Trust & Identity Incubator
SimpleSAMLPhp OIDC OP module

September 21, 2021

Marko Ivancic, Patrick Radtke and
Sergio Gómez

Background

SimpleSAMLphp (SSP) is a commonly used software product for both SP and IdP deployments in Research and Education

SSP is extensible through a module system.

SSP has modules to authenticate user for CAS protocol and ws-fed

Project goal is to add an OIDC OpenID Provider module to SSP

Starting Point

University of Cordoba & RedIRIS (Spanish NREN) had done some work on a module.

Supports basic flow, but not yet conformant to the spec.

Module used in production by Srce (University Computing Centre Zagreb) and others.

Allows mapping of SAML attributes to OIDC Claims

Allows custom scopes and claims

Goals

Pass conformance tests

Add implicit flow support

Allow entitled users to register OIDC clients

Add F-TICKS support

Automated testing

Conformance Tests

May

Name	Variant	Description	Started	Modules
oidcc-basic-certification-test-plan	discovery, static_client	oidc-provider OIDC	9/20/2021, 2:59:19 PM	

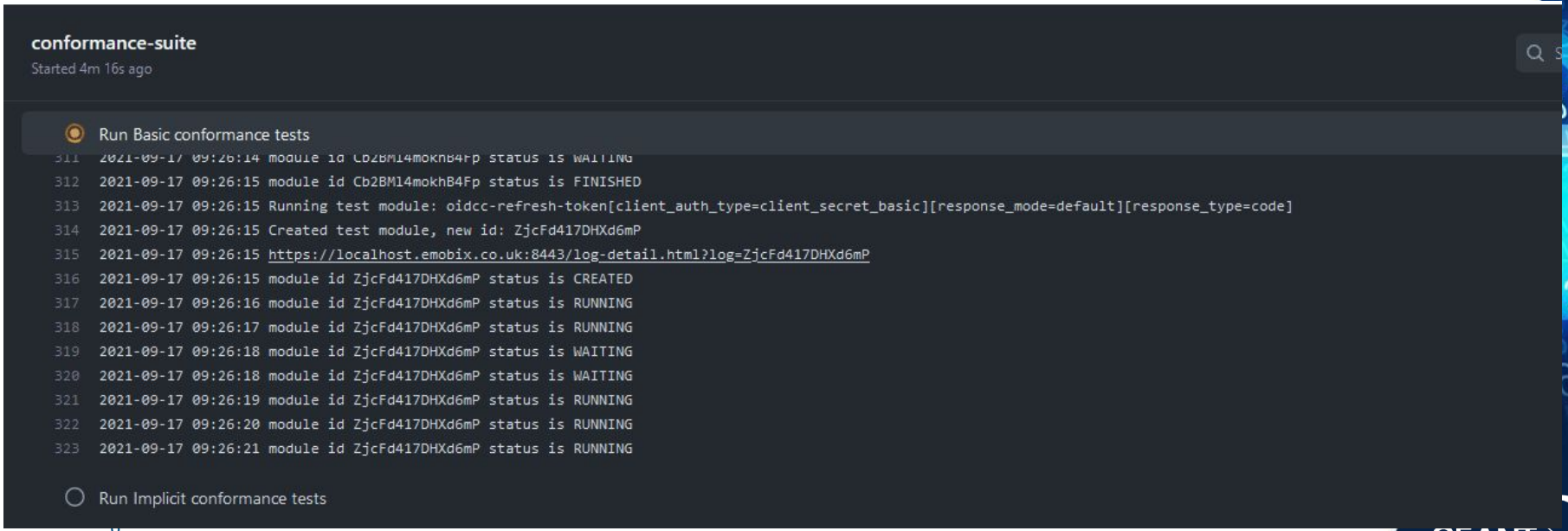
Now!

Name	Variant	Description	Started	Modules
oidcc-basic-certification-test-plan	discovery, static_client	oidc-provider OIDC	9/16/2021, 4:41:16 PM	

Green = pass, Black = fail, Orange = warning, Blue = needs manual verification

Conformance Tests

Conformance tests (and unit tests) are run for every pull request



Improvements

OIDC

- Authentication Context request
- Support for individual claim requests
- Support bool, int and json object claim types
- Error message improvements

UI

- Pagination of clients
- Authorized user self-management

Security

- Invalidate tokens if auth code is re-used
- Various dependency updates

Accomplishments

- Passing Basic and Implicit Conformance Tests
- Project moved to https://github.com/simplesamlphp/simplesamlphp-module-oidc
- FTICKs
- Authorized users can get register clients
- Docker image for testing
- Compatible with SSP's "newui" option enabled

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).