



# Trust & Identity Incubator SimpleSAMLPhp OIDC OP module

September 21, 2021

Marko Ivancic, Patrick Radtke and  
Sergio Gómez

[www.geant.org](http://www.geant.org)

## 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

```
conformance-suite
Started 4m 16s ago

Run Basic conformance tests
311 2021-09-17 09:26:14 module id Cb2BM14m0kNB4Fp status is WAITING
312 2021-09-17 09:26:15 module id Cb2BM14m0kNB4Fp status is FINISHED
313 2021-09-17 09:26:15 Running test module: oidcc-refresh-token[client_auth_type=client_secret_basic][response_mode=default][response_type=code]
314 2021-09-17 09:26:15 Created test module, new id: ZjcFd417DHXd6mP
315 2021-09-17 09:26:15 https://localhost.emobix.co.uk:8443/log-detail.html?log=ZjcFd417DHXd6mP
316 2021-09-17 09:26:15 module id ZjcFd417DHXd6mP status is CREATED
317 2021-09-17 09:26:16 module id ZjcFd417DHXd6mP status is RUNNING
318 2021-09-17 09:26:17 module id ZjcFd417DHXd6mP status is RUNNING
319 2021-09-17 09:26:18 module id ZjcFd417DHXd6mP status is WAITING
320 2021-09-17 09:26:18 module id ZjcFd417DHXd6mP status is WAITING
321 2021-09-17 09:26:19 module id ZjcFd417DHXd6mP status is RUNNING
322 2021-09-17 09:26:20 module id ZjcFd417DHXd6mP status is RUNNING
323 2021-09-17 09:26:21 module id ZjcFd417DHXd6mP status is RUNNING

Run Implicit conformance tests
```

# 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



# Thank you

Any questions?

[www.geant.org](http://www.geant.org)

