Trust & Identity Incubator
Add OIDC OP support to SimpleSAMLphp

Sergio Gómez, Marko Ivancic, Patrick Radtke

Sprint demo 4.3 - June, 1st 2021

Public

www.geant.org
Overview

• Security Assertion Markup Language (SAML)
  • Authentication and authorization exchanging
  • Used in enterprise and government applications
• OpenID Connect (OIDC) is a widespread authentication protocol
  • Authentication layer on top of OAuth 2.0
  • Focused in mobile and web applications
## Overview: SAML vs OIDC comparison

<table>
<thead>
<tr>
<th>SAML</th>
<th>OIDC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Provider (SP)</td>
<td>Relying Party (RP)</td>
</tr>
<tr>
<td>Identity Provider (IdP)</td>
<td>OpenID Provider (OP)</td>
</tr>
<tr>
<td>XML based</td>
<td>JSON based</td>
</tr>
<tr>
<td>Feature rich</td>
<td>Lightweight</td>
</tr>
</tbody>
</table>
Overview

• SimpleSAMLphp (SSP) application that deals with authentication
  • Focused in SAML 2.0 SP and IdP deployments
  • Extensible with modules
  • Only supports OIDC Relaying Parting interface
• This activity seeks to implement an OIDC OP in accordance with the OIDC specification into SSP.
Background

- Existing module available
  - https://github.com/rediris-es/simplesamlphp-module-oidc
- Developed by University of Cordoba for RedIRIS, Spanish NREN.
- Basic flow support and not certified
Requirements

- Implement and certificate OP OIDC profiles:
  - Basic
  - Implicit
  - Hybrid

- Improve UI in SSP:
  - Users self RP registration
  - Custom scopes and claims configuration

- Other requirements
  - F-Tick support
Architecture

- Build over OAuth2.0 library:
  - Not fully standard compliant
  - Added anticorruption layer using OOP
- Added OIDC layer to check profile request validation
Achievements

• Implement basic profile
• Implemented f-tick support
• Small UI admin changes
• Dockerized development environment
• Dockerized conformance test environment
• Workshop of using Symfony in SimpleSAMLphp
Next steps

- Implement implicit and hybrid profile
- Pass OpenID certification
- UI to self-registering RP
- UI to configure custom claims and scopes
Thank you

Any questions?

www.geant.org