Leveraging ADFS

Overview:

The project involved Research and development of a custom integration with Active Directory Federation Service (ADFS) to allow for Single Sign-On (SSO) authentication to a custom core PHP application. SimpleSAMLphp was used to implement the Service Provider (SP) interfaces and communicate with the Identity Provider (IDP). The integration module was developed as a standalone service to reuse on new setups and allow for seamlessly authenticating users who have access privileges managed in AD.

Client details:

Name: Confidential | **Industry:** Software | **Location:** USA

Technologies:

Core PHP, SimpleSAMLphp library, ADFS

Project Description:

The integrated application connects a core PHP application to a remote ADFS server with proper authentication i.e. SSO (Single Sign-On).

What is ADFS?

- Active Directory Federation Services (ADFS) is a Single Sign-On (SSO) solution created by Microsoft as a component of Windows Server Operating Systems.

- ADFS gives organizations the ability to control their employees' accounts while simplifying the user experience. It was developed to provide flexibility. Employees only need to remember a single set of credentials to access multiple applications through SSO.

How does ADFS Work?

- ADFS manages authentication through a proxy service hosted between AD and the target application.

- It uses a "Federated Trust", linking ADFS and the target application to grant access to users. This enables users to log onto the federated application through SSO without the need to authenticate their identity on each and every application directly.

The authentication process follows these four steps:

1. The user navigates to a URL provided by the ADFS service.
2. The ADFS service then authenticates the user via the organization's AD service.
3. Upon authenticating, the ADFS service provides the user with an authentication claim.
4. The user's browser then forwards this claim to the target application, which either grants or denies access based on the Federated Trust service created.

What is Single Sign-On?

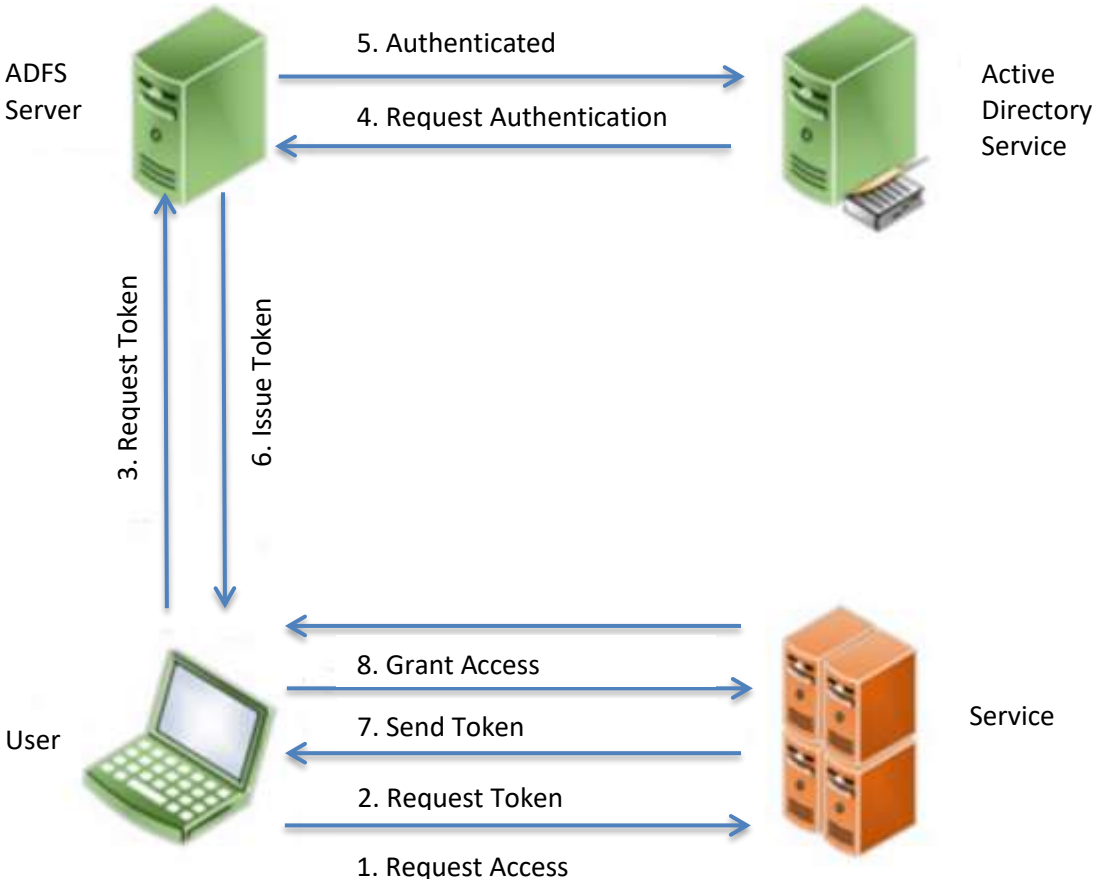
- Single sign-on (SSO) is a user authentication tool that enables users to securely access multiple applications and services using just one set of credentials.

- SSO is built on the concept of federated identity. When the system trusts the user, they are automatically granted access to all other applications that have established a trusted relationship with it.

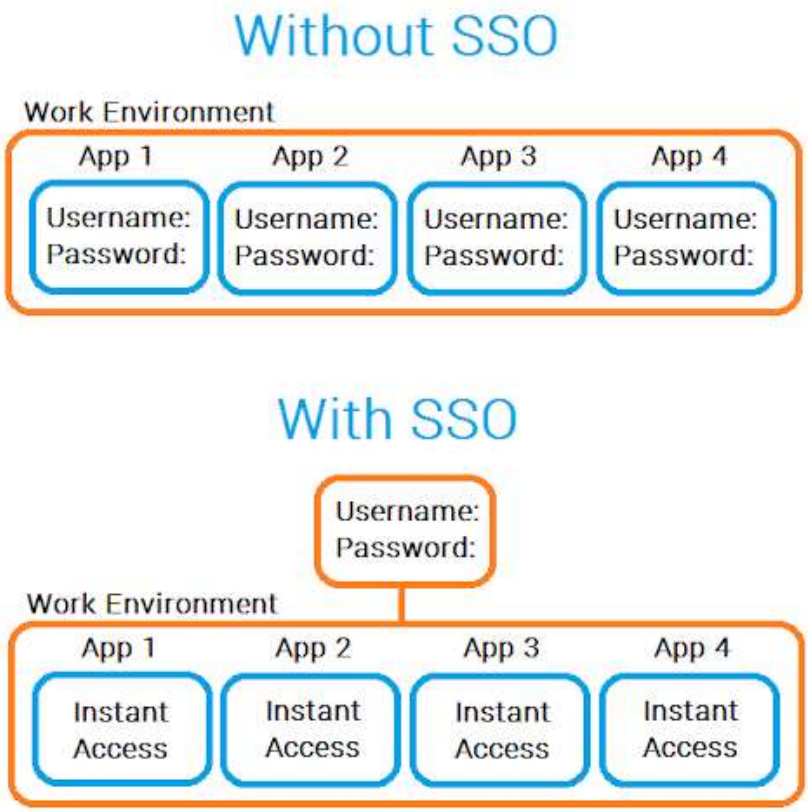
- This provides the basis for modern SSO solutions, which are enabled through protocols like OpenID Connect and SAML 2.0. For this test application SAML 2.0 protocol was used to implement SSO.

- When a user signs in to a service with their SSO login, an authentication token is created and stored in their browser. Any app or website the user subsequently accesses will check with the SSO service, which then sends the user's token to confirm their identity and provide them with the access.

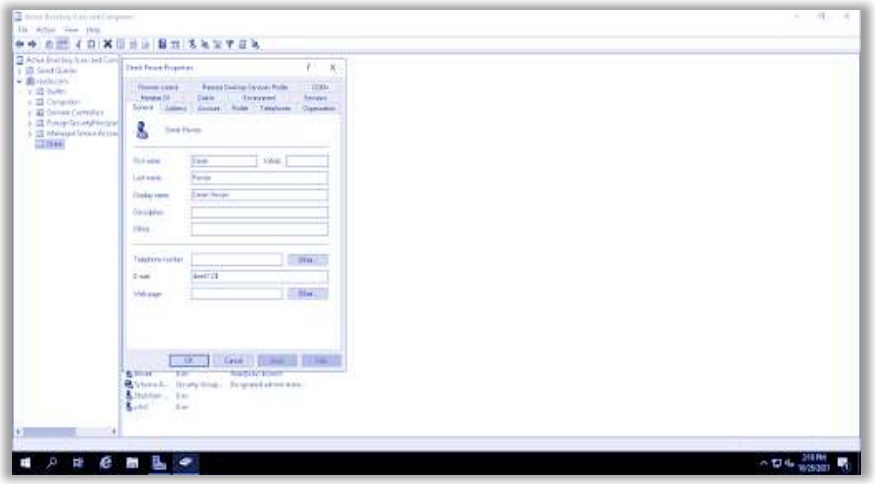
Architecture:



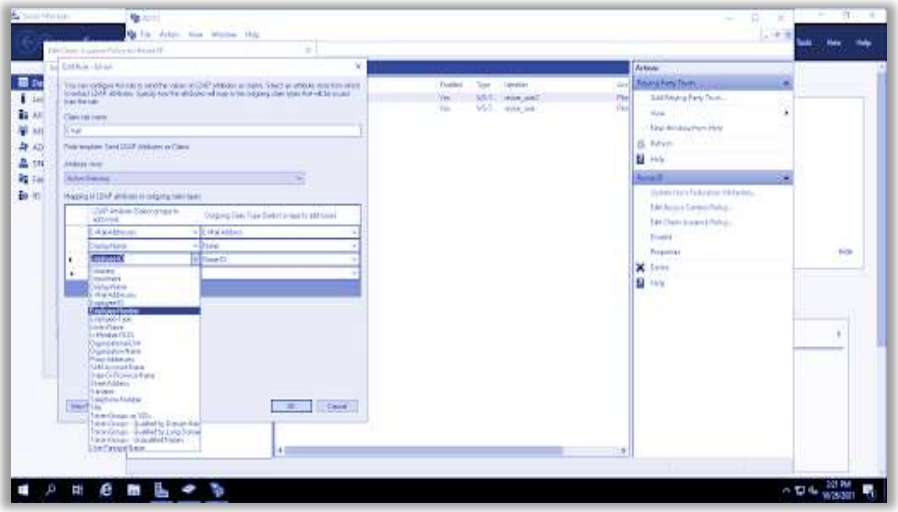
Flow Diagram:



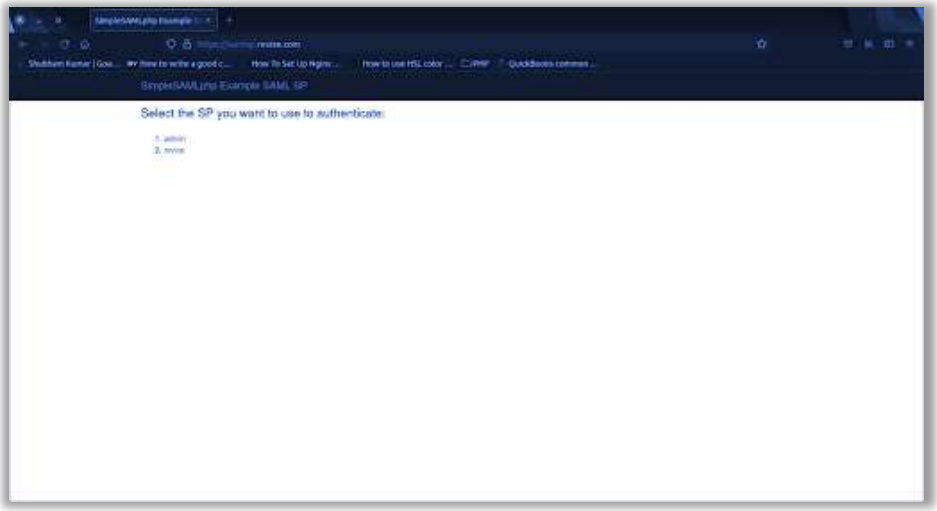
Screenshots:



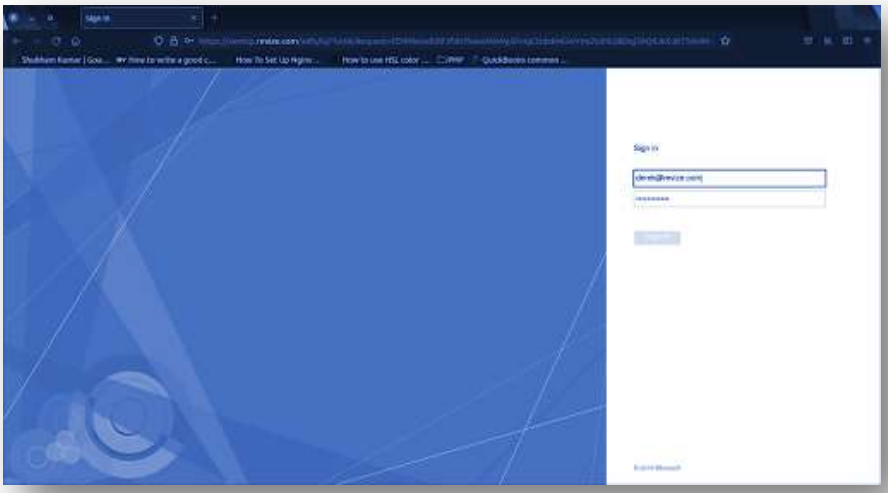
Screenshot 1: Add user to ADFS



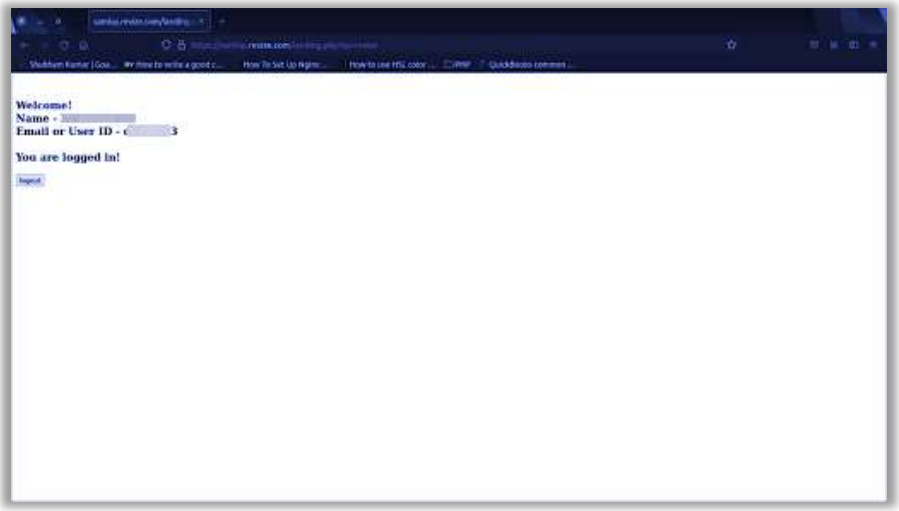
Screenshot 2: Map Attributes



Screenshot 3: Application SP Selection screen



Screenshot 4: Add credentials in ADFS Login screen



Screenshot 5: User logged in