Terminology

[A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Y] [Z]

A

AAI

Acronym for "Authentication and Authorization Infrastructure".

(SAML) Assertion

A digital statement issued by an IdP, derived from the Digital Identity of an End User. Typically an Assertion is digitally signed and optionally encrypted.

Authentication

Process of identifying of a previously registered user.

Authorization

Process of granting or denying access to a resource for an authenticated user.

(Authorization) Attributes

User data (such as name, affiliation, study branch, etc.) needed for access control decisions. The attributes used by eduGAIN are defined in the eduGAIN Attribute Profile.

Attribute Authority

The AA is a component of the Identity Provider. It issues attributes on behalf of an organization.

Attribute Release Policy (ARP)

It defines which attributes are going to be released to a requesting resource (the attribute filter). It is a mechanism to implement privacy and data protection.

Attribute Resolver

A component of the Identity Provider. It retrieves attributes from various data sources (LDAP, Active Directory, ...) and performs the necessary transformations for SAML transport.

B

C

D

Digital Identity

A set of information that is attributable to an End User It is issued and managed by an IdP Operator on the basis of the identification of the End User.

Discovery Service

Technical term/synonym for WAYF.

E

End User

Typically, a human person who belongs to an organization, typically an employee or student, who uses Federated Authentication via its IdP. However, an End User can also be a legal person, a virtual artifact (e.g. a computer process, an application), a tangible object (e.g. a device) or a group of other entities (e.g. an organization) of an organization.

Entitlement

Entitlements form a specialized class of Authorization Attributes important enough to call out separately. They can be used to identify a user's eligibility to access a given resource such as an e-journal, see common-lib-terms.

EntityID

The EntityID is a unique identifier, identifying each Service Provider and Identity Provider.

F

Federated Authentication

An End User uses his Digital Identity to authenticate for accessing services offered by SP Operators within the same or a different organization.

Federated Identity Management

The management and use of identity information across security domains, e.g. between individual universities. It deals with issues such as interoperability, liability, security, privacy and trust.

Federation

A federation is a collection of organizations that agree to interoperate under a certain rule set.

Federation Member

A Federation Member is an organization (such as a university, library, etc.) that runs one Identity Provider and any number of AAI-enabled Resources. Federation Members usually have to agree on a common set of policies and rules defined in a service/federation agreement.

Federation Operator

The organization managing the Federation, operating the central components and acting as a competence centre. SWITCH is for example the Federation Operator of the SWITCHaai Federation, the Swiss identity federation.

Federation Technology Profile

The technology profiles specify how to use which subsets of a specific federation technology in the context of a Federation.

G

H

Home Organization, Home Institution

A participating organization representing a user community, e.g. a university, library, university hospital etc. A Home Organization registers users and stores information about them. Furthermore, it is able to authenticate its users an it operates an IdP.

I

Identity Provider (IdP)

The system component that issues Assertions on behalf of End Users who use them to access the services of SPs.

IdP Operator

The organization operating an IdP. IdP Operator refers to the legal entity that signs contracts, is a Federation Participant and is responsible for the overall processes supporting the IdP.

Interfederation

Interfederation takes place if a user from one federation accesses a service which is registered in another federation. eduGAIN is the most known and largest academic Interfederation service to exchange trusted identity information across boundaries of (national) identity federations.

J

K

L

Lazy Session Establishment

This special form of session establishment allows access to a URL or resource prior to authentication. The point is that the application decides when a user has to authenticate. More information is available for example on the SWITCHaai Demo Resource.

M

Metadata

The Metadata contains technical details and descriptive information about the IdPs and SPs. For interoperability in a specific context, the Metadata format definition is part of a Federation Technology Profile.

N

O

P

Federation Participant

An organization that participates in an Identity Federation.

Q

R

Relying Party

In general, one or more Service Provider or Identity Provider that is sender or recipient of an Assertion. A relying party could be a single Service Provider or a group of Service Providers. The SPs and IdPs can be grouped into a relying party by including them into an *EntitiesDescriptor* element in the Metadata . Such a group of Service Providers can then for example be used tell an Identity Provider to use a special way to transmit the attributes to the components of this relying party.

Resource

Web application, web site, information system, etc. An AAI-enabled Resource requests attributes about users from an IdP and makes access decisions (authorization) based on these attributes.

S

SAML

SAML - the Security Assertion Markup Language - is an XML framework for exchanging authentication and authorization information. SAML is a standard of OASIS. The software Shibboleth is based on SAML.

Service Provider (SP)

The system component that evaluates the Assertion from an IdP and uses the information from the Assertion for controlling access to protected services. Synonym for an AAI-enabled Resource, although used in a more technical sense.

Shibboleth

The name an open source SAML implementation developed by Shibboleth Consortium. Shibboleth is based on SAML and allows the implementation of an AAI. eduGAIN makes use of SAML.

Simple SAML PHP

SimpleSAML PHP is another very popluar open source SAML software. It supports SAML and additional protocols that can be used for federated identity management.

SP Operator

The organization operating an SP. SP Operator refers to the legal entity that signs contracts, is a Federation Participant and is responsible for the overall processes supporting the SP.

Single Sign-On (SSO)

Single Sign-On enables the user to gain access to multiple Resources by authenticating only once.

T

U

V

W

WAYF (Where Are You From)

The WAYF service, also called Discovery Service, lets the user choose his Home Organization from a list and then redirects the user to this Home Organization's login page for authentication.

X

Y

Z

Many of the above entries were with permission copied from SWITCHaai Glossary.