

<b>Third Committee Draft ISO/IEC 3<sup>rd</sup> CD 29146</b>		Reference number: ISO/IEC JTC 1/SC 27 <b>N14154</b>	
Date: 2014-06-16		Supersedes document SC 27 N13381	
THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.			
ISO/IEC JTC 1/SC 27 Information technology – Security techniques Secretariat: DIN, Germany		Circulated to P- and O-members, and to technical committees and organisations in liaison for voting (P-members only) by: <b>2014-09-17</b> Please return all votes and comments in electronic form via the SC 27 e-balloting application by the due date indicated.	
<b>ISO/IEC 3<sup>rd</sup> CD 29146</b> <b>Title: Information technology – Security techniques -- A framework for access management</b> Project: 1.27.64 (29146)			
<b>Explanatory Report</b>			
<b>Status</b>	<b>SC 27 Decision</b>	<b>Reference documents</b>	
		<b>Input</b>	<b>Output</b>
<i>For details regarding previous development stages please see the subsequent pages 2 and 3.</i>			
<b>ISO/IEC 29146 1<sup>st</sup> CD</b>	15 <sup>th</sup> SC 27/WG 5 Plenary, April 2013, resolutions 1, P4 (N12555); 25 <sup>th</sup> SC 27 Plenary, April 2013, resolution 7 (N12739).	SoCom (N12264).	Liaisons to: Art. 29 (N12506); Kantara (N12520); SC 37 (N12523); Editors' report (N12558); DoCom (N12539); Text f. 1 <sup>st</sup> CD (N12540).
<b>ISO/IEC 29146 2<sup>nd</sup> CD</b>	16 <sup>th</sup> SC 27/WG 5 Plenary, Oct. 2013, resolutions 1, 14 (N13373).	SoV (N12982).	Liaisons to: Art. 29 (N13351); Kantara (N13361); SC 37 (N13341); DoCom (N13380); Text f. 2 <sup>nd</sup> CD (N13381).
<b>ISO/IEC 29146 2<sup>nd</sup> CD</b>	16 <sup>th</sup> SC 27/WG 5 Plenary, Oct. 2013, resolutions 1, 14 (N13373).	SoV (N12982).	Liaisons to: Art. 29 (N13351); Kantara (N13361); SC 37 (N13341); DoCom (N13380); Text f. 2 <sup>nd</sup> CD (N13381).
<b>ISO/IEC 29146 3<sup>rd</sup> CD</b>	17 <sup>th</sup> SC 27/WG 5 Plenary, April 2014, resolutions 1, 5, 9, P1 (N14199); 26 <sup>th</sup> SC 27 Plenary, as per resolution 8 Delegation of Authority f. DIS (N14200).	SoV (N13775).	Liaisons to: Art. 29 (N14132); Kantara (N14142); SC 37 (N14121); DoCom (N14153); Text f. 3 <sup>rd</sup> CD (N14154).
<b>3rd CD Consideration</b> In accordance with resolution 9 (see SC 27 N14199) of the 17th SC 27/WG 5 Plenary meeting held in Hong Kong, China, 11th April 2014, the hereby attached document is being circulated for a 3rd Committee Draft (CD) letter ballot closing by <b>2014-09-17</b> Medium: <a href="http://isotc.iso.org/livelink/livelink/open/jtc1sc27">http://isotc.iso.org/livelink/livelink/open/jtc1sc27</a> No. of pages: 1 + 32			

Secretariat ISO/IEC JTC 1/SC 27 -

DIN Deutsches Institut für Normung e.V., Am DIN-Platz, Burggrafenstraße 6, D-10772 [D-10787] Berlin, Germany

Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-4-2652; E-mail: krystyna.passia@din.de;

<HTTP://www.jtc1sc27.din.de/en>

Explanatory Report (pages 2-3)			
Status	SC 27 Decision	Reference documents	
		Input	Output
NWIP	3 <sup>rd</sup> SC 27/WG 5 Plenary, Oct. 2007, resolution 13 (N6251).		NWIP (N6256rev1).
ISO/IEC NP 29146 1 <sup>st</sup> WD	5 <sup>th</sup> SC 27/WG 5 Plenary, April 2008, resolutions 1, 8, 9, 10, P6 (N6726).	SoV (N6525).	Call f. contr. (N6807); Text f. 1 <sup>st</sup> WD (N6756) N/A.
ISO/IEC 29146 1 <sup>st</sup> WD	6 <sup>th</sup> SC 27/WG 5 Plenary, Oct. 2008, resolutions 1, 4, 8, P1 (N6726).	US NB contr (N8621).	DoCom (N7244); Text f. 1 <sup>st</sup> WD (N7245rev2).
	7 <sup>th</sup> SC 27/WG 5 Plenary, May 2009, resolutions 1, 5, P1, P2, P10 (N7724).	BR NB com (N7635); SC 37 com. (N8045);	Call f. proj. edit.(N7720) Call f. contr. (N7720); DoCom (N7756).
	21 <sup>st</sup> SC 27 Plenary, May 2009, resolution 24 (N7777).		
ISO/IEC 29146 2 <sup>nd</sup> WD	8 <sup>th</sup> SC 27/WG 5 Plenary, Nov. 2009, resolutions 1, 7, 15 (N8811).	SoCom (N8054); SC 37 com. (N8045);	Call f. co-editor (N8377); Liaisons to: Art. 29 (N8155); SC 31 (N8140); SC 37 (N8155); DoCom (N8274); Text f. 2 <sup>nd</sup> (N8275).
ISO/IEC 29146 3 <sup>rd</sup> WD	9 <sup>th</sup> SC 27/WG 5 Plenary, April 2010, resolutions 1, 7, 15 (N8828rev.).		Editors' report (N8937); DoCom (N8811); Text f. 3 <sup>rd</sup> (N8812).
ISO/IEC 29146 4 <sup>th</sup> WD	10 <sup>th</sup> SC 27/WG 5 Plenary, Oct. 2010, resolutions 1, 5, P5, P9 (N9402).	SoCom (N9155); SC 37 com. (N9292); TC 215 com. (N9159)	Request/endorsement f. limit dates extension (N9526); Editors' report (N9437); Call f. co-editor (N9262); Liaisons to: Art. 29 (N9253); TC 215 (N9242); SC 31 (N9243); SC 37 (N9255); DoCom (N9231); Text f. 4 <sup>th</sup> (N9232).
	22 <sup>nd</sup> SC 27 Plenary, Oct. 2010, resolution 30 (N9460).		

Explanatory Report (pages 2-3)			
Status	SC 27 Decision	Reference documents	
		Input	Output
<b>ISO/IEC 29146 5<sup>th</sup> WD</b>	11 <sup>th</sup> SC 27/WG 5 Plenary, April 2011, resolutions 1, 4, P4 (N9920).	JP nomin. f. proj. editor (N9725); SoCom. (N9726).	Art. 29 (N9757); SC 31 (N9767); SC 37 (N9751); DoCom (N9909); Text f. 5 <sup>th</sup> (N9910).
	12 <sup>th</sup> SC 27/WG 5 Plenary, Oct. 2011, resolutions 1, 5, 10 (N10525).	SoCom (N10355); JP com. (N10365); SC 37 com. (N10362).	Establim. of ad hoc group (ToR N10565); Art. 29 (N10536); SC 31 (N10526); SC 37 (N10528); Kantara (N10540); DoCom (N10559); Advice to editors (N10547); Updated text of 5 <sup>th</sup> WD (N10956*). *replaces N10560, N10660
<b>ISO/IEC 29146 6<sup>th</sup> WD</b>	13 <sup>th</sup> SC 27/WG 5 Plenary, May 2012, resolutions 1, 2, 5 15 (N11280).	Ad hoc group com N10952); Darft DoC (N10974);	Formal LB limit dates extension (N11769); SoV on N11769 (N12070); Call f. contr. (N11336); Liaisons to: Art. 29 (N11263); SC 37 (N11258); Text f. 6 <sup>th</sup> (N11247).
<b>ISO/IEC 29146 7<sup>th</sup> WD</b>	14 <sup>th</sup> SC 27/WG 5 Plenary, Oct. 2012, resolutions 1, 14 (N11701).	SoCom (N11570); CA NB com. (N11372); Kantara com. (N11552).	Liaisons to: Art. 29 (N11714); Kantara (N11720); SC 37 (N11705); DoCom (N11737); Text f. 7 <sup>th</sup> (N11736).

ISO/IEC JTC 1/SC 27 N14154

Date: 2013-12-15

ISO/IEC 3<sup>rd</sup>CD 29146

ISO/IEC JTC 1/SC 27/WG 5

Secretariat: DIN

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

*Élément introductif — Élément central — Élément complémentaire*

### Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

### Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

Secretariat, ISO/IEC JTC 1/SC27  
DIN - Deutsches Institut für Normung e.V.  
Burggrafenstrasse 6  
DE-10772 Berlin  
Germany

Telephone: + 49 2601-2652  
Facsimile: + 49 2601-1723  
E-mail: [krystyna.passia@din.de](mailto:krystyna.passia@din.de)  
Web: [www.jtc1sc27.din.de/en](http://www.jtc1sc27.din.de/en)  
<http://isotc.iso.org/livelink/livelink/open/jtc1sc27> (SC 27 documents)

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Contents	Page
Foreword .....	v
Introduction.....	vi
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions .....	2
4 Symbols and abbreviated terms .....	5
5 Concepts .....	6
5.1 A model for controlling access to resources .....	6
5.1.1 Overview.....	6
5.1.2 Relationship between identity management system and access management system .....	7
5.2 Relationships between logical and physical access control.....	8
5.3 Access management system internals .....	8
5.3.1 Overview.....	8
5.3.2 Policy management.....	8
5.3.3 Privilege management .....	9
5.3.4 Policy related attribute information management .....	10
5.3.5 Authorization .....	10
5.3.6 Monitoring and record keeping management .....	11
5.3.7 Federated Access Control .....	11
6 Reference architecture.....	13
6.1 Logical view of basic components .....	13
6.2 Implementing components as services .....	14
6.2.1 Initial Endpoint Discovery service .....	14
6.2.2 Policy Enforcement Point (PEP) .....	14
6.2.3 Policy Decision Point (PDP) .....	14
6.2.4 Communication between PDP and PEP.....	14
6.2.5 Security Token Service (STS) .....	14
6.2.6 Policy Administration Point (PAP).....	15
6.2.7 Resource Endpoint Discovery Service (REDS).....	15
6.2.8 Aggregation Service.....	15
6.2.9 Interactions of components .....	15
7 Requirements.....	18
7.1 Threats and countermeasures .....	18
7.2 Access to administrative information .....	19
7.3 Compliance .....	19
7.3.1 Policies in access management .....	19
7.3.2 Policy on access control model.....	19
7.3.3 Policy from organizational considerations.....	19
7.3.4 Legal and regulatory requirements .....	20
8 Practice.....	21
8.1 Processes.....	21
8.1.1 Authorization process.....	21
8.1.2 Privilege management process .....	21
8.1.3 Availability of privilege information .....	21
Annex A Current access models (informative) .....	23
A.1 General .....	23
A.2 Models .....	23
A.2.1 (DAC).....	23
A.2.2 (MAC) .....	23
A.2.3 RBAC .....	24
A.2.4 IBAC .....	24
A.2.5 ABAC .....	24

## Figures

Figure 1 – Access control model .....	6
Figure 2 – Identity management system and access management system.....	7
Figure 3 – Authorization of delegate access .....	10
Figure 4 – Federated Access Control .....	12
Figure 5 – AMS Reference Architecture .....	13
Figure 6 – Components interactions .....	17

## 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 29146 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information technology Subcommittee*.



## 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 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, nowadays, information technology resources can be located over distributed networks, and the access to them needs to be managed in conformity under a policy. Therefore, it was expected to have common terms and models as a framework on access management.

Within the management of information security, identity management also plays a key role. Access management is mediated through the identification and authentication of subjects that seek to access information technology resources. This standard depends on the existence of an underlying identity management system or identity management infrastructure. Regarding this topic, see references pointed out in normative references section.

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

It focus mainly on access control for a single organisation, but adds other considerations for access control in collaborative arrangements across multiple organisations.

# 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 ICT information 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, "A framework for identity management".

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

## 2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the addition cited applied. For undated references, the latest edition of the referenced document (including any amendments) applies.

- ISO/IEC 24760-1, Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts.
- ISO/IEC 24760-2,<sup>†</sup> Information technology -- Security techniques -- A framework for identity management -- Part 2: Reference architecture and requirements.
- ISO/IEC 24760-3,<sup>†</sup> Information technology -- Security techniques -- A framework for identity management -- Part 3: Practice.
- ISO/IEC 29115 – Information technology -- Security techniques -- Entity authentication assurance framework.

---

<sup>†</sup> to be published

<sup>†</sup> to be published

### 3 Terms and definitions

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

**3.1**  
**access control**  
process of granting or denying access to a **resource** (3.9)  
)

NOTE 1 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 When an authenticated subject 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** (3.9)  
)

NOTE Access management involves a set of resources and a set of using subjects.

**3.3**  
**endpoint**  
programming interface where the service can be called

**3.4**  
**least privilege**  
security objective to establish for an authorized subject the minimum rights for accessing to a specific resource in order to accomplish its assigned tasks

**3.5**  
**need to know**  
security objective of keeping the subject's access to data resources to the minimum necessary for them to perform their functions

**3.6**  
**obligation to share**  
requirement for one party to provide information to another party to comply with previously agreed information sharing policy and for the good of the community

**3.7**  
**privilege**  
access rights

permission

Assignment to a particular subject of the right to access data associated with specific roles given to the subject or to identity attributes possessed by the subject

NOTE A privilege does not guarantee access. Access occurs when the resource owner authorizes (or grants access to) a user to access a resource following an access request. The access request (or assertion) must provide evidence that the requestor has previously assigned the appropriate privileges.

**3.8**  
**role**  
name given to a defined set of system functions that may be performed by multiple entities.

NOTE 1: The name is usually descriptive of the functionality

NOTE 2: Entities are typically but not necessarily human subjects"

NOTE 3 Usually a roles are implemented by a set of privilege attributes that are needed to access different data objects

NOTE 4 Subjects that are assigned the same role can have their common privileges/access rights managed via a single role. This ensures consistent access control decisions

### **3.9**

#### **resource**

#### **object**

physical, network, financial or information asset that can be accessed for use by a subject

### **3.10**

#### **subject**

user

entity involved in access control (3.1) as holder of a privilege

### **3.11**

#### **policy decision point**

PDP

access decision

system component which evaluates applicable policy and makes an authorization decision

NOTE This term corresponds to "Access Decision Function" (ADF) in [ISO10181-3]. It is supposed that this function is located over network from the subject, and may be located over network from the corresponding PEP.

### **3.12**

#### **policy enforcement point**

PEP

system component that performs access control to resource, based on the authorization decisions made by PDP

NOTE This term corresponds to "Access Enforcement Function" (AEF) in [ISO10181-3]. It is supposed that this function is located over network from the subject, and may be located over network from the corresponding PDP.

### **3.13**

#### **policy administration point**

PAP

system component that provides a user interface for administrating a policy or policy set

### **3.14**

#### **policy information point**

PIP

system component that acts as the source of policy related attribute information needed by the PDP to make the authorization decision

### **3.15**

#### **security token service**

STS

system component that function as a service that builds, signs, and issues security tokens



## 4 Symbols and abbreviated terms

ABAC	attribute based access control
AM	access management
AMS	access management system
ICT	information and communication technology
IMS	identity management system
IT	information technology
PII	personal identifiable information
PDP	policy decision point
PEP	policy enforcement point
PIP	policy Information point
PAP	policy administration point
RBAC	role based access control
STS	security token service
XACML	extensible access control markup language

NOTE identity management system is also called IDMS

## 5 Concepts

### 5.1 A model for controlling access to resources

#### 5.1.1 Overview

Figure 1 – Access control model

shows the conceptual sequence in giving access to resource in real-time activity:

- An authenticated subject (a human or an ICT system component) submits a request to the policy decision point component for access to a protected resource.
- Corresponding policy decision point (PDP) makes an authorization decision based on its policy: allow or deny,
- Policy enforcement point (PEP) which is protecting the resource will enforce the authorization decision result.

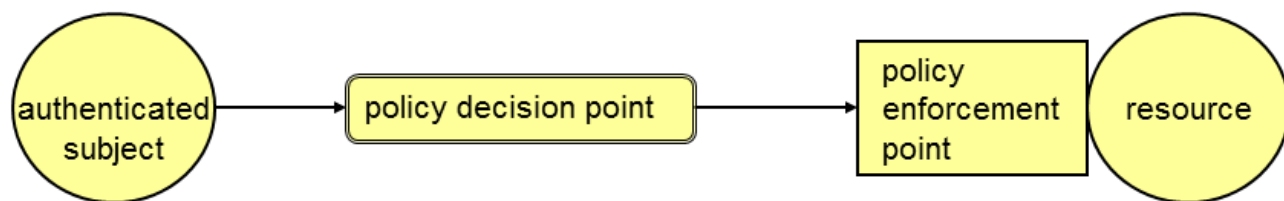


Figure 1 – Access control model

Subject and resource are depicted as balloons, and conceptual functions are depicted as rectangle.

A resource is characterised by:

- An identifier, either for a specific resource or for a resource class,
- A set of control attributes;
- One or more modes of access.

This conceptual sequence in giving access to resource is usually supported by administrative activity. Usage activity is also supported by identity management system and access management system.

### 5.1.2 Relationship between identity management system and access management system

First, the subject successfully authenticates using the identity management system (IMS), which is described in ISO/IEC 24760-2. The authenticated subject then requests access using the access management system (AMS). Authorization addresses two aspects that can be granted previously or during operational use:

- The pre-assignment of resource access privileges to subjects
- 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).

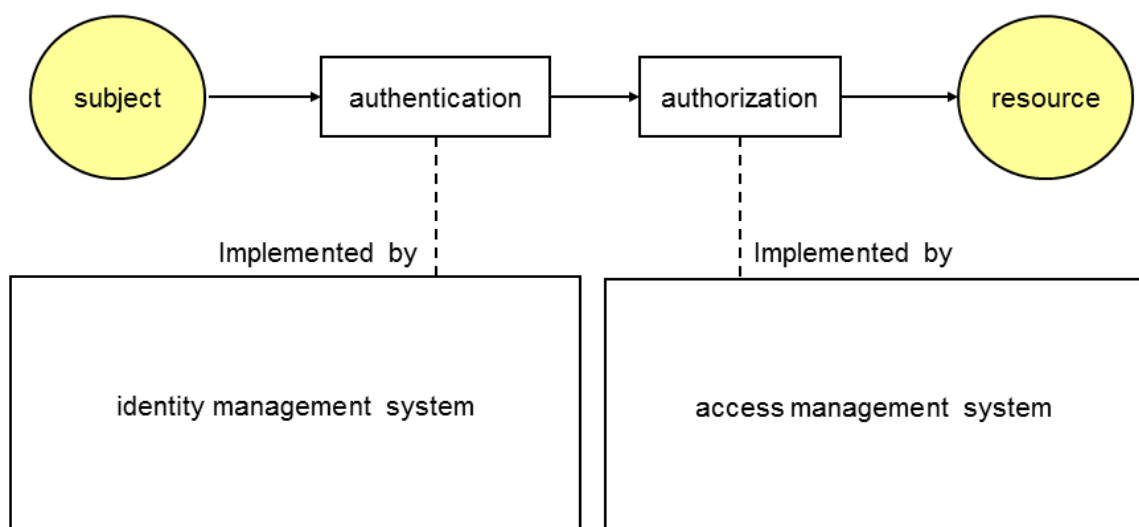


Figure 2 – identity information management and access information management

Authentication is implemented by identity management system (IMS) and it 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. The identity management system supports the functions of subject authentication identity information management.

**NOTE** Granting access to a resource may require a level of assurance in authentication. The required level depends on the resource to be accessed. For further information on authentication level of assurance, see ISO/IEC 29115 - Entity authentication assurance framework.

In the same way, authorization is supported by access management system (AMS) that supports access information management.

The actual procedure to access some resource may be performed differently from this conceptual model:

- When an AMS is implemented as Web service system, a subject may request access to a resource without first being authenticated. Then, the AMS will urge the subject to go to IMS to get authentication.
- When ABAC policy is adopted, there is a possibility for a subject not be required any authentication. In this case, anonymous entity may be allowed to go directly to the AMS, and authorization decision will be made based on the asserted attribute.

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



## 5.2 Relationships between logical and physical access control

This 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 outsourced service, the outsourced service shall be accountable for its physical access control so that it can be trusted by the subject.

## 5.3 Access management system internals

### 5.3.1 Overview

The access management system (AMS) provides real-time authorization to access protected resources and have two core functions:

- - to assign resource access privileges to subjects in advance of operational use
- - to use these privileges (together with other information where appropriate) to control subject access to system resources in operational use.

Administrative functions to support the core functions include:

- Policy management
- Policy-related attribute management
- Monitoring and record keeping management

Resource access policy shall conform to the following principles:

- Setting access privileges on a "need to know" basis
- Data access minimisation to use only strictly required data and minimize data leakage and disclosure risk
- Segregation and protection of sensitive data
- Protection of PII.

### 5.3.2 Policy management

An access management system (AMS) enforces an access control policy. There are several access control models which are applicable to adopt as policy in distributed network environment:

- Identity-based Access Control (IBAC)
- Role-based Access control (RBAC)
- Attribute-based Access Control (ABAC).

An access control policy should be developed based on the relevant model(s). For further information on the models, see Annex A

First, access control policy shall 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 and so on This policy based on the natural language (or other) representation shall be implemented in software algorithms or mechanisms in the access control system.

Second, there may be multiple access control policies within an organization hierarchy. Some policy may be applied to a division's resource, and other policy may be applied to overall organization. To support consistent policy within an organization, those policies should be deconflicted and documented.

Access control is typically provided through the mechanism of granting and enforcing access that allow specific subjects types to access to specific resources based on the policy.

Authorization decision is conducted based on comparison of subject descriptor and permission. The comparison may be implemented by means of an access control matrix associated with each resource which lists the identity of all subjects authorized to access the resource together with their assigned access privileges. IBAC and RBAC models are in some ways special cases of ABAC in terms of the attributes used. IBAC/ACLs work on the attribute of "identity. RBAC works on the attribute of "role".

To administrate access control policy, a user interface is required. It is called policy administration point (PAP).

### 5.3.3 Privilege management

Privilege management is conducted mainly within identity management system (IMS). And privilege management is affected by the access control policy above.

Under Identity based access control policy, privilege setting and removal is conducted for each identity based account. IBAC policy employs mechanisms such as access control lists (ACLs) to capture the identities of those allowed to access the object. If a subject presents a credential that matches the one held in the ACL, the subject is given access to the object. Each object needs its own ACL and set of privileges assigned to each subject. In the IBAC model, the authorization decisions are made prior to any specific access request and result in the subject being added to the ACL.

Under RBAC policy, privilege is not set directly within IMS. Instead, a role is set to each identity based account. Authorization decision is made based on the role within the access management system (AMS).

In the same way, under ABAC policy, privilege is not set within IMS. Instead, a policy related attribute is set to each identity based account. Authorization decision is made based on the policy related attribute within the AMS. A subject may access resources as a member of a group, the possessor of attributes or as an individual and that role based, attribute based and individual based access control schemes can exist concurrently in an access control system.

Privilege management comprises the following activities:

- The definition of privileges to access resources in order to control business activities,
- Establishing the rules specifying the assignment of privileges to The authorization of assigning these to subjects,
- The assigning of privileges relating to subjects that are referenced by the PDP in order to decide whether or not to authorize subjects to access resources
- The update or revocation of privileges,
- The application of policy and privileges in verifying an access request.

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 set to both human subjects and non-human subjects. For example, when a device or a service is added to a network, they may have privileges.

### 5.3.4 Policy related attribute information management

Policy related attribute information management is conducted within AMS. And policy related attribute information management is affected by the access control policy above.

Under ABAC policy, policy related attribute information is needed by authorization decision. And, role in RBAC policy may be recognized as a typical instance of attribute from viewpoint of ABAC policy.

Management of Information about these setting of privilege to attribute is an administrative activity. This kind of information can be managed in centralized manor. The system component which is called policy information point (PIP) stores this kind of information. PIP acts as the source of required role or attribute information needed by the PDP to make the authorization decision.

### 5.3.5 Authorization

#### 5.3.5.1 Basic authorization

Authorization is real-time activity, and is performed by policy decision point (PDP) in accordance with the access control policy. This activity is supported by administrative activity.

In principle, authorization is performed under pre-defined access control policy.

#### 5.3.5.2 Authorization of delegate access

Different context of access authorization is possible. A legitimate delegate of the subject may be allowed to access particular protected resource as in Figure 3.

NOTE: This is a case OAuth technology is supposing.

The authorization decision is made 'on the fly' by the resource owner. The policy enforcement point (PEP) will ask the resource owner if allow or deny access by the delegate.

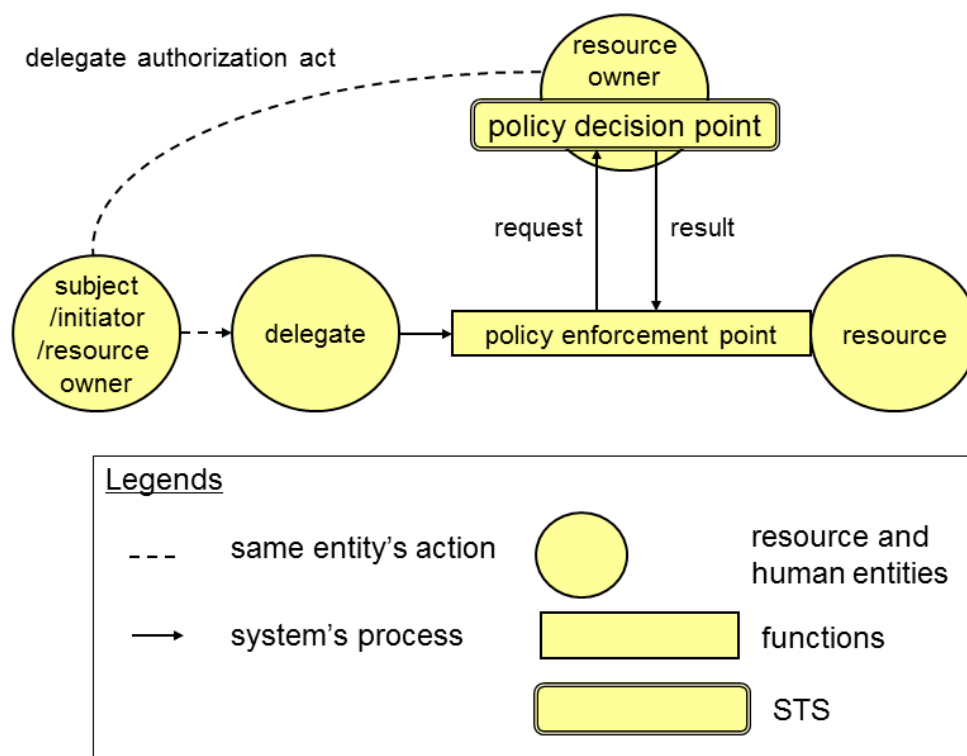


Figure 3 – Authorization of delegate access

### 5.3.6 Monitoring and record keeping management

Access management system (AMS) should provide a minimum set of capabilities to monitor and record to facilitate addressing their responsibilities.

If the process of authentication, prior to the processes that result in authorization requires certain level of assurance, AMS is affected and expected to keep the same level of requirements on monitoring and record keeping functionality.

Activities associated with access management have to be monitored for compliance, regulatory and investigative purpose.

### 5.3.7 Federated Access Control

Federated identity and access management is required when an authenticated subject from one organisation seeks to access a resource in another organisation. There are several models for federated identity management, which are considered in ISO/IEC 24760. Assuming a user can authenticate in a federation model, the federated access control requires the functional requirements for access control to be distributed across the relevant organisations within the community of trust, in accordance with common policies agreed by the organisations participating in the community. Federated access control requires:

- The subject to authenticate to his parent organisation's source of authority; then for
- For the subject's organisation to provide an access control assertion to the resource owner's organisation, which confirms the subject's authentication is valid and provides the authentication context and agreed access control attributes, including the ABAC or RBAC access rights; then for
- The data resource owner to accept the assertion and examine the attributes in relation to the data resources owner's access control policies; then for
- The data resource owner to authorise the subject to access the resource, or to deny access and inform the subject.
- All authorities to record access control events.

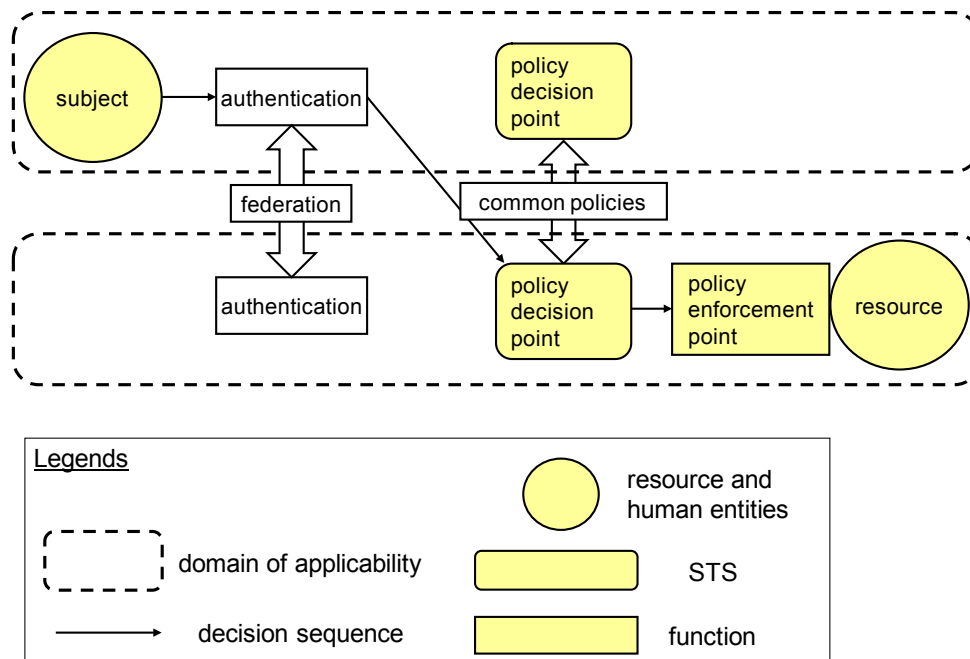


Figure 4 – Federated Access Control

Editors notes: accept the picture with modifications: legend, explain dotted lines (domain), change common policies with agreements, remove the arrow behind 'common policies'

The authentication context includes sufficient information about the event of authentication to the data resource owner, to enable the owner to authorise access (or not), and meet audit and liability requirements.

This assumes that the data resource owner has categorised and classified his information so that it can be accessed in a repeatable, predictable and controlled manner.

The federation common policy for access control should:

- Be based on common policy requirement to protect information for reasons of legal and regulatory compliance and intellectual property.
- Contain a policy hierarchy, based upon the common policy, from which access control rules and taxonomy can be based.
- Describe the attribute management regime, supported by the taxonomy. This taxonomy will enable policy interoperability and compliance across organisations.
- Describe procedures for the provisioning and management of access rights, the access control process and exception handling i.e. where an access request is rejected or a policy violation occurs.

## 6 Reference architecture

### 6.1 Logical view of basic components

Figure 5 – AMS Reference Architecture

presents basic functional components in understanding access management system:

- PEP: policy enforcement point: this component is a component of policy-based management. PEP may be accessed by subject before authentication and PDP. Then, PEP may request authentication and subsequently request authorization decisions to PDP. PEP performs access control to resource, based on the authorization decisions made by PDP. The result of the authorization decisions may be passed by security tokens.
- PDP: policy decision point: this component is also a component of policy-based management. PDP may make authorization decisions in response to PEP. PDP returns the decision to PEP.
- PAP: policy administration point: this component provides a user interface for administrating a policy or policy set. The administration of policy may include creating, testing, debugging and storing.
- PIP: policy information point: this component acts as a source of attribute and environment information needed by the PDP to make the authorization decision.

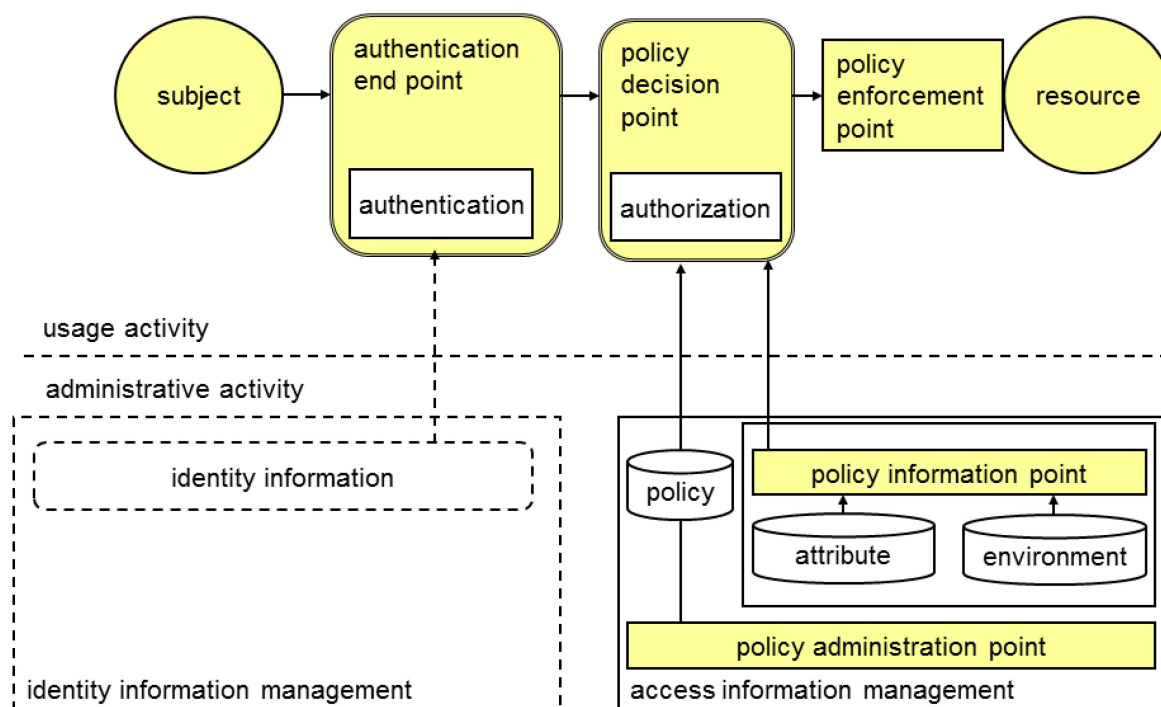


Figure 5 – AMS Reference Architecture

## 6.2 Implementing components as services

In implementing logical view of components as services, several components may be additionally introduced, and some considerations are required.

### 6.2.1 Initial Endpoint Discovery service

- There may be adopted a service to discover access control functions over a network, initially. Those access control functions are recognized as endpoints in network environment.
- Usually, the initial endpoint will be the subject authentication endpoint, or authorization endpoint which is equal to policy decision point (PDP).

NOTE: Subject authentication Service is not described here. Refer to ISO/IEC 24760 Parts 1 and 2, and x.1254/29115. Sometimes resource endpoint discovery happens here as well, in some optimizing situations where these are pushed together and where privacy/data protection is not an issue.

### 6.2.2 Policy Enforcement Point (PEP)

- Policy enforcement point (PEP) protects resource from unauthorized access.
- PEP intercepts the subject's access request to the resource and redirect to the authorization decision, which is made by the Policy Decision Point (PDP).
- PEP may allow access to the resource by accepting security token.

### 6.2.3 Policy Decision Point (PDP)

- Policy decision point holds the access policy or policy set for the resource. Based on the policy or policy set, PDP decides whether the subject may access to the resource.
- In some cases, the policy is created 'on the fly' through some kind of user interface. (In this case, this component is usually called as 'authorization endpoint', and the decision is called 'authorization decision'.
- PDP is supported by policy information point.

### 6.2.4 Communication between PDP and PEP

- Separating PEP and PDP as independent components produces compatibility and efficiency in developing access system to distributed resources. It is expected that even when the policy is changed, the separated implementations of PEPs may work without any modification.
- Trust relationship between Policy Decision Point and Policy Enforcement Point shall be required.

If PDP and PEP are located in distant networked environment, the communication between them shall be secured. PDP and PEP shall be able to confirm the authenticity of each other.

### 6.2.5 Security Token Service (STS)

- Security token service (STS) translates authorization decision made by PDP into some kind of security token.
- Security tokens are described differently in different technical standards. (Primary examples are the OAuth access token, the WS Trust Security Token, SAML assertion etc. Refer to the applicable standards for details on these.)

#### 6.2.6 Policy Administration Point (PAP)

- Policy Administration Point (PAP) provides a user interface for administrating a policy or policy set. The administration may include creating, testing, debugging and storing policy or policy set.
- 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 will be translated into digital policy so that PDP can use for authorization decision.

#### 6.2.7 Resource Endpoint Discovery Service (REDS)

- Resource endpoint discovery service (REDS) provides resource endpoints information as a protected resource. Therefore, the authorization decision is required to access REDS.
- In general, the endpoint information 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 cases, the response from 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, REDS may be a kind of STS, because it may provide a new token to access the resources.

#### 6.2.8 Aggregation Service

- Resource aggregation service aggregates multiple resources so that the subject can access the distributed multiple resources by going through just one endpoint in certain 'optimizing' situations. To optimize access performance, aggregation service may cache the resources.
- Trust relationship between the aggregation service and each PEP of resources is required.

#### 6.2.9 Interactions of components

There are several patterns of implementing components as services.

Following figure shows the case where subject plays the central role.



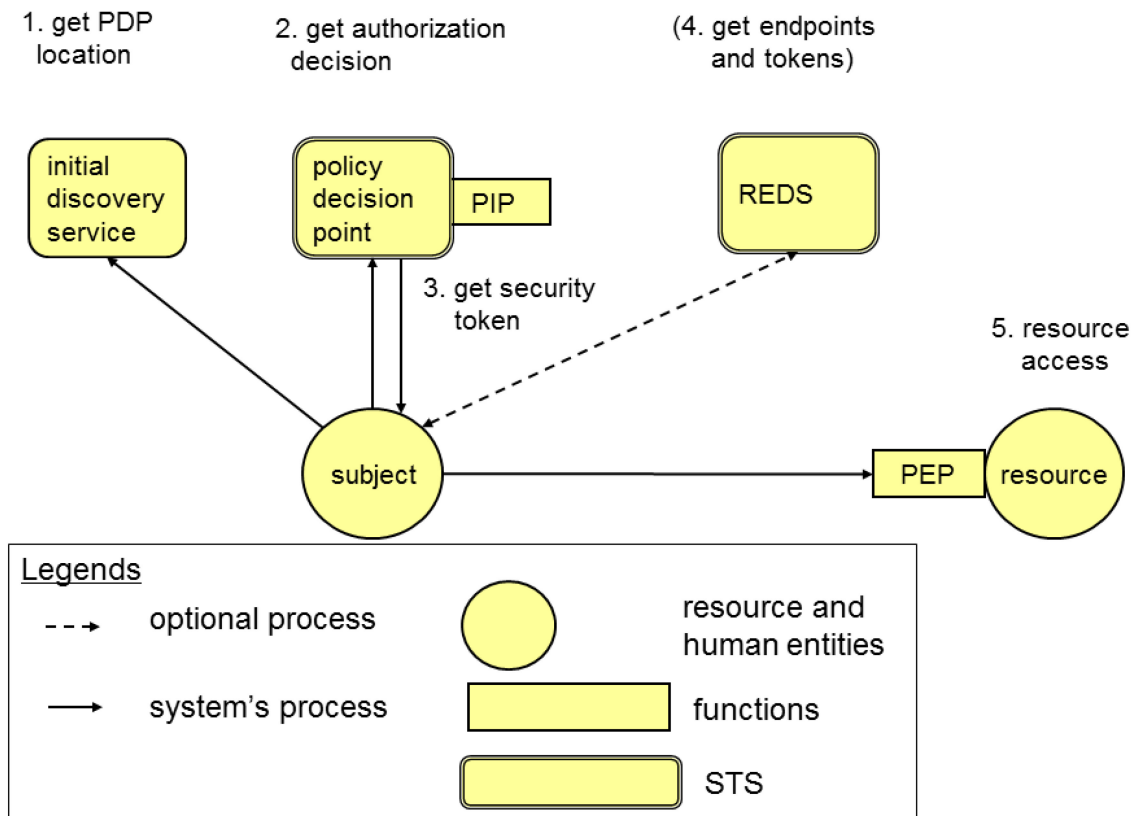


Figure 6 – Components interactions

Controlled access to resources may be performed in the following steps:

1. An authenticated subject may start from initial discovery service from which it finds out the location of the PDP and STS.
2. Then, the subject requests the access authorization to certain resources to PDP. Based on the policy or policy set, the PDP returns the access authorization to the subject.
3. The authorization decision is translated into a security token at the STS. The subject will get the security token.
4. Unless the resource location is known from the initial discovery, the subject obtains the resource endpoint information. At that time, the subject may also obtain a new token to access the resources.
5. The resource access may be performed in two ways:
  - (a) Using the security token, the subject accesses to individual resources.
  - (b) In some cases, it is desired that the subject to access the resources through an aggregation service instead of querying each resources. It is the case that the subject does not want the resources to know he is accessing.

Following figure shows the case where PEP plays the key role.

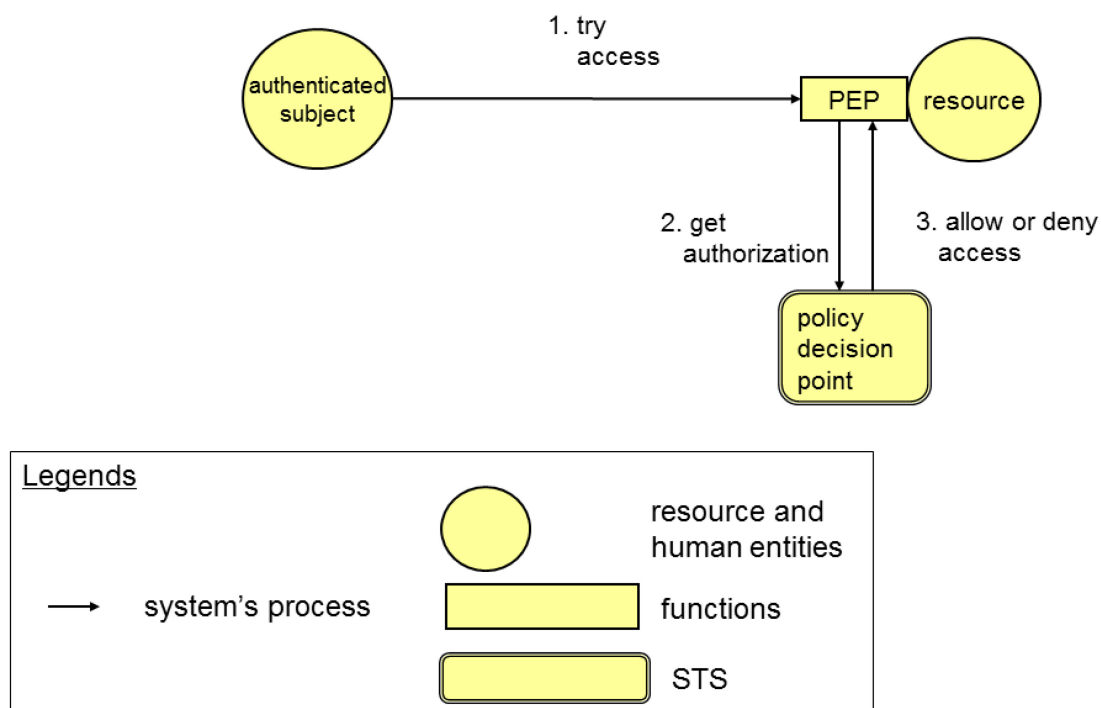


Figure 7 – Components interactions

Controlled access to resources may be performed in the following steps:

1. An authenticated subject may try to access resource. However the PDP blocks the access.
2. Then, the PEP asks for authorization to STS.
3. The authorization decision is translated into a security token at the STS. The PEP get the security token and enforce the access decision.

## 7 Requirements

### 7.1 Threats and countermeasures

There are following threats with Security token between PEP and PDP:

1. Security token manufacture/modification  
Attacker may generate a bogus security token or modify the security token content.
2. Security token disclosure  
Disclosure of security token may make the AMS vulnerable to other types of attacks, because it may contain sensitive authorization and attribute information.
3. Security token repudiation by the PDP  
Security tokens may be repudiated by PDP if the proper mechanisms are not in place.
4. Security token redirect  
An attacker uses the access token to one PEP to obtain access to second PEP.
5. Security token reuse  
An attacker attempts to use the access token that has already been used with the intended PEP.
6. Authenticator manufacture  
An attacker may attempts to generate a valid authenticator in Security token and use it to impersonate a Subject.
7. Authenticator capture  
An attacker may use a session hijacking attack capture the authenticator in Security token.
8. Security token substitution  
A Subject may attempt to impersonate a more privileged Subject by subverting the communication channel between PDP and PEP.

To mitigate these threats, following countermeasures may be required:

- Security token may be sent over a protected session such as TLS/SSL, for threat 1, 2, 7 and 8.
- Security token may be digitally signed by PDP using a key that support authentication, for threat 1.
- Security token may be digitally signed by PDP using a key that support non-repudiation, for threat 3.
- Security token may include the identity of the PEP for whom it was generated, for threat 4.
- Security token may include a timestamp and have a short lifetime of validity, for threat 5.
- The authenticator in Security token may contain sufficient entropy that an attacker without direct access to PDP random number generator cannot guess the value of the authenticator, for threat 6.

## 7.2 Access to administrative information

Access to administrative components of access management system (AMS) shall be restricted to people who have legitimated privilege.

Access to administrative information may be operated from policy administration point (PAP). And attribute information of resources which is related to access control policy is stored in policy information point (PIP). Also the system administration may be conducted either from local or remote.

Therefore, the design of an AMS shall have its information access policy to define:

- Criteria for authorizing each administrative access to the information;
- Conditions and mechanisms to access the information;
- Conditions of use of the information;
- Which operations of access to information needs to be recorded, and with what details;
- The duration of the retention of the records;
- The duration and conditions of the AMS almighty system administrator account.

## 7.3 Compliance

### 7.3.1 Policies in access management

Compliance is to be considered based on the policies regarding to access management.

Access management policies shall address the following concerns:

- applying some access control model for authorization decision,
- requiring some level of assurance for the subject authentication as the basis for authorization,
- monitoring and record keeping authorization related events to keep accountability, and
- management of privacy sensitive information.

### 7.3.2 Policy on access control model

There are several access control models which should be adopted in distributed network environment. An enterprise organization may choose to adopt role based access control (RBAC) model, and some community may choose to adopt attribute based access control (ABAC) model to manage their resources.

NOTE: see Annex A about access control models.

First, the policy may be documented in natural language. Subsequently, the policy shall be translated in digital policy. Finally, it shall be confirmed that the digital policy is equivalent to the natural language policy. Acceptable evidence of conformity to these requirements should be included.

### 7.3.3 Policy from organizational considerations

Organization may have added some policies regarding to access management. For example:

- Organization may have a policy requiring some level of assurance for the subject authentication as the basis for authorization.
- Organization may have multiple levels of policy administration point (PAP) and policy information point (PIP) to deal with hierarchically managed resources.

**7.3.4 Legal and regulatory requirements**

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

- monitoring and recording access events, and
- management of privacy sensitive information.

## 8 Practice

### 8.1 Processes

#### 8.1.1 Authorization process

In case authorization is to be implemented as service, STS, the interaction can adopt standardized format. For example XACML specification [11] can be adopted.

#### 8.1.2 Privilege management process

The privilege management process implements the access control policy for the domain of applicability through the assignment of resource access privileges. For example; in the case of an RBAC model the privilege management process would provide the following functions:

- Assignment of individuals to a role and setting of role privileges
  - within IMS: assigning the appropriate role name attribute to individuals who will act in that role
  - within AMS: assigning the relevant resource access control privileges to the role name
- Within AMS: assigning the relevant resource access control privileges to the role name modifying privileges for a role:
  - within IMS: usually there will be no changes needed but 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.
  - within AMS: modifying the access control privileges assigned to the role.
- Change of assignment of individuals to a role
  - within IMS: changing the assignment of role name for an individual to the new role name
  - within AMS: usually there will be no changes needed

#### 8.1.3 Availability of privilege information

Privilege information to access protected resources can be registered into PIP, and made available from PDP at any time. AMS should support high-availability of such privilege information.

NOTE At the same time, confidentiality should be required to such administrative information.

It is best practice for many organisations to extend their access control policies by including:

- Data loss prevention, where any data object sent outside the resource owner's organisation retains its access control. When a subject requests access to the data object, which is now in his own organisation, the object either contains the ability to authorise access or it refers back to the data resource owner's access regime for a new authorization request as if the data were still in the owning organisation.
- Enterprise information protection, which controls the flow of data between systems and actors

within the resource owner's organisation, and also externally to other organisations based the owning organisation's policies. Such protection is to prevent specific data leaving the organisation in any event and particularly if there is an access control failure. This includes, for example, email filters.

## **Annex A**

### **Current access models (informative)**

#### **A.1 General**

This annex introduces access control models which may be adopted as the basis of access control policy.

#### **A.2 Models**

Primarily, logical access control solutions have been based on the identity of a subject requesting execution of an operation upon an object. This is the case of IBAC or RBAC models where access to an object has been individually granted to a locally identified subject, or has been granted to locally defined roles that the subject is a member of.

When a subject request access to an object 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 user requests based on arbitrary attributes of the user and arbitrary attributes of the object, and environment conditions that may be globally recognized and more relevant to the policies at hand.

##### **A.2.1 (DAC)**

Discretionary Access Control (DAC) model allows a subject to limit access to objects based on the identity of the subject / or groups to which it belong. Therefore a subject that has been granted access to information can do one or more of the following:

- pass the information to other subjects or objects;
- grant its privileges to other subjects;
- change security attributes on subjects, objects, information systems, or system components;
- choose the security attributes to be associated with newly-created or revised objects; or
- change the rules governing access control. Mandatory access controls restrict this capability

##### **A.2.2 (MAC)**

Mandatory Access Control (MAC) model prevents access to objects based on a established policy that is uniformly enforced by an authority across all subjects and objects within the boundary of an information system.

On the contrary to DAC, in this model, a subject that has been granted access to information cannot change privileges and is constrained from doing any of the following:

- passing the information to unauthorized subjects or objects;
- granting its privileges to other subjects;
- changing one or more security attributes on subjects, objects, the information system, or system components;
- choosing the security attributes to be associated with newly-created or modified objects;
- changing the rules governing access control. Organization-defined subjects may explicitly be granted organization-defined privileges (i.e., they are trusted subjects) such that they are not limited by some or all of the above constraints



### A.2.3RBAC

This model employs pre-defined roles that carry a specific set of privileges associated with them and to which subjects are assigned. Thus, the access is implicitly predetermined by the subject assigning the roles to each subject and explicitly by the subject owner of the object when determining the privilege associated with each role.

When the subject made a request the access control system evaluates the role assigned to the subject and the set of operations this role is authorized to perform on the object before rendering and enforcing an access decision.

Three primary rules are defined for this model [8]:

1. Role assignment:

A subject can execute a transaction only if the subject has selected or been assigned a role.

2. Role authorization:

A subject's active role shall be authorized for the subject. With rule 1 above, this rule ensures that subjects can take on only roles for which they are authorized.

3. Transaction authorization:

A subject can execute a transaction (business action that involves access to resources) only if the transaction is authorized for the subject's active role. With rules 1 and 2, this rule ensures that subjects can execute only transactions for which they are authorized.

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

The benefit of introducing roles is that it becomes not necessary to assign privilege for each subject, and becomes efficient; ( i.e roles can be updated without updating the privileges for every user on an individual basis); but RBAC does not easily support multi-factor decisions (for example, decisions dependent on physical location, and specialized training. Also as RBAC role assignments tend to be based upon more static organizational positions limiting RBAC architectures where dynamic access control decisions are required.

### A.2.4 IBAC.

GB 56 describing IBAC and explain why IBAC is not addressed in detail by this standard.

Identity Based Access Control (IBAC) model is based on the identity of the subject and employs mechanisms such as access control lists (ACLs) to capture the identities of those subjects allowed to access the object. If a subject presents a credential that matches the one held in the ACL, the subject is given access to the object.

In the IBAC model, the authorization decisions are made prior to any specific access request and result in the subject being added to the ACL.

### A.2.5ABAC

Attribute Based Access Control (ABAC) It is a logical access control model where authorization for a subject to access an object is granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions relevant to the request, and a set of policies that are specified in terms of those attributes and conditions. It is bound to identity attribute authentication process [9][10]. The basic idea of

ABAC is not to define permissions directly between subjects and objects, but instead to use their attributes as the basis for authorization decision. ABAC relies upon the assignment of attributes to subjects and objects, and the development of policy that contains the access rules. Each object within the system must be assigned specific object attributes that characterize the object. This avoids the need for capabilities (operation/object pairs) to be directly assigned to subject requesters or to their roles or groups before the request is made.

Permissions consist of the combination of a so-called object descriptor, which consists of a set of attributes and environment conditions. Subjects and objects are both represented by a set of attributes and related attribute values.

Under ABAC each subject that uses the system must be assigned specific attributes. Access decisions can change between requests by simply changing attribute values, without the need to change the subject/object relationships defining underlying rule sets. This way ABAC avoids the need for explicit authorizations to be directly assigned to individual subjects prior to a request to perform an operation on the object minimizing the management of access control lists or roles and groups in large organizations.

Authorization decision is conducted based on comparison of subject descriptor and permission.. ABAC systems are capable of enforcing both Discretionary Access Control (DAC) and Mandatory Access Control (MAC) concepts. IBAC /ACLs and RBAC are in some ways special cases of ABAC in terms of the attributes used. ACLs work on the attribute of "identity". RBAC works on the attribute of "role". The key difference with ABAC is the concept of policies that express a complex Boolean rule set that can evaluate many different attributes.

The access control is done through Policy, rules, and relationships that determine how resources or objects are to be protected under which environment conditions. These policies must be enforced through the different components of the access control system.

In an organization it should be necessary for an ABAC system to establish management capabilities to ensure consistent sharing and use of policies and attributes and the controlled distribution and employment of access control mechanisms throughout the organization.

## Bibliography

- [1] Recommendation ITU-T X.812 | ISO/IEC 10181-3, Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework 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>
- [2] ITU-T X.1252 : Baseline identity management terms and definitions (04/10)
- [3] SC 27 Standing Document 6 (SD 6) Glossary of IT security terminology
- [4] Review Developing Definitions ISO/IEC JTC 1/SC 27 N5603
- [5] Dieter Gollmann, "COMPUTER SECURITY", WILEY (1999)
- [6] The OAuth Security Model for Delegated Authorization,  
<http://tools.ietf.org/html/draft-barnes-oauth-model-01>
- [7] Torsten Priebe, Wolfgang Dobmeier, Christian Schläger, Nora Kamprath, 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)
- [8] National Institute of standards and Technology (NIST), "Role Based Access Control and Role Based Security";  
<http://csrc.nist.gov/groups/SNS/rbac/>.
- [9] 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>
- [10] National Institute of standards and Technology (NIST), SP800-162  
Guide to Attribute Based Access Control (ABAC) Definition and Considerations  
January 2014
- [11] OASIS Standard, "eXtensible Access Control Markup Language (XACML) Version 1.0" (February 2003)  
<https://www.oasis-open.org/committees/download.php/2406/oasis-xacml-1.0.pdf>