Glossary

Account Linking: A process by which a person links multiple modes of authentication (i.e., authentication through multiple Identity Providers) to a single logical identity in an application or system (e.g., a single User ID that refers to a single person). "Account Linkage" is defined in the SAML 2.0 glossary as: "A method of relating accounts at two different providers that represent the same principal so that the providers can communicate about the principal. Account linkage can be established through the sharing of attributes or through identity federation."

Assertions: An assertion is a unit of information related to security. Assertions are made up of statements that can be used to make decisions about authorization (access to resources). The definition of "Assertion" in the SAML 2.0 glossary is: "A piece of data produced by a SAML authority regarding either an act of authentication performed on a subject, attribute information about the subject, or authorization data applying to the subject with respect to a specified resource."

Authentication (AuthN): The process of proving one's identity to an application or system. Often this involves presentation of "credentials" – e.g., a User ID and a password. More broadly, a person is authenticated based on "factors of identification" that may include something the person knows, something she has, or something she is. Examples of each of these: a person might *know* a password; might *have* an identity card; and might *be* identifiable based on biometrics such as a fingerprint or retinal pattern. When a user is authenticated, her identity is considered to be known to some level of certainty or assurance. The definition of "Authentication" in the SAML 2.0 glossary is: "To confirm a system entity's asserted principal identity with a specified, or understood, level of confidence."

Authorization (AuthZ): The grant or specification of access rights to resources within an application or system. For example, a doctor may be *authorized* to view her patients' medical records. The definition of "Authorization" in the SAML 2.0 glossary is: "The process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. Usually, authorization is in the context of authentication. Once a subject is authenticated, it may be authorized to perform different types of access."

Collaborative Organization: (cf. *Virtual Organization*)

Credentials: Evidence presented in the course of an Authentication process intended to prove identity. A familiar form of credentials is a User ID and the Password associated with that User ID. "Credentials" is defined in the SAML 2.0 glossary as: "Data that is transferred to establish a claimed principal identity."

Digital Identity:

Discovery:

Enterprise Identity:

EntityID:

Exposure:

Federated Identity: A mode of establishing identity that is agreed-upon by multiple identity and/or service providers. "Federated Identity" is defined in the SAML 2.0 glossary as: "A principal's identity is said to be federated between a set of Providers when there is an agreement between the providers on a set of identifiers and/or attributes to use to refer to the Principal"

Federation of Trust: (cf. *Trust Federation*)

Gateway: (cf. *Social-to-SAML gateway*)

InCommon Federation: The InCommon Federation defines itself as "a formal federation of organizations focused on creating a common framework for collaborative trust in support of research and education."

Identity Proofing: Assuring that digital identities and associated credentials belong to the real-world individuals they purport to represent. Cf., for example, *What Is Online Identity Proofing and How Does It Work* (eWeek, 2 Aug 2007)

Identity Provider (IdP): A type of application or system that is trusted to authenticate users. "Identity Provider" is defined in the SAML 2.0 glossary as: "A kind of service provider that creates, maintains, and manages identity information for principals and provides principal authentication to other service providers within a federation, such as with web browser profiles."

Level of Assurance (LoA):

LoA: (cf. *Level of Assurance*)

OAuth:

OpenID:

out-of-band:

PII: (see *Personally identifiable information*)

Personally identifiable information: Information that can be used to identify a particular person. Examples of personally identifiable information (sometimes referred to as "PII") include: full name, national identification number (e.g., passport number or social security number), driver's license number, credit card number(s), birth date, birthplace, etc.

Relying Party: An application or system that relies on another application or system to fulfill some of its functionality (e.g., to authenticate a user). "Relying Party" is defined in the SAML 2.0 glossary as: "A system entity that decides to take an action based on information from another system entity. For example, a SAML relying party depends on receiving assertions from an asserting party (a SAML authority) about a subject."

Risk:

SAML / **SAML2**: SAML is an OASIS standard that defines how security-related statements (assertions) are expressed; cf. SAML 2.0 on the Oasis Standards page; and the OASIS Security Services (SAML) Technical Committee page. As defined in the SAML 2.0 glossary , "Security Assertion Markup Language (SAML)" is: "The set of specifications describing security assertions that are encoded in XML, profiles for attaching the assertions to various protocols and frameworks, the request/response protocol used to obtain the assertions, and bindings of this protocol to various transfer protocols (for example, SOAP and HTTP)."

SAML2 metadata files:

Service Provider (SP): An application or system that delivers functionality (services) to people or other applications / systems. As defined in the SAML 2.0 glossary , a "Service Provider" is:"A role donned by a system entity where the system entity provides services to principals or other system entities."

Single SignOn (SSO):

Social Identity:

Social-to-SAML Gateway:

Trust Federation: An organization (such as the InCommon Federation in which members trust each other to honestly and reliably authenticate users and present information about them ("assertions") to others in the federation.

Virtual Organization:

Web Single SignOn (SSO):