Introduction to Identity Federation

What is Identity Federation?

A **federated identity** in information technology is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems. The federation is a system of trust between two parties for the purpose of authenticating users and sharing information needed to authorize their access to resources.

> A federated identity in information technology is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems.
>
> It is related to single sign-on (SSO), in which a user's single authentication ticket, or token, is trusted across multiple IT systems or even organizations. SSO is a subset of federated identity management, as it relates only to authentication and is understood on the level of technical interoperability and it would not be possible without some sort of federation.

Federated identity is related to single sign-on (SSO), in which a user's single authentication ticket, or token, is trusted across multiple IT systems or even organizations. SSO is a subset of federated identity management, as it relates only to authentication and is understood on the level of technical interoperability and it would not be possible without some sort of federation.

With the identity federation, we get to separate the applications and, the login and get permissions process. Currently, there are two mainstream identity federation standards: **SAML** and **OpenID-Connect**.

The authentication service is responsible for identifying users and passing the information to the applications.

Which protocols are supported by Soffid?

- SAML
- OpenID-Connect
- CAS
- Radius
- TACACS+

SAML (Security Assertion Markup Language)

> Visit the SAML Chapter for more information.

OpenID-Connect

> Visit the OpenID-Connect Chapter for more information.

The main differences between SAML and OpenID-connect

- OpenID-connect uses simple form encoding or JSON rather than complex XML documents.
- OpenID-connect does not encrypt or sign requests or responses. Instead, it uses simple username/password authentication leveraging HTTPS transport security.

- OpenID-connect requires server to server communication to transfer security tokens. SAML allows this kind of communication, but does not need it.

---

https://en.wikipedia.org/wiki/Federated_identity

Revision #46
Created 4 August 2021 09:39:07
Updated 11 July 2023 13:18:23