MACE-paccman-glossary

MACE-paccman Glossary

Comments and feedback are welcome and encouraged. Authenticated users may post comments, or you may send e-mail to <mace-paccman-contact AT internet2 DOT edu>. Instructions for obtaining editing access can be found at http://middleware.internet2.edu/docs/internet2-spaces-instructions-200703.html.

General Privilege Management Concepts

The language of Privilege Management is rich and often interchangeable - one "may", one "can", one "is authorized", "has a privilege", "is allowed", "has access", etc. The definitions below are meant to clarify general concepts.

CONCEPT	**DEFINITION**
Access Control	The act of allowing access to facilities, programs, resources or services to authorized persons (or other valid subjects), and denying unauthorized access. Access Control requires that rules or policies be in place, that privileges be defined, so that they can be enforced.
Access Management	That part of Identity Management comprising the processes and tools used to associate privileges with subjects in accord with the wishes of Authorities.
Action	Function, Action, and Verb are close synonyms within the privilege and access control domain. They are used interchangeably in the tuple data model where a privilege is defined by Subject + Function + Scope. See "Function" for examples.
Assertion	A declaration or claim. Typically, when the term *assertion* is used in conjection with privilege management it tends to connote a claim formatted with a particular formal syntax. For example the document or speaker may be talking about a claim formatted as an assertion conformant to the SAML specification.
Attribute	A distinct characteristic of a subject. An object's *attributes* are said to describe it. Attributes are often represented as pairs of "attribute name" and "attribute value(s)", e.g. "foo" has the value 'bar', "count" has the value 1, "gizmo" has the values "frob" and "2", etc. Often, these are referred to as "attribute value pairs". The term also refers to properties of objects or elements of assertions whether or not they represent subjects.
Authentication	The process of confirming the identity of a principal. Since computer identification cannot be absolute (e.g., passwords can be stolen), authentication relies on a related concept of *level of trust*, in which an institution relies on good identity management practice (so that the institution believes they have correctly identified an individual) and secure mechanisms for sharing identity. This is sometimes referred to as ***AuthN*** (authentication), in contrast to ***AuthZ*** (authorization).
Authority	1) A broad term than can cover most aspects of creating policies and rules governing who has rights and privileges for an organization. It includes the process or workflow used to attest or assign rights and privileges , the ability to control the dissemination of those rights, as well as an organization's responsibilities to enforce those rights. This is sometimes referred to as AuthZ (authorization), in contrast to AuthN (authentication. 2) It can also refer to a person or policy or rule that confers privileges to subjects, either directly by use of an access management system, or indirectly. 3) It can also be used more specifically in a singular authorization situation to say whether a principal has "authority" to take an action. In this sense, ***authority*** and ***privilege*** can be used interchangeably.
Authorization	The process of deciding if a subject (person, program, device, group, role,etc.) is allowed to have access to or take an action against a resource. Authorization relies on a trusted identity (*authentication*) and the ability to test the privileges held by the subject against the policies or rules governing that resource to determine if an action is permitted for a subject.
Claim	A declaration, or assertion, made by an entity. Hopefully the entity is a reliable third party. Examples of claims include names, affiliations, group membership, or capabilities.
Delegation	The process used, or task performed, by a grantor to assign privileges to other subjects within the limits of its authority. A subject with delegated privileges does not have to perform any type of impersonation in order to exercise the privileges.
Effective	Indirect, inherited. Opposite of immediate. An assignment is "effective" if it exists because of other assignments or rules. Some examples: - A privilege may be granted due to another granted privilege (e.g. if you are granted READ access to the Arts and Sciences school in the payroll system [immediate], then you also have READ access to the English department in that system [effective]). - A privilege may be granted via an assignment to a role, and the role or other role in a hierarchy is assigned the privilege. - A group membership might exist due to a group being a member of another group. An effective assignment generally cannot be directly unassigned.
Eligibility	A concept closely related to authorization in that it can use the same mechanisms of authentication, policies, rules, and role evaluation. The differences are semantic - one is "eligible for something" as opposed to "authorized to do something" - so each is appropriate to use to describe different use cases. For instance, "all students are eligible for an email account", vs "students in this class are authorized to download course materials". Eligibility is more akin to a "right", in legal terms, than a "privilege", but the technical differences in how they are accomplished in an online environment are generally negligible. The term has sometimes been used in circumstances in which subjects must take a specific step in order to receive an authorization.
Entitlement	Often used the same as Privilege, entitlement carries the feeling of something owed or of a right granted. We make limited use of the word here. An authority-related eduPerson attribute - eduPersonEntitlement - uses this term specifically as an attribute that conveys ownership of the named right or privilege, a token that can be used directly or in a rules evaluation in determining authorization. It's noteworthy that privileges with qualifications, limits, scope, attributes, conditions, or prerequisites aren't called entitlements. It seems to be used only for simple, non-parameterized expressions.
Entity	A collection of identifiers and attributes managed by an Identity Management System representing any real-world actor, such as a person, process, system, etc. This is very similar to one definition of Subject below, with the possible distinction that a Subject can represent groups and roles in addition to real-world actors.
Function	Function, Action, and Verb are close synonyms within the privilege and access control domain. They are used interchangeably in the tuple data model where a privilege is defined by Subject + Function + Scope. Examples: Subject + Function + Scope Joe + Can Access + Oxford English Dictionary Online Jane + Can Download + MS Office 2007 Jim + Can Create Functions + In category HR Juan + Can Spend or Commit + On Cost Object Q678543 Attila + Can Approve + On Cost Object Q678543 James + is a Principal Investigator + in School of Science

Grantor	A principal authorized to delegate some portion of its own authority and that has exercised that privilege.
Group	A collection of subjects, which can include subjects representing other groups.
Identity Management	Identity management is often used broadly to encompass not only activities to correctly identify and maintain attributes about subjects, but also the manifestations of that knowledge through infrastructure supplying access and security services - single sign-on, account/service provisioning, authentication and authorization. Here we focus on a narrower definition, principally the need to identify persons as one individual despite multiple associations and roles, proper identification of other entities and agents (organizations, applications, groups, services, resources, etc), and the management of that information over time and across the enterprise. Sometimes the term "Identity and Access Management" is used to be explicitly inclusive of access management within this practice. When the number of subjects that need to be given identifiers for use in Identity and Access Management systems is very large, the ability to name things may itself be controlled by access management. This requires an underlying identity management practice for namespaces.
Immediate	Direct. Opposite of effective. An assignment is "immediate" if there is an explicit assignment from the subject to the resource (and perhaps including qualifiers). An immediate assignment does not depend on other assignments to exist. An immediate assignment can be unassigned directly.
Namespace	A domain in which an identifier is unique in representing a single object.
Permission	A closely related term to *access control*, a permission is the control specifically related to a resource and an action - a subject must have permission to take that action. Note - paccman is deprecating this term and suggest that privilege be used consistently.
Policy	A policy is used to describe general access control requirements. There are many existing proprietary and application-specific languages for creating policies, but XACML has several points in its favor: it's standard, it's generic, it's distributed, it's powerful. A XACML policy has at least one, and possibly more rules. A policy may be written to have a single effect, meaning that each policy has a single rule that either permits or denies access. This style of policy writing results in many individual policies, but each policy is atomic and uncomplicated. An alternative is to have fewer policies, each with multiple rules within. A XACML policy contains one or more RULEs, which may contain a TARGET and a CONDITION. A TARGET consists of a SUBJECT, an ACTION, a RESOURCE, and optionally an ENVIRONMENT. RULEs can be composited.
Principal	A subject whose identity can be authenticated.
Privileges	Etymologically speaking, a privilege is a "personal law", making privileges a set of personal rights. Privileges amount to the sum of what a subject may do, as granted to them or inherited. In the context of a Privilege management system, Privilege is used to describe the combination of a subject or group, their current allowable actions, and any qualifications or scoping limitations that shall be imposed on those allowable actions.
Provisioning	The process of managing attributes and accounts within the scope of a defined business process or interaction. Provisioning an account or service may involve the creation, modification, deletion, suspension, or restoration of a defined set of accounts or attributes.
Qualifier	In the context privilege manage and access control, Qualifier and Scope are close synonyms, often used interchangeably. A qualifier, or scope, mediates (or restricts) the applicability of a Verb or Function. For example, within a financial system, we may have a verb or function called "can spend" and the scope will specify the cost objects or account numbers to which this verb can legitimately be applied. In another example, library systems may have a verb or function named "can access" and the scope or qualifier may specify a particular database or resource such as "Oxford English Dictionary Online". A slightly self-referential example, occurs when a privilege management system has a verb or function called "can create Functions" and the scope or qualifier might be "in the category of HR".
Resource	Resource and Target are often used synonymously when discussing privilege management colloquially. As with Target, the term is context dependent when used informally. At times, Resource is another close synonym of Qualifier and Scope. However, people tend to use this term when speaking about more "tangible" scopes such as "Oxford English Dictionary Online" or "Ethnic Newswatch". There are other qualifiers and scopes that people don't typically think of as a resource, for example "the category of HR", "NULL", and depending how closely you work with the financial system, cost objects and account numbers. See *Qualifier*
Responsibility	A responsibility is an action that a principal assigned to a role is expected to perform. Similar to a privilege except that the principal not only has the ability to perform the action, but is expected to perform the action. In the Kuali Enterprise Workflow system, an example of a responsibility is a step in a workflow where a subject needs to respond to a workflow action. Note that more than one person could have the same responsibility.
Role	Colloquially we use "roles" very broadly. In higher-ed some of the common roles are Dean, Department Chair, Principal Investigator, Faculty, Post-Doc, ... In the context of privilege management and access control, a Role centric model presumes that given the precise position or title of a person within an organization, the privilege management system can draw conclusions about what privileges should be granted to the person. Roles may also be thought of as meta-privileges which are used a short hand for granting a wide range of finer grained privileges to someone that "has the role." It is also noted that a Role may imply one or more Roles. For example a Department Chair will also be presumed to be a Faculty member. Modeling roles can be problematic. In some systems it may be appropriate to define a role of "Dean" while in other systems it may be important to create "Dean of Biology" , "Dean of School of Science", ... It is important to understand how the modeling will impact the finer grained privileges that will be conveyed to the individuals associated with specific roles, for a particular implementation. 10/5/09:~~A collection of *privileges* usually relating to a task, responsibility, or qualification associated with an enterprise. Collections may be comprised of any combination of implicitly and/or explicitly defined privileges. Roles within an enterprise typically have overlapping privileges. Role based access control systems often include features to establish role hierarchies, where a given role can include all of the privileges of another role. Roles can generally be associated with subjects (person, program, device, group, etc.)~~
Rule	A prescribed evaluation of data which is used to confer a privilege, to a subject or a collection of subjects.
Scope	See *Qualifier*
Subject	An entity whose identifiers and attributes are managed by an Identity and Access Management practice.
Target	The term "Target" should be deprecated. Target is a matter of perspective and context. When people are discussing privilege and access control informally, a target is often the same as a Resource. However, at other times, the focus is on the Subject. In yet different contexts the target is actually the set of people that have a specific verb and scope applied to them, as in the "target group".
Verb	See *Function*
Workflow	Workflow is concerned with the automation of procedures where documents, information or tasks are passed between participants according to a defined set of rules to achieve, or contribute to the authority assigning privileges.

Comparative Taxonomy

During the June 2009 EDUCAUSE and Internet2 Advanced CAMP, participants suggested that MACE-paccman create a comparitive taxonomy that would explore the differences, as well the commonality, between several systems that have importance or relevance to the CAMP attendees and the MACE-paccman community. The subsequent work is taking place here.

References and acknowledgements

This glossary has been heavily influenced by the Signet glossary.

Other valued references include:

- Enterprise Authentication Roadmap
- Identity Gang's Lexicon
- Identipedia Terms
- SAML2 Glossary
- NIST Special Publication 800-63
- Internet Security Glossary
- Wikipedia
- eduPerson
- Practices in Directory Groups
- Privilege Management Recipe
- The Architecture Journal, vol 16
- Kuali Identity Management glossary
- Grouper glossary
- SPML Core
- NIST RBAC model

See Also: More generalized glossary work at https://spaces.at.internet2.edu/display/macepaccman/Another+Glossary+Page