

# Interop testing

---

Presentation at the OpenId Connect Tech Summit by Roland Hedberg  
<[roland.hedberg@adm.umu.se](mailto:roland.hedberg@adm.umu.se)>

# Who we are

---

- Andreas Åkre Solberg
  - Works at UNINETT, Norway
  - Father of SimpleSAMLphp
  - Project leader of gn3-jra3-t2 (GN3 Identity Federations research task force)
- Roland Hedberg
  - Employed by Umeå University, Sweden
  - Responsible for pySAML2
  - Long experience of writing and implementing specifications.



# How we have divided it

---

- Andreas does the web front-end
- I do the protocol engine
  - accessible through a command line script

# Testing OpenID Connect Provider



Descriptive name of test server

## Client Credentials

Client identifier

Client secret

## Callback URL

Please configure to trust this callback URL on your provider

## Principal Authentication

Username

Password

## Setup service endpoints

### OAuth Authorization Endpoint:

### OAuth Token Endpoint:

### OpenID Connect Check Session Endpoint:

### OpenID Connect User Info Endpoint:

Mockup for OP registration

# What's going to be tested

---

- Conformance to the standards (Oauth2 + OpenI Connect)
  - OP and RP
- Extensions

# How

---

- A number of 'flows' will be defined
  - You can decide which ones to run
  - The flows are hierarchically organized; if a base flow doesn't work then the derivatives will not be tried.
- Minimal, dynamic, complete

Configure your SP | Register your SP | Prepare for testing | **Running tests**

Collapse debug | Expand debug | Success (52) | Errors (21) | Warnings (2) | Notices (11)

This test sends IdP initiated LogoutRequest to SP before the authn Response.

Session fixation check

SP MUST accept LogoutRequest with sessionindex in a separate session, not relying on the session-cookie.

SP MUST accept an LogoutRequest with no sessionindex (sent in separate session, no session-cookies)

SP MUST accept an LogoutRequest with two sessionindexes (first valid) (sent in separate session, no session-cookies)

SP MUST accept an LogoutRequest with two sessionindexes (second valid) (sent in separate session, no session-cookies)

SP MUST NOT accept LogoutRequest when NameID content is wrong

SP MUST NOT accept LogoutRequest when NameID@Format is wrong

SP MUST NOT accept LogoutRequest when NameID@SPNameQualifier is wrong

SP MUST NOT logout user when invalid SessionIndex is sent

SP MUST NOT accept LogoutRequest when Destination is wrong

SP MUST NOT accept unsigned LogoutRequest

SP SHOULD find attributes in a second Assertion/AttributeStatement, not only in one of them (test 1 of 2 - attributes in first).

SP SHOULD find attributes in a second Assertion/AttributeStatement, not only in one of them (test 2 of 2 - attributes in last).

SP MUST NOT accept a replayed Response. An identical Response/Assertion used a second time. [Profiles]: 4.1.4.5 POST-Specific Processing Rules (test 2 of 2: unsolicited response)

SP should accept a Response with two SubjectConfirmation elements representing two recipients (test 1 of 2, correct one last)

SP should accept a Response with two SubjectConfirmation elements representing two recipients (test 1 of 2, correct one first)

SP should not accept a Response with a SubjectConfirmationData elements with a incorrect @Address attribute

SP should accept a Response with multiple SubjectConfirmation elements with /SubjectConfirmationData/@Address-es, where one is correct (test 1 of 2, correct one last)

SP should accept a Response with multiple SubjectConfirmation elements with /SubjectConfirmationData/@Address-es, where one is correct (test 1 of 2, correct one first)

SP should not accept a Response with a AuthnStatement missing

SP should not accept an IssueInstant far (24 hours) into the future

SP should not accept an IssueInstant far (24 hours) into the past

# GN3 Federation lab automatic SAML2 tester

Result presentation