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

SAML	OIDC
Service Provider (SP)	Relying Party (RP)
Identity Provider (IdP)	OpenID Provider (OP)
XML based	JSON based
Feature rich	Lightweight

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.

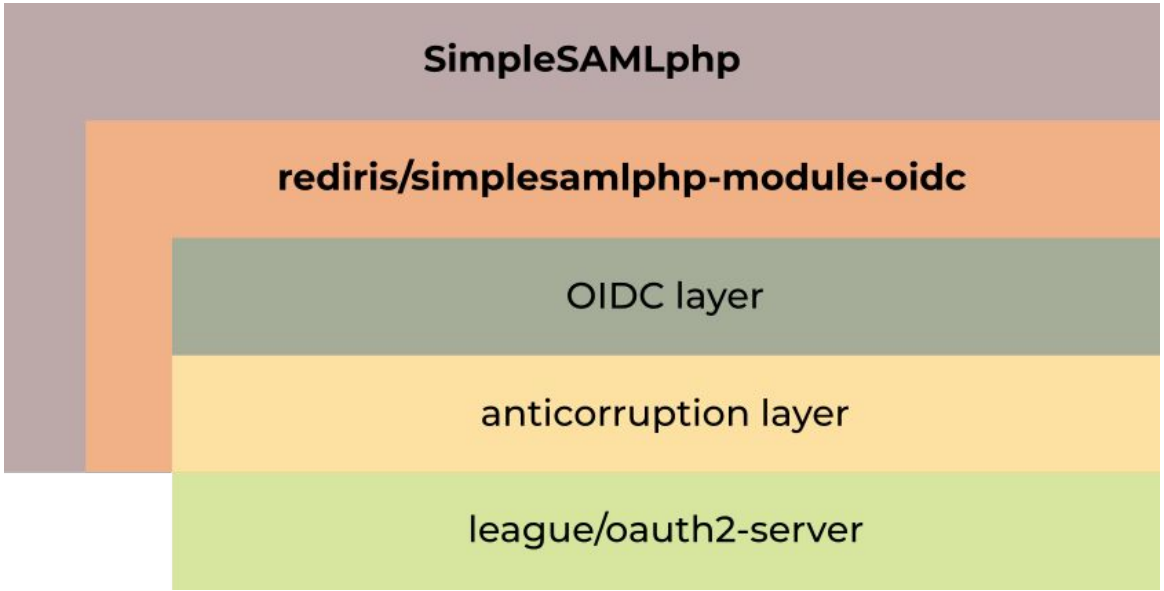
Background

- 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

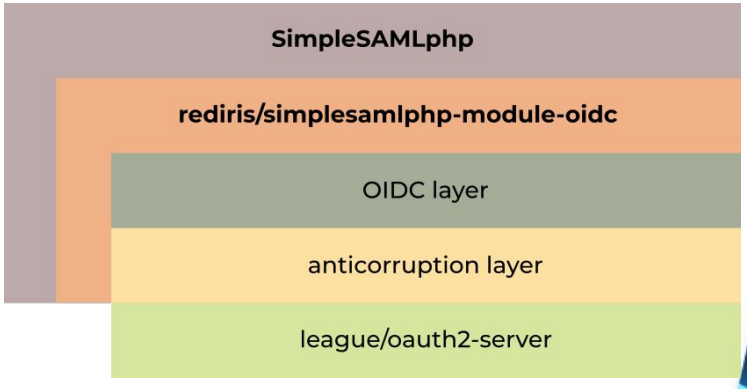
- Implement and certificate OP OIDC profiles:
  - Basic
  - Implicit
  - Hybrid
- Improve UI in SSP:
  - Users self RP registration
  - Custom scopes and claims configuration
- Other requirements
  - F-Tick support

Architecture

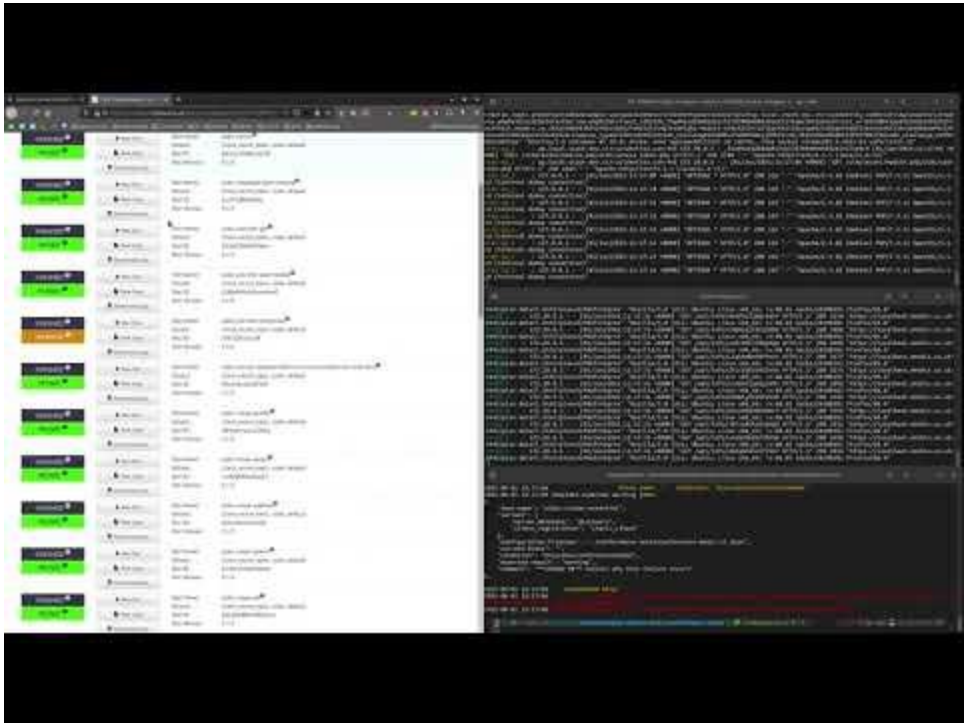


Architecture

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



Demo



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

GÉANT
Networks • Services • People

Thank you

Any questions?

www.geant.org

The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).