Introduction to Identity Federations

August 2, 2017

Repository ID: TI.26.2
Authors: David Walker <https://orcid.org/0000-0003-2540-0644>
Ann West
Sponsor: Internet2
Superseded documents: (none)
Proposed future review date: December 1, 2019
Subject tags: policy, service

© 2017 Internet2

This work is licensed under a Creative Commons Attribution 4.0 International License.

Introduction to Identity Federations

An identity federation is a coalition of organizations, called *Participants*, that share information about their community members according to mutually agreed and usually legally binding policies, processes, and technologies. The purpose of this information sharing is to enable collaboration among community members and provide access to resources offered by the Participants for the federation's community members.

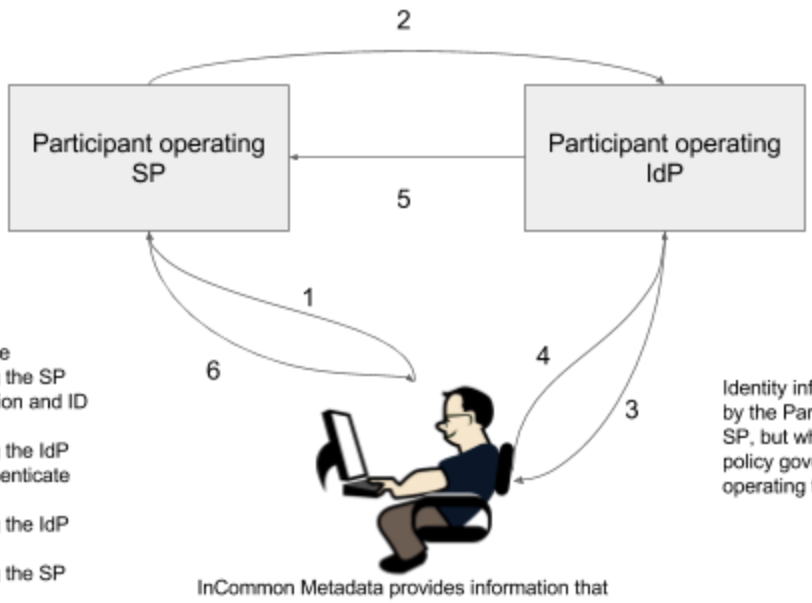
In a federated transaction, the organization that manages authentication for the individual is not the one hosting the service that the person wants to access. One organization authenticates the individual (in many cases a college or lab), and one offers services (such as a cloud provider, research collaboration, federal agency) and grants access.

The Security Assertion Markup Language (SAML) is the basis for the technology standards used by InCommon and other identity federations established to support research and education internationally. It defines a common format for the information about community members (called *Identity Assertions*) that is exchanged, as well as a protocol for accomplishing that exchange.

In the SAML protocol, Participants operate network services called *Identity Providers (IdP)* that respond to requests for *Identity Assertions* from *Service Providers (SP).* These SPs provide collaboration tools and access to resources of interest within the federation. Identity Assertions contain information about individuals for the purpose of personalizing the service and making authorization decisions; they include such elements as group memberships, roles, friendly names, contact information, and identifiers. eduPerson is a community standard that defines Identity Assertion content that is commonly used within research and education.

When an IdP receives a request for an Identity Assertion from an SP (as the result of its user's request for service), it assesses the request in light of its policies concerning the release of each requested element of information for that specific user to that specific SP. The IdP will release only information that is allowed by its policy. When the SP receives the resulting Identity Assertion, it will then make decisions about how to address the user's request for service. Those decisions might include tailoring the user's experience within the service, requesting more information like name or email address from the user, restricting the user's access to certain operations within the service, or completely denying access.

The following diagram illustrates the SAML protocol.



1 User requests service
2 Participant operating the SP requests authentication and ID info
3 Participant operating the IdP prompts user to authenticate
4 User authenticates
5 Participant operating the IdP returns identity info
6 Participant operating the SP provides service

Identity information is requested by the Participant operating the SP, but what is sent is subject to policy governing the Participant operating the IdP.

InCommon Metadata provides information that enables the Participants' IdP and SP to interoperate with trust.