Glossary

Access Management: A comprehensive set of tools and processes for assign and revoke access to resources to digital identities.

Access Rights: The full set of resource permissions or entitlements that a Subject or group possesses.

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 OMB-04-04 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 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.

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 an online system.

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 pay-as-you go utility model. Cloud computing uses the Internet to share resources, software and information on-demand, 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.

eduPerson: An LDAP object class authored and promoted by the EDUCAUSE/Internet2 eduPerson Task Force to facilitate the development of inter-institutional 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.internet2.edu/display/InCFederation/Supported+Attribute+Summary.

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 on-line resources. Through the federation, Identity Providers can give their users single sign-on convenience and privacy protection, while online Service Providers control access to their protected resources.

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 non-reassignable.

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: A comprehensive set of tools and processes for creating and managing digital identities for all entities that are affiliated in some capacity with the institution and that need access to IT resources.

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 short-term and long-term 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.

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.

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 long-term goals.

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 mapping of digital identities to accounts, credentials and access rights.

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 campus-based collaboration services are examples of service providers that could be categorized as Research and Scholarship.

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: An identity data element that represents a collection of permissions or entitlements.

Role-Based Access Control (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 computer-system 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.

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 browser-based electronic resources with a single Credential and requiring only one authentication event.

Stewardship: the responsible overseeing and protection of something considered worth caring for and preserving.

Subject: A real-world 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.

System of Record: A system that is authoritative for one or more Subject identity data elements.

Sources:

Brendan Bellina. 2002. Metadirectory Practices for Enterprise Directories in Higher Education.
InCommon. 2013. Identity Assurance Assessment Framework. http://www.incommon.org/docs/assurance/IAAF.pdf
InCommon. 2013. Identity Assurance Profiles, Bronze and Silver. http://www.incommon.org/docs/assurance/IAP.pdf
Internet2 Middleware Initiative. 2000. Identifiers, Authentication, and Directories: Best Practices for Higher Education.
Internet2 Middleware Initiative. 2002. Practices in Directory Groups.
University of Michigan Information Technology Services. 2007. MCommunity Design Requirements Documents. http://www.itcs.umich.edu/mcommunity/
Wikipedia. https://en.wikipedia.org/wiki/Role-based_access_control
InCommon Glossary. http://www.incommon.org/glossary.html