WHAT ARE FEDERATIONS?

Fed erated identity, or the "federation" of identity, describes the technologies, standards and use-cases which serve to enable the portability of identity information across otherwise autonomous security domains. The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration.

Identity federation comes in many flavors, including "user-controlled" or "user-centric" scenarios, as well as enterprise controlled or B2B scenarios. Federation is enabled through the use of open industry standards and/or openly published, formal specifications, such that multiple parties can achieve interoperability for common use cases. The Security Assertion Markup Language (SAML), developed by Internet2, is the language that is typically used in communications within federations.

The Federation is accomplished via a trust mechanism that each member of the federation agrees to and joins. Historically, federations have been created to allow cross-domain single sign-on to web portals. Recently published standards now extend these technologies to web services, potentially opening the door to massive growth in the development and adoption of web services with a scalable and secure security infrastructure.

Use of identity federation standards can reduce cost by eliminating the need to scale one-off or proprietary solutions as it keeps user identities where they are authoritative, at the user's home domain. It can increase security and lower risk by enabling an organization to identify and authenticate a user once, and then use that identity information across multiple systems, both internally and externally including external partner websites.

It can improve privacy compliance by allowing the user to control what information is shared, or by limiting the amount of information shared. And lastly, it can drastically improve the end-user experience by eliminating the need for new account registration through automatic "federated provisioning" or the need to redundantly login through cross-domain single sign-on.

The notion of identity federation is extremely broad, and also evolving. It could involve user-to-user, user-to-application and application-to-application use-case scenarios at both the browser tier as well as the Web services or service-oriented architecture (SOA) tier. It can involve high-trust, high-security scenarios as well as low-trust, low security scenarios.

The levels of identity assurance that may be required for a given scenario are also being standardized through a common and open Identity Assurance Framework. It can involve user-centric use-cases, as well as employee-centric use-cases.

The term "identity federation" is by design a generic term, and is not bound to any one specific protocol, technology, implementation or company. Levels of assurance define the quality of the credentials each member of the Federation is offering. There are published standards defining these levels of assurance, and what an organization must comply with to qualify at each level.

One thing that is consistent, however, is the fact that "federation" does describe methods of identity portability which are achieved in an open, often standards-based manner – meaning anyone adhering to the open specification or standard can achieve the full spectrum of use-cases and interoperability.

Identity federation can be accomplished any number of ways, some of which involve the use of formal Internet standards, such as SAML, and some of which may involve open source technologies and/or other openly published specifications. (From Wikipedia.com).

WHAT IS THE RELATIONSHIP BETWEEN FEDERATIONS AND EDUNIFY?

In general due to the synergy between federations and the mission of PESC specifically related to cost-effectiveness and system connectivity, PESC supports the growth of federations, and encourages the use of federated authentication to both web portals and web services.

Many of the Web services registered and published in EdUnify will require federated authentication in order to make informed authorization decisions and in order for them to be useful outside their home institutions. Publishing Web services in EdUnify that are not already SAML enabled may provide opportunities for developers to take existing services and make them more valuable by adding federation-based technologies to them.