SSO Protime

myProtime - Web

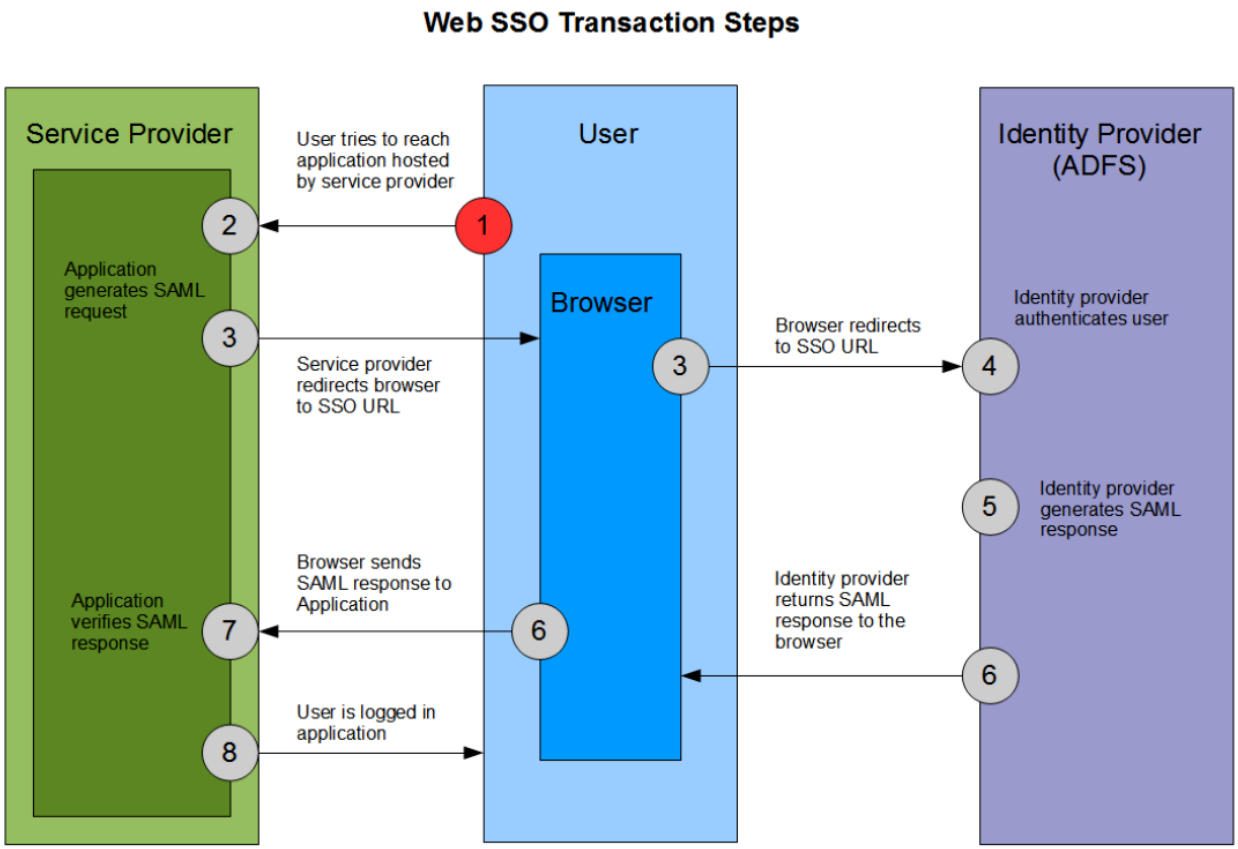
SAML Web SSO

Web Single Sign-On (Web SSO) systems consist of an agent installed on web servers, and a central infrastructure that includes a directory and servers or logic to manage authentication and access control.

When users attempt to access a web SSO-enabled web server or web application, the web SSO agent redirects the user's web browser to an authentication server, where the user signs in. The web browser is then redirected back to the requested web application, and the user can access the application or web content.

When an already authenticated user accesses another web application, the agent on the web application retrieves the user's validated credentials, thus eliminating any need for the user to sign on again.

Web SSO systems also incorporate access control mechanisms, where either the agent installed on each web server, or the web applications themselves (using an API), may check whether a user is entitled to access data or functions.



Most Web SSO systems also include a distributed administration interface, for defining new user accounts and managing existing ones.

In the web SSO design in Active Directory Federation Services (ADFS) 2.0, users must authenticate only once to access multiple ADFS-secured applications or services. In this design all users are external, and no federation trust exists because there are no partner organizations. Typically, you deploy this design when you want to provide individual consumer or customer access to one or more ADFS 2.0–secured services or applications over the Internet.

With the web SSO design, an organization that typically hosts an ADFS-secured application or service in a perimeter network can maintain a separate store of customer accounts in the perimeter network, which makes it easier to isolate customer accounts from employee accounts.

You can manage the local accounts for customers in the perimeter network by using either Active Directory Domain Services (ADDS), SQL Server, or a custom attribute store.

Supported SAML bindings

myProtime only supports the **SAML HTTP Post binding** for both Single Sign On (SSO) as Single Log Out (SLO).

Metadata URL

myProtime SAML Service provider configuration is available via the **SAML Metadata URL** which is available at the following url:
https://authentication.myprotime.eu/tenants/<tenant_name>/gatekeeper/spmetadata

Any external SAML identity provider is preferred to expose a similar SAML Metadata URL.

SAML Assertion - Subject

myProtime uses the **NameID** of the **Subject** to identify the authenticated user. This **MUST** be a valid email adress.