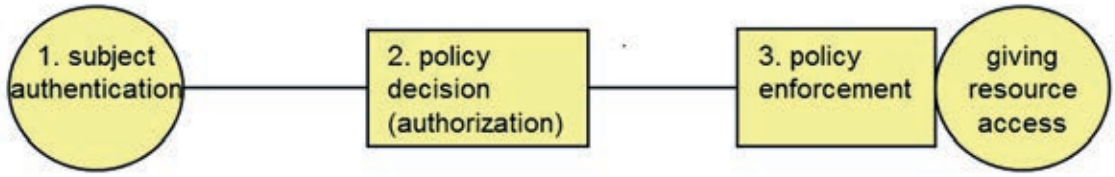

Figure 1 — Access control model sequence

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

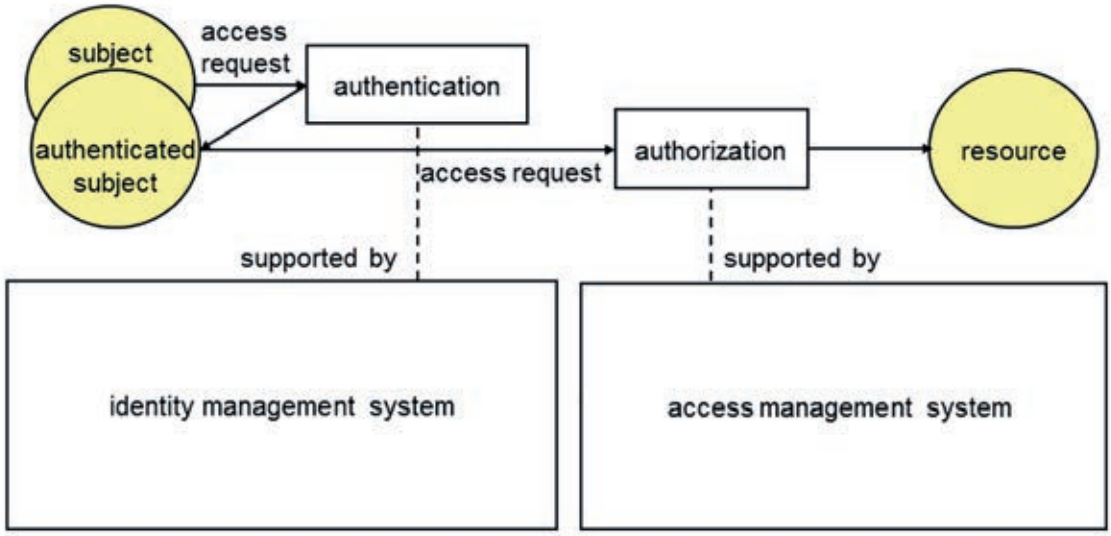

Figure 2 — Identity management system and access management system relationship

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 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 vary according to the architecture and the access control model used, e.g.

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 subject not to require any authentication. In this case, anonymous entity may be allowed to go directly to the AMS, and 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 need to be validated 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 International Standard 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 (AMS) 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, and

— 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 (AMS) enforces an access control policy. A number of access control models exist (see Annex A). This International Standard 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);

— Role-based Access control (RBAC);

— Attribute-based Access Control (ABAC).

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 and this 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 could 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 MAC 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 may be applied sequentially, the order of application might 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 most general case where access control is based on AMS defined attributes possessed by subjects. IBAC, PBAC and RBAC are particular cases of ABAC where the attributes are, respectively, identity, pseudonymous identity and role. These four models may be implemented using ACLs.

When the subject presents a capability ticket (in a CBAC model) for authorization, 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 PBAC, IBAC, RBAC, ABAC 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 role-based access control (RBAC), 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 (AMS). 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 attribute-based access control (ABAC), 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 and 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) the creation of 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 may be assigned to both human subjects and non-human subjects. For example, when a device or a service is added to a network, it may 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), and

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 access control lists (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 policy decision point (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 could 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 and will need to be authenticated in the same or in an equivalent way to that for the subject. 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 will need to be contacted to ask if this unauthorized person is allowed to access the resource.

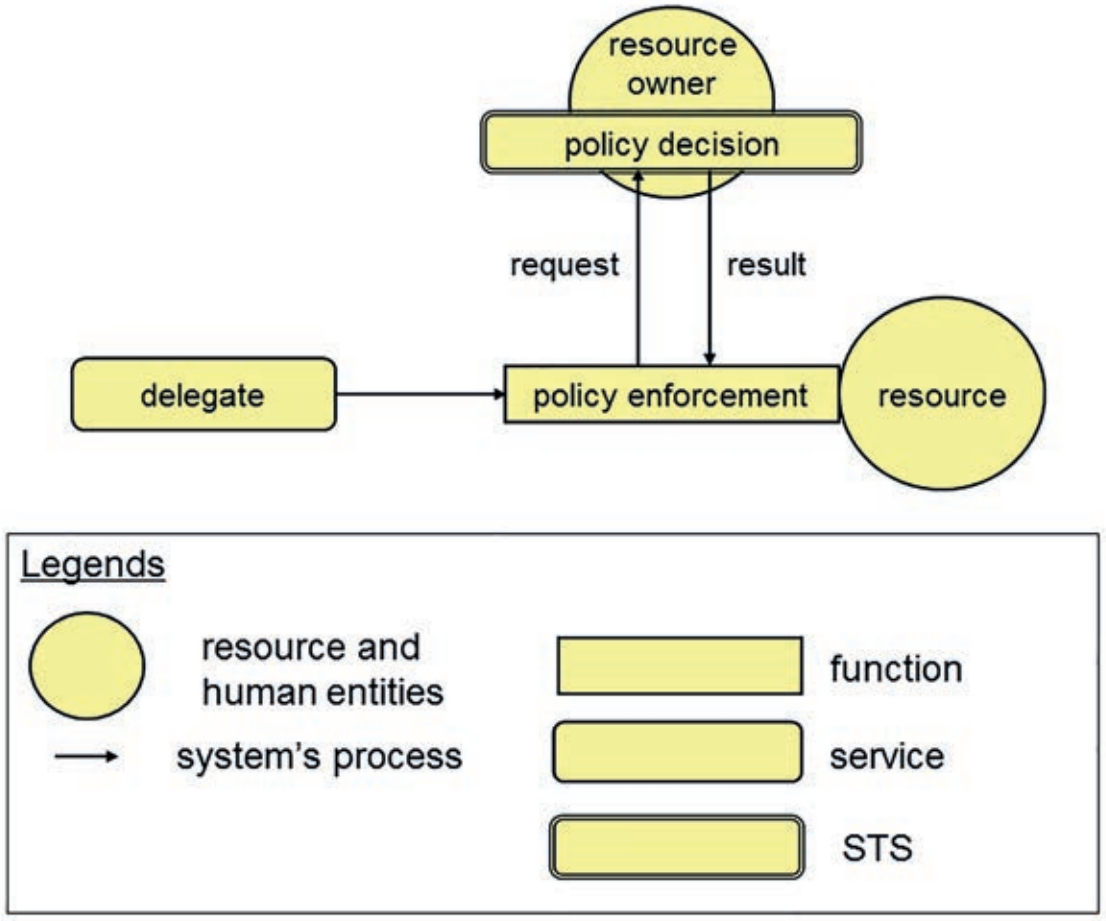

Figure 3 — Authorization of delegate access

5.3.6 Monitoring management

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

The access management system (AMS) should provide auditable monitoring and record keeping capabilities for the purposes of regulatory compliance, liability, and investigation.

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 could 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

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 ISO/IEC 24760. 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.

a) The subject to authenticate 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.

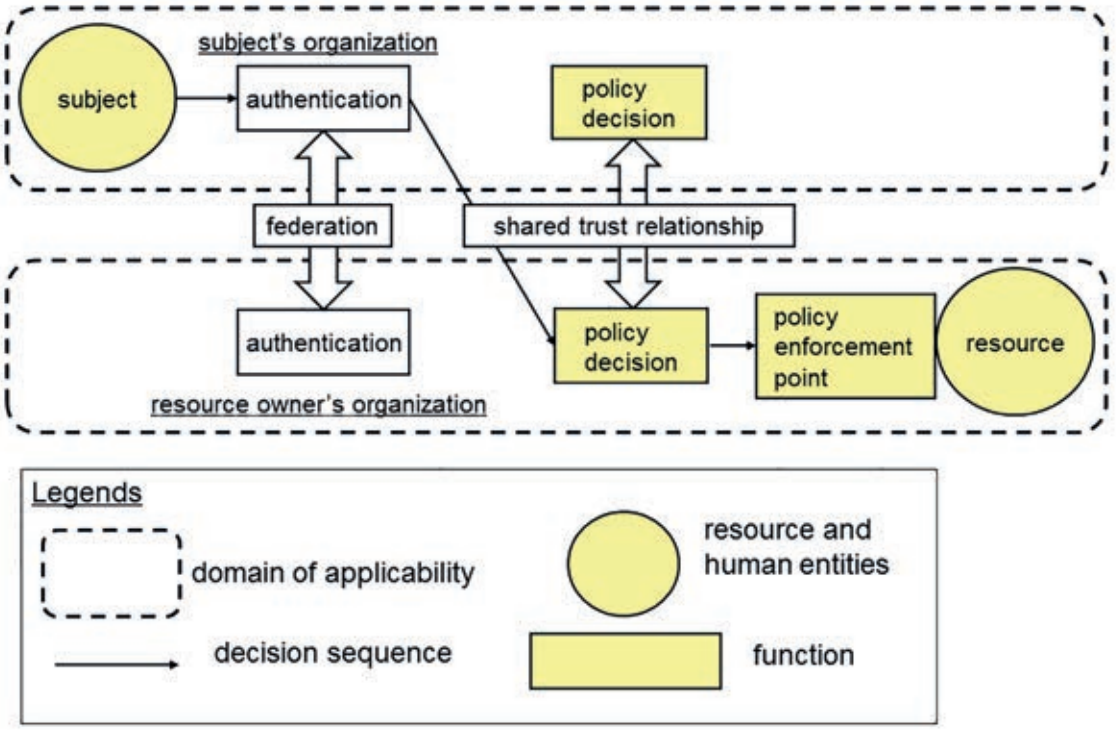

Figure 4 — Federated access control

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

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

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

c) 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.

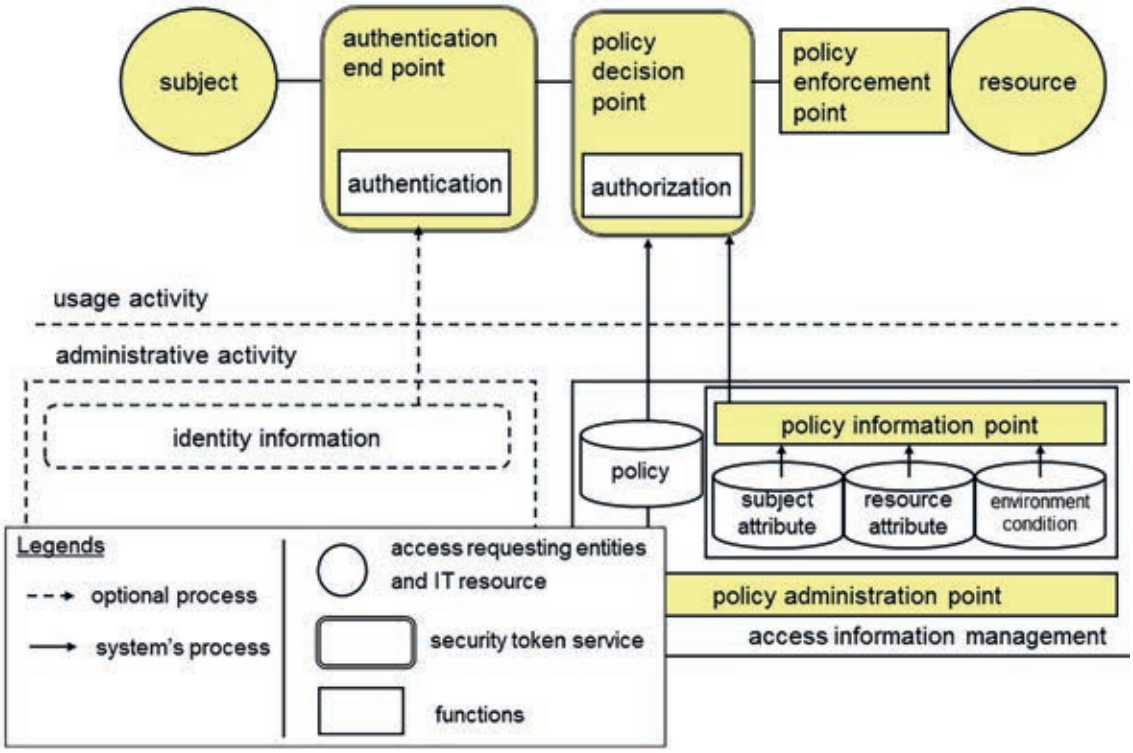

Figure 5 — AMS reference architecture

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 (PDP)

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 (PIP)

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 (PAP)

This component provides the interface for administrating policy set and related information on PIP. The administration of them 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 (PEP)

The policy enforcement point (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 Policy Decision Point (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.

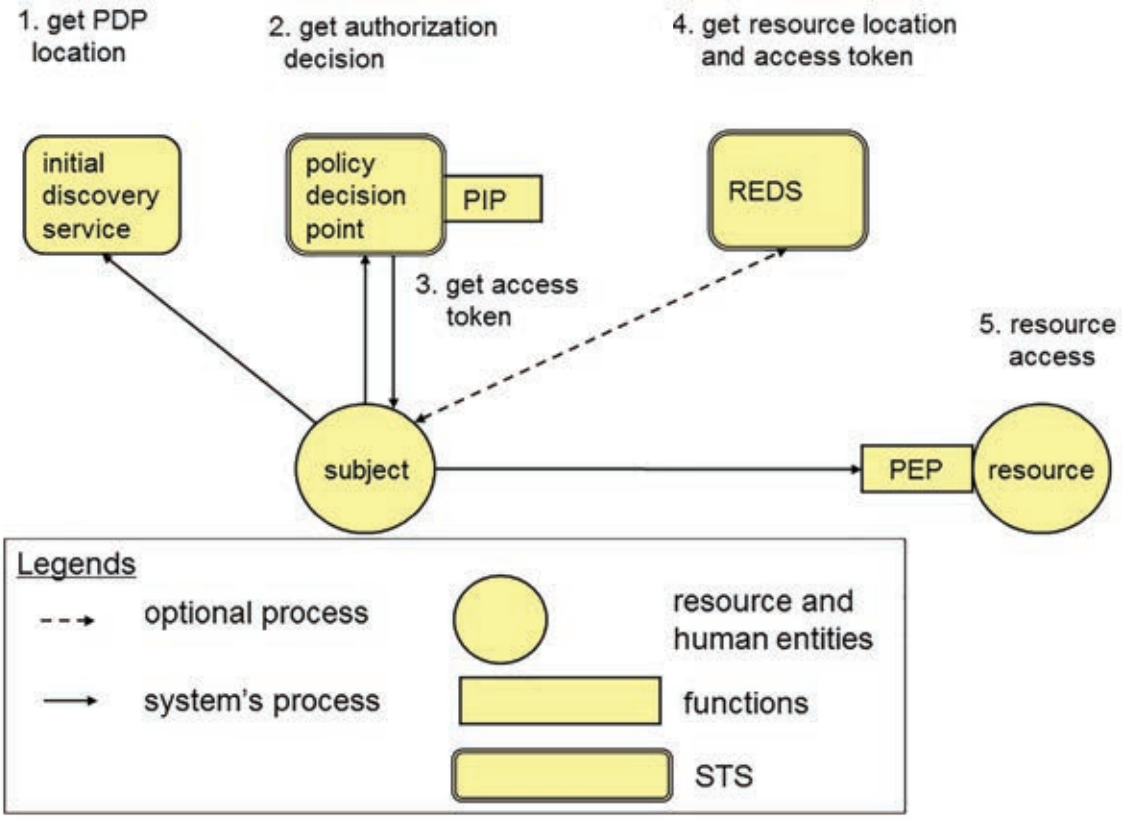

Figure 6 — Components services interactions in subject centric situation

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 (STS)

Based on the decision made by the policy decision point (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, SAML assertion etc. Refer to the applicable standards for details on these.

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

6.3.2.4 Resource discovery service (REDS)

A resource discovery service (REDS) provides 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.

There is some information about data location which needs to be protected because it may reveal privacy sensitive information. (e.g. location of a medical record may reveal the nature of the illness.)

NOTE In some situations, the response from the REDS may be uniform across the subjects and stable for prolonged periods. Therefore, the response may be resolved through static metadata, rather than dynamically. Also, in some AMS implementations, a REDS may 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 in 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 1 The resource access may 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 he needs.

An example of the latter situation is when the subject does not wish to reveal its identify 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 policy enforcement point (PEP) plays a crucial role.

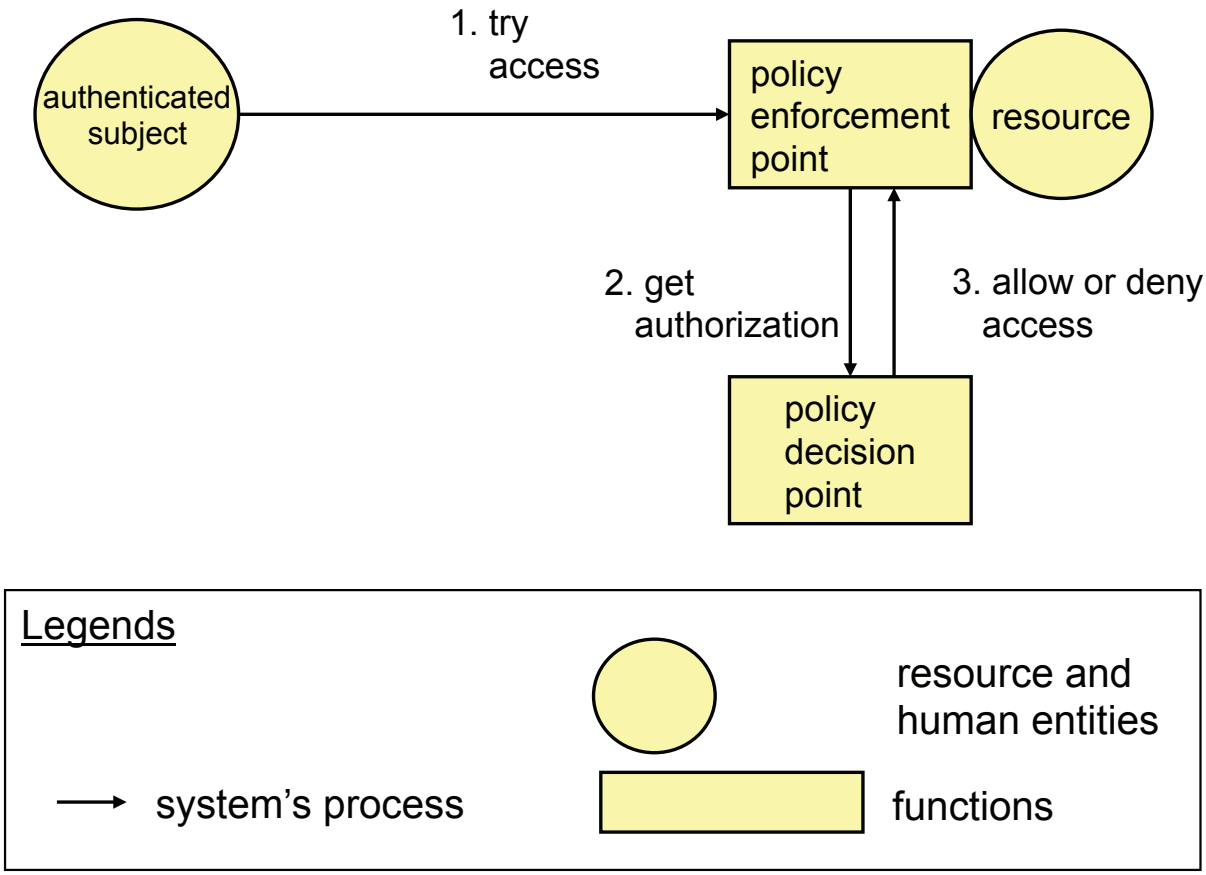

Figure 7 — Components services interactions in enterprise situation

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 need to be changed and the PEP will continue to function unchanged.

There should be a trust relationship between the policy decision point and the policy enforcement point.

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 in the following steps.

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

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

c) The PDP makes 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 (PAP).

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

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 needs to 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 about 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 need to be established for these activities together with compliance criteria and means of monitoring and assessing compliance.

Policy will be dependent on the access control model chosen and the details of the implementation while the setting up of 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

The implementation of an access management system should conform to any legal and regulatory requirements applicable in the jurisdictions of its use. For example, there may be some legal and regulatory requirements on

a) monitoring and recording access events, and

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. Reference [12] and Reference [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 to be 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 not, 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 may be personal or private and may require protection against unauthorized disclosure.

Access control policies should additionally include the following measures.

a) When a resource needs to be accessed by a subject from a trusted relationship or trusted third party, 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, following threats are assumed on request/response communication between PEP and PDP interactions.

a) PDP masquerading

   PDP may be a bogus service.

b) Subject identifier capture

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

c) Subject identifier manufacture

   An attacker may 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

Attacker may generate a bogus access token or modify the access token content.

f) Access token substitution

A subject may 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 could result in a denial of service to subjects.

Referring to Figure 6, components services interactions in subject centric implementation, 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

In 8.3.1 objectives and controls to be verified when setting up or reviewing an implementation of an access management system (AMS) are summarized.

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.

The groups of subjects recognized in the framework, their authentication process, the access control policies and authorized models, the identification of 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 in the framework, and the framework's possible extensions within a federation, should be documented.

8.3.2.1.2 Scope and limits of the management framework

Control

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

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.

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.

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

8.3.2.1.3 Documenting policies

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.

Implementation guidance

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

a) 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;

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

c) 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.

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

Control

To ensure entities that make control of access to resources to subjects (e.g. PDP and PEP) are recognized in a framework for access management.

Implementation guidance

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

b) Entities endorsing management and regulator responsibilities for the preservation of privilege information should also be identified [Policy Information Points (PIP)].

Other information

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

8.3.2.1.5 Identifying authorities of the management framework

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 Policy Decision Point, Policy Enforcement Point, and the Policy Information Point.

Implementation guidance

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

8.3.2.2 Assuring privacy of subjects when required

Control

To ensure the privacy of subjects is preserved at any time as part of the objectives of establishing a framework for access management, at a level of assurance required by the subjects.

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 to conform to ISO/IEC 24760–1.

Other information

Requirements for the handling of sensitive identity information are given in the following International Standards:

a) ISO/IEC 29100

b) ISO/IEC 29101

8.3.2.3 Maintaining the management framework definitions

Control

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

Implementation guidance

a) 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).

b) Access management framework verifications 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 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 Identity Management System (IMS, defined and document in ISO/IEC 24760) and an AMS. The implement of this ISO/IEC 27001 and/or ISO/IEC 27002 objective consequently imposes the AMS to comply with a number of control objectives. These control objectives include the following:

a) listing components and structure for operating the controls of access;

b) defining and documenting access models (e.g. IBAC, RBAC, ABAC; CBAC, PBAC);

c) defining privileges and attributes under specific access models;

d) defining and documenting the authorization processes;

e) auditing and mitigating the risk associated to an AMS.

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

Control

An access management system should include, at a minimum, the following:

a) 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;

b) 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;

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

d) 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;

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

f) definitions for points of decision (PDP), enforcements (PEP), information (PIP), administration (PAP);

g) 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.

All these components should be properly documented.

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 needs to respond to functional requirements specific and largely different from any other usual IT system.

8.3.3.2.3 Documenting the access models

Control

The description of an access right (privilege) to access resources in the framework, the rules specifying the method of assigning the privilege to recognized subjects, the authorization process of assigning the privilege to subjects, the update or revocation process of privileges, and the verification method of accessing resources should be documented.

Implementation guidance

a) A subject can have multiple privilege assignments based on different models in a framework. In a domain of applicability of the framework, a subject may have resources authorized based on a particular model, and in another domain of applicability become a distinguishing subject to be distinguished 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.

b) 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

Control

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

Implementation guidance

a) 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.

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

c) 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

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.

Implementation guidance

a) 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.

b) 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.

Other information

ISO/IEC 27002:2013, Clause 9, provides additional information on controlling the access to the information.

8.3.3.3.3 Privilege information definition

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.

Implementation guidance

a) 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.

b) 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

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.

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 based on user identification to which a password is associated and shall be verified with some levels of severity, and one 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

Control

Administering an access management system should be limited to people dedicated to its maintenance, related authorities and relying parties.

Implementation guidance

An Access management system should develop the required interfaces and procedures to guarantee proper access information maintenance according to the rights defined and authorized by the relevant authorities.

8.3.3.4.3 Auditing an access management system

Control

An access management system and other components required for the establishment of a framework for access management should be assessed or audited annually on a regular basis, mitigating the risks associated to an AMS.

Implementation guidance

The audit or assessment should validate that the access management system is operating in accordance with its documented policies and procedures and is compliant with legal and other externally imposed requirements (e.g. privacy requirements).

Assessments or audits should:

a) include statements describing the operations performed by the access management system, in particular with respect to meeting operational policies,

b) include the verification of the secure communication between the components of the framework,

c) validate that the privilege management system reports on specific operations (e.g. vulnerabilities), assess if the operations meet applicable policies (e.g. privacy control), and alert on any discrepancies, and

d) include accountability of a subject.

Objectives and controls for the mitigation of the risks described in 8.2 should be further developed depending on the components composing the AMS.

8.3.4 Validating the maintenance of an implemented AMS

The Maintenance of the management framework was addressed at 8.3.2.3. The AMS includes also many definitions that require maintenance.

8.3.4.1 Maintaining the authorizations

8.3.4.1.1 Objective

— To ensure the framework can keep effective maturity in its control by maintaining the definitions and the procedures.
— To ensure that the privileged information is maintained and protected in a framework.

8.3.4.1.2 Maintaining the processes of authorizing a subject to access a resource

Control

A formalized process should be documented that verifies the requirements defined by the privilege definition of assigning a privilege to a subject in order to access resources.

Implementation guidance

a) The process of authorizing a privilege assignment to a subject should involve the owner of the accessed information and the verification authorities' representatives. It should guarantee that the controls foreseen in the privilege definition should be validated prior to the assignment and provisioning of a privilege to a subject.

b) The process should dissociate the need-to-have from the need-to-know questions. The need-to-have should validate the justification of requesting the access. The need-to-know should, in addition, validate condition for accessing the information (e.g. segregation of duties guarantee, privacy guarantee). Conditions are formulated by the information owner and the verifiers.

c) The process should be formal and should minimize the number of controls to the steps required by the sensitivity of the information being accessed. It should take into account controls already be verified when accessing the information and that can be conditional requirements for the provisioning of the access rights (e.g. the subjects is already authenticated in the networks of the organization).

d) Allocation of access rights in a distributed network environment should be managed recognizing all type of connections available, considering different roles and profiles, ensuring the documentation of rights is formally reviewed, and segregating the controls of the request, the authorization, and the administration.

e) Business needs and effective employment status should be periodically reviewed to re-confirm the assignment of privileges, and when required removed (see also 8.3.4.2.2).

The use and the management of user identities and authentication information should be monitored, recorded and archived.

Other information

ISO/IEC 27002:2013, Clause 9, provides additional information on controlling the access to the information.

8.3.4.1.3 Review of privilege definitions

Control

Information privilege definitions should be reviewed for accuracy and need to have on regular basis.

Implementation guidance

a) Access management definition should include policies, processes, data, technology, and standards to ensure the control of keys important components of the framework over their lifecycle.

b) All the key components should have their definition be maintained. People controlling the authorization process may change over time, technologies may be replaced. Information defining privileges should be controlled and accordingly reviewed on a regular basis.

c) Systems may also change over time, may be created and terminated or their conditions of usability may change (e.g. change of access control model).

d) A process should be documented that ensures the maintenance of the information of the defined privileges in a framework.

e) Changes to privileges definitions should be logged for reviews.

8.3.4.2 User access management

8.3.4.2.1 Objective

To ensure the access rights assignments reflect the business needs and do not pose risks.

8.3.4.2.2 Review of users' access rights assignments

Control

Information owners should review users' privileges and their justifications at periodic intervals using a formal process.

Implementation guidance

a) Privileges should be reviewed at periodic intervals and the business needs for the access rights should be re-validated. The periodicity of the review should be clarified by the information owner and made part of the review procedure. Periodicity of reviews should be linked to the sensitivity of the information being accessed (refer also to information classification guidelines). Reviews should be recorded for inspection.

b) Privileges should be reviewed, removed or re-allocated when the user is moving from one employment to another within the organization.

c) Changes to privileges assignments should be logged for reviews.

8.3.4.3 Monitoring and record keeping management

Control

Access rights definitions, authorizations, provisions and accountability of a subject should be recorded for auditing. Record keeping management should define the conditions of tracing and archiving the access request information, with objective of confirming that the operation of the AMS complies with the access control policy.

Implementation guidance

Audit trails of privilege definitions, authorizations and provisions should be kept for inspection and history tracing. The conditions for record keeping should be defined by the information owner. It should take into account the sensitivity of the accessed information

Annex A
(informative)

Current access models

A.1 General

Annex A introduces access control models which may be adopted as the basis of access control policy.

A.2 Access management models

A.2.1 General

Primarily, logical access control solutions have been based on the identity of a subject requesting execution of an operation upon a resource. This is the case of the IBAC model where access to a resource has been individually granted to a locally identified subject. Later on, a similar model has appeared where access to a resource has been granted to locally defined roles that the subject was a member of.

When a subject request access to a resource the qualifiers of identity, groups, and roles are often insufficient to express the different possibilities of combinations to grant the access. An alternative is to grant or deny subject requests based on arbitrary attributes of the subject and arbitrary attributes of the resource, and environment conditions that may be globally recognized and more relevant to the policies at hand.

A.2.2 Discretionary Access Control (DAC)

In a Discretionary Access Control (DAC) model, each resource has an owner and each owner can determine the operations other subjects can perform on that resource. The Discretionary Access Control (DAC) model allows a subject that has been assigned resource access privileges the discretion to delegate the privileges to other subjects or groups of subjects.

A.2.3 Mandatory Access Control (MAC)

The Mandatory Access Control (MAC) is most often used in systems where priority is placed on data confidentiality.

MAC was originally a security model that restricts the ability resource owners have to grant or deny an operation to be performed on objects placed in a file system. The controls were originally strictly enforced on a single machine by the Operating System (OS) which includes a security kernel.

Mandatory Access Control works by assigning a classification label to each file resource. Classifications include (1) a category of information and (2) a sensitivity level, like confidential, secret or top secret. Each subject is assigned a similar classification, called a clearance.

When a subject tries to access a specific resource, the system will check the subject's privileges to determine whether access will be granted but will also compare the clearance of the subject against the classification of the resource.

The MAC model defines is built upon the Discretionary Access Control (DAC) model with two additional MAC rules.

The Discretionary Security Property - individual resource owners can assign security controls on the objects they control, coming from the Discretionary Access Control (DAC) model.

The Simple Security Property - a subject at a given security level may not read a resource at a higher security level (no read-up).

The *-property (read “star”-property) - a subject at a given security level should not write to any resource at a lower security level (no write-down).

The *-property can only be enforced when using specific terminals and/or between systems that are both able to enforce the *-property.

However, the Simple Security Property can be enforced in a distributed environment. When a subject tries to read the content of a resource, the system will check the subject’s privileges to determine whether the read access can be granted using the DAC rules, but will also compare the clearance of the subject against the classification of the resource and will thus apply the Simple Security Property rule.

The MAC rules are not administered by the resource owners, but by security officers.

A.2.4 Identity-Based Access Control (IBAC)

An Identity-Based Access Control (IBAC) model employs mechanisms such as Access Control Lists (ACLs) which contain the identifiers of those subjects together with the operations allowed on that resource.

The identifiers being used usually carry some semantics related to the identity the subject.

Very often, the same identifier is used for all the resources. When it is the case, this provides the possibility to link the operations made by the same subject on different servers or machines.

The identifier may be an authenticated identifier obtained after a successful authentication exchange or may be included in an access token.

In the IBAC model subject identities are authorized and added to the ACL together with the relevant subject resource access privileges in order to allow the subject to access resources subsequently. When an identifier matches the one held in the ACL, the subject is given the privilege to perform on the resource the operations mentioned for that subject in the ACL.

The management of the ACL is necessary prior to any specific access request and results in the identifier being added into the ACL together with specific operations for the resource.

A.2.5 Role-Based Access Control (RBAC)

A Role-Based Access Control (RBAC) model employs mechanisms such as Access Control Lists (ACLs) which contain the roles of those subjects together with the operations allowed on that resource.

The roles being used usually carry some semantics but are shared by several subjects.

The role may be included in an access token (push model) or may be obtained from a Directory after a successful authentication (pull model).

When a role matches the one held in the ACL, the subject is given the privilege to perform on the resource the operations mentioned for that role in the ACL.

The management of the ACL is necessary prior to any specific access request and results in the role being added into the ACL together with specific operations for the resource.

The benefit of introducing roles is that it becomes not necessary to list an identifier in an ACL for each subject. RBAC role assignments are efficient when static organizational positions are being used.

Role may be inherited through a role hierarchy and typically reflect the privileges needed to perform defined operations within an organization. A given role may apply to a single subject or to several subjects.

A.2.6 Attribute-Based Access Control (ABAC)

An Attribute-Based Access Control (ABAC) model employs mechanisms such as Access Control Lists (ACLs) which contain the attributes of those subjects together with the operations allowed on that resource.

The attributes may be included in an access token (push model) or may be obtained from a Directory after a successful authentication (pull model).

When an attribute matches the one held in the ACL, the subject is given the privilege to perform on the resource the operations mentioned for that attribute in the ACL.

The management of the ACL is necessary prior to any specific access request and results in the attribute being added into the ACL together with specific operations for the resource.

A.2.7 Pseudonym-Based Access Control (PBAC)

A Pseudonym-Based Access Control (PBAC) model employs mechanisms such as Access Control Lists (ACLs) which contain the pseudonyms of those subjects together with the operations allowed on that resource.

The pseudonyms being used carry no semantics related to the identity the subject.

Often, a different pseudonym is used for each different server or service. When it is the case, this provides the impossibility to link the operations made by the same subject on different servers or machines.

The pseudonym may be an authenticated pseudonym obtained after a successful authentication exchange or may be included in an access token.

When a pseudonym matches the one held in the ACL, the subject is given the privilege to perform on the resource the operations mentioned for that subject in the ACL.

The management of the ACL is necessary prior to any specific access request and results in the pseudonym being added into the ACL together with specific operations for the resource.

A.2.8 Capability-Based Access Control (CBAC)

A Capability-Based Access Control (CBAC) model employs capabilities assigned to a subject in relation to the requirements for accessing a resource. In access control, capabilities are typically embodied within access tokens, which are issued by a trusted authority to subjects that are permitted to access the relevant resources. An access token contains information that enables the token and the issuing authority to be validated (e.g. through digital certificates and signing) and to specify the access permissions for the subject to the resources. An access token may also contain information that enables a subject to be authenticated as the true owner of the token. Issuing an access token (capability) to a subject authorizes the subject to access the relevant resources with given permissions.

A CBAC model token employs capability tickets which contain two main components: (a) the identifier of a resource and (b) the operation(s) allowed on that resource.

These tickets are granted by an Authority. A PDP will not trust all the authorities, and for the authorities that it trusts, it will only accept tickets that contain a specific set of operations.

The PDP will thus manage a matrix which contains several lines, with, for each line,

a) an identifier of a recognized authority that may issue capability tickets, and

b) the operation(s) that may be included in a capability ticket for that recognized authority.

A capability may be included in an access token (push model) or may be obtained from a Directory after a successful authentication (pull model).

When a capability ticket matches with the content of a line of the matrix, the subject is given the privilege to perform on the resource the operations mentioned in the matrix.

The management of the matrix is necessary prior to any specific access request and results in the identifier of a recognized authority that may issue capability tickets being added into the matrix together with specific operations that may be included in a capability for that recognized authority.

In order to fulfil audit requirements, it is necessary to be able to identify the subject that has been authorized to perform an operation on a resource. This is done differently whether a push model or a pull model is being used.

In a push model; the capability is included in an access token and some other information present in the token allows to identify indirectly the subject (usually only with the cooperation of the Authority that has issued the access token).

In a pull model, the subject is first authenticated and the identifier used during the authentication exchange is included into an audit trail.

The token issuance process may be a one-time operation, i.e. once the access token is issued, it can be used by the subject for multiple access requests until/unless the access token is revoked. This is commonly the case where physical access tokens are used (e.g. smartcards). In other situations, access token issuance may be of a transient nature with a token having a limited (e.g. per session; per transaction) usage.

In the CBAC model, the access token issuing authority fulfils the role of the policy decision point in an access control system, the decision being embedded in the token. A subject requesting access to a resource presents the access token directly to the policy enforcement point (PEP) for the resource. The PEP validates the integrity of the access token and its issuing authority and checks the embedded resource access permissions before granting access to the resource by the subject.

Bibliography

[1] Recommendation ITU-T X. 812 | ISO/IEC 10181-3, Information technology — Open Systems Interconnection — Security frameworks for open systems: Access control framework

[2] Identity Management, Document No: W041, Copyright © [March 2004] The Open Group (Skip Slone and The Open Group Identity Management Forum), http://www.opengroup.org/onlinepubs/7699959899/toc.pdf

[3] ITU-T X.1252:2010, *Baseline identity management terms and definitions (04/10)*

[4] SC 27 Standing Document 6 (SD 6) Glossary of IT security terminology

[5] Review Developing Definitions ISO/IEC JTC 1/SC 27 N5603

[6] Gollmann Dieter "COMPUTER SECURITY", WILLEY (1999)

[7] RFC 6749, The OAuth 2.0 Authorization Framework, IETF (October 2012), http://www.ietf.org/rfc/rfc6749.txt

[8] Priebe T., Dobmeier W., Schläger C., Kamprath N. Supporting Attribute-based Access Control with Ontologies, In proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), IEEE Computer Society (2006)

[9] National Institute of standards and Technology (NIST), "Role Based Access Control and Role Based Security"; http://csrc.nist.gov/groups/SNS/rbac/.

[10] National Institute of standards and Technology (NIST), NISTIR 7657, "A Report on the Privilege (Access) Management Workshop" http://csrc.nist.gov/publications/nistir/ir7657/nistir-7657.pdf

[11] National Institute of standards and Technology (NIST), SP800-162 Guide to Attribute Based Access Control (ABAC) Definition and Considerations (January 2014)

[12] Standard O.A.S.I.S. "eXtensible Access Control Markup Language (XACML) Version 3.0" (January 2013) http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf

[13] Identity Management Audit / Assurance Program, ISACA, ISBN 978-1-60420-298-4

[14] The IT Assurance Guide Using COBIT, ISACA

[15] COBIT (Control Objectives for Information and Related Technology) 4.1 and 5.0, A Business Framework for the Governance and Management of Enterprise IT, ISACA

[16] Part 2: ITU-T X.509 |ISO/IEC 9594-8:2014 Information technology — Open Systems Interconnection the Directory: Public-key and attribute certificate frameworks

[17] Kantara Initiative. "User-Managed Access (UMA) Profile of OAuth 2.0", Version 1.0 (2015-02-23), https://docs.kantarainitiative.org/uma/draft-uma-core.html

ICS 35.040

Price based on 35 pages