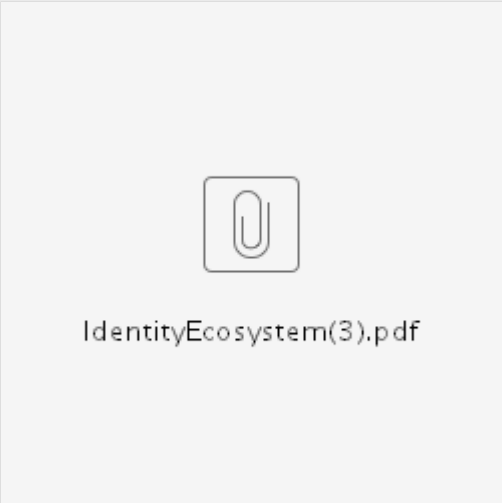
IAM Functional Model and IAM Glossary

IAM Functional Model: Diagram, Table and Glossary

Identity Ecosystem Diagram



Functional Service Model with Sub-services and API

. -Note: Items in this color are minimum viable IAM system requirements.

Items in this black are subsequent release requirements

TIER Functional Service Model	Subservice	Minimum Viable IAM Required Capabilities
Repository Components (limited to Person for now)	Registry	New SOR Person, Inbound to Repository
	Group	
	ODS/MDM	
	Rule	
Account & Credential Management Service		Create Credential
		Expire Credential
		Change Credential
Account Linking Service		
Registration and Enrollment Service from SOR	Search/Match Entity	Search Match Person (Stub)
	Resolve Entity	
	Split Entity	
	Merge Entity	
Group Management Service	Create Group	Create Group
	Add Member	Add Member
	Remove Member	Remove Member
	Is Member Of	Is Member Of
	Show me Groups for person	Show Me Groups for Person
	Show me all members of Group	Show Me All Members of Group
Privilege Management Service	Create Privilege	Create Privilege

	Add Member	Add Member
	Remove Member	Remove Member
	Show me Privileges for Person	Show me Privileges for Person
	Show me all member with Privilege	Show me all member with Privilege
Provisioning /De-Provisioning Consumers Service	Person Entity	
	Guest Entity	
	Group member	
	Privilege	
Provisioning Connectors	LDAP	Manage LDAP Entry
	ORACLE	
	Kerberos	Manage Kerberos Principal
	Active Directory	
Identity Proofing Service	Person Entity	
Rules Engine Service	Filtering	
	Routing	
	Integration	
	Provisioning/De-Provisioing	
	LifeCycle	
Audit - Monitoring Operations Service	Transaction History (Human Readable)	Send basic logs to a log aggregation service
	Point In Time Logs	
	Manual History Records (comments)	
	Operational Monitoring	
	Usage Monitoring	
Administrative Configuration Service	User Interface (UI)	
	Institution Terminology (Translations)	
Reporting / Information Analytics Service	Notifications	
	Authn and Authz Analytics	
	Authn and Authz Audit / Compliance	
Authentication (Authn)		Authenticate user
Authorization (Authz)		Deliver user attributes/groups to application

The term **Entity Registry (Person Registry)** is explained well in this document Functional Model (Identity Registry)

TIER IAM Glossary of Terms:

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. A comprehensive set of tools and processes for assign and revoke access to resource to digital identities.
Access Rights	The full set of resource permissions or entitlements that a Subject or group possesses.

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.
Assurance	The degree of confidence in the vetting process used to establish the identity of the Subject to whom the Credential was issued, and the degree of confidence that the individual who uses the Credential is the Subject to whom the Credential was issued. The US government uses the four assurance levels defined in OMB0404 to express the degree of confidence: Level 1: Little or no confidence in the asserted identity's validity Level 2: Some confidence in the asserted identity's validity Level 3: High confidence in the asserted identity's validity Level 4: Very high confidence in the asserted identity's validity InCommon currently defines two assurance levels: Bronze: Little or no confidence in the asserted identity's validity (comparable to US government Level 1 assurance) Silver: Some confidence in the asserted identity's validity (comparable to US government Level 2 assurance)
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.
Attribute Release	A Service Provider often requires identity attributes for the Subject for access control, personalization, and other purposes. These attributes are included in the assertion issued by the Identity Provider at the time the Subject attempts to access the service.
Attribute Release Policy	Rules that an Identity Provider follows when deciding whether or not to release an attribute and its value(s). Attribute release policies can be customized for a given Service Provider or Service Provider category.
Authentication	The security measure by which a Subject transmits a Credential and validates his or her association with a Digital Identity. An example of authentication is submitting a username and password that is verified as correct or incorrect. Alternative definition: 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 for determining a specific Subject's eligibility to gain access to a resource or service, a right or permission granted to access a system or information. 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. AKA AuthZ
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.

Chain of Authority	The chain of command within an organization that confers the power to order subordinates to perform a task within their job description. The chain of authority within a business establishes who is in charge of giving who orders, and it contributes to the efficient attainment of the company's objectives when properly used.
Change Management	The controlled identification and implementation of required changes within a system.
Cloud Resources	"Cloud" often refers to "Cloud Computing" but the simplest definition of "Cloud" is that it is the Internet, the infrastructure that allows vendors to supply computing, platform, software and services to their customers on a payasyou go utility model. Cloud computing uses the Internet to share resources, software and information ondemand, much like a public utility allows many people to share the same water or power system, paying only for what they need.
Credential	A unique identifier and associated authentication material used by the Subject in the authentication process.
Credential Lifecycle Management	The Credential lifecycle consists of an initialization phase, where the credential is issued to the Subject, an operational phase, where the Subject uses the Credential to access resources, and the termination phase, where the Credential expires and may be renewed or revoked.
Credential Syncing	The propagation of the same credential to multiple repositories.
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.
eduPerson	An LDAP object class authored and promoted by the EDUCAUSE/Internet2 eduPerson Task Force to facilitate the development of interinstitutional applications. The eduPerson object class focuses on the attributes of individuals. InCommon Identity Providers are expected to populate a number of the eduPerson attributes. Current documentation on the eduPerson object class is available at http://www.educause.edu/eduperson/ . InCommon IdP attribute population requirements are provided at https://spaces.at.internet2.edu/display/InCFederation/Supported+Attribute+Summary .
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.
External Collaboration	Working with personnel at one or more other institutions on a given project or program. The collaboration creates a need for shared access to resources that may be hard to achieve due to the lack of a common Identity Provider.
Federation	A federation is an association of organizations that come together to exchange information as appropriate about their users and resources in order to enable collaborations and transactions. A federation provides a common framework for trusted shared management of access to online resources. Through the federation, Identity Providers can give their users single signon convenience and privacy protection, while online Service Providers control access to their protected resources.
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	An identity data element that represents a collection of objects. The chief characteristic of a group is its membership, i.e. the set of objects that belong to the group.
Group Management	Group management consists of the processes in place to maintain group membership information. Group membership can be maintained dynamically, based on information from systems of record, or manually.
Guideline	Recommended practice that allows some discretion or leeway in its interpretation, implementation, or use.
Identifier	An Identity Data element or attribute that uniquely identifies or resolves to an individual Subject. In an enterprise setting, there are likely to be needs for several types of identifiers. Examples of identifiers include email address, login ID, person registry ID, administrative system ID (employee ID, student ID), driver's license number, passport number, Social Security Number, card ID, library ID. Identifier characteristics of particular interest: Persistent identifier: An identifier that is permanently assigned to a Subject. By its nature, a persistent identifier is nonreassignable. Reassignable identifier: An identifier value that can be assigned to a different Subject. At a given point in time, only one Subject will possess the identifier. Over time, multiple Subjects may utilize/possess the identifier.
Identity or Digital Identity	The electronic representation of a Subject, which participates in electronic transactions on behalf of the Subject.
Identity Data	The set of information that pertains to a Subject. This information is used to uniquely identify the Subject and communicate with the Subject. It may also include group memberships, roles and eligibility. Also referred to as Identity Attributes .

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.
Identity Management Architecture	A coherent set of standards, policies, certifications and management aimed at providing a context for implementing a digital identity infrastructure that meets the current goals and objectives of the business and is capable of evolving to meet future goals and objectives.
Identity Management Roadmap	A plan that matches shortterm and longterm goals with specific identity management technology solutions to help meet those goals. It is a plan that applies to a new product or process, or to an emerging technology. Developing a roadmap has three major uses.It helps reach a consensus about a set of identity management needs and the technologies required to satisfy those needs it provides a mechanism to help forecast identity management developments and it provides a framework to help plan and coordinate identity management developments.
Identity Management System (IdMS)	A system that fulfills enterprise identity and access management needs. It maintains a database of Subjects with information gathered from Systems of Record and a store to house Subject Credentials and is responsible for properly merging identity data, determining group memberships, provisioning resources, and managing Subject Digital Identities and Credentials.
Identity Matching	The process of comparing information from different Systems of Record and deciding when records from different sources apply to the same or different individuals. A common strategy is to compile a list of attributes and use them as a basis for comparison. In general, the effectiveness of identity matching is controlled by the consistency, quality and amount of data used in the comparison.
Identity Provider (IdP)	The originating location for a user. An IdP is a campus or other organization that manages and operates an identity management system and offers information about members of its community to other federation participants.
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.
InCommon	The InCommon Federation is the U.S. education and research identity federation.
Integration Technologies	Technology used to bring together or incorporate identity data from multiple sources into a merged record.
IT strategy	The discipline that defines how IT will be used to help businesses win in their chosen business context.
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	The set of basic principles and associated guidelines, formulated and enforced by the governing body of an organization, to direct and limit its actions in pursuit of longterm goals.
Policy (2)	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.
Program	A group of related projects, subprograms, and program activities that are managed in a coordinated way to obtain benefits not available from managing them individually.
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 in order to affect the subjects access rights. The mapping of digital identities to accounts, credentials and access rights.
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".
Research and Scholarship Entity Category	The Research & Scholarship (R&S) Category is a designation that can be awarded to a Service Provider in the InCommon Federation. The designation indicates the service provider supports research and scholarly activities. Virtual organizations and campusbased collaboration services are examples of service providers that could be categorized as Research and Scholarship.
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.
Risk Level	A Risk is the amount of harm that can be expected to occur during a given time period due to a specific harm event (e.g., an accident). Statistically, the level of risk can be calculated as the product of the probability that harm occurs (e.g., that an accident happens) multiplied by the severity of that harm (i.e., the average amount of harm or more conservatively the maximum credible amount of harm). In practice, the amount of risk is usually categorized into a small number of levels because neither the probability nor harm severity can typically be estimated with accuracy and precision.
Role (Security 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. An identity data element that represents a collection of permissions or entitlements.

	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.
	-
Role Based Access Controll (RBAC)	In computer systems security, role based access control is an approach to restricting system access to authorized users. RBAC is sometimes referred to as role based security. Within an organization, roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles. Members or staff (or other system users) are assigned particular roles, and through those role assignments acquire the computer permissions to perform particular computersystem functions. Since users are not assigned permissions directly, but only acquire them through their role (or roles), management of individual user rights becomes a matter of simply assigning appropriate roles to the user's account this simplifies common operations, such as adding a user, or changing a user's department.
Rule	A prescribed evaluation of data which is used to confer a privilege, to a subject or a collection of subjects.
Service Provider (SP)	A campus or other organization that makes online resources available to users based in part on information about them that it receives from an Identity Provider.
Single Sign On	The use of a centralized authentication service which enables a Subject to access multiple browserbased electronic resources with a single Credential and requiring only one authentication event.
Scope	See Qualifier
Stewardship	the responsible overseeing and protection of something considered worth caring for and preserving.
Subject	A realworld entity. The term is usually taken to mean an individual human being. However, a broader definition also includes organizations, companies and even individual electronic devices. Any entity whose identifiers and attributes are managed by an Identity and Access Management practice.
System of Record	A system that is authoritative for one or more Subject identity data elements. SOR
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.