T&I Incubator Test IdP

Sprint demo #4.6 – 21st September 2021

Niels van Dijk, Martin van Es, Alan Lewis, Uros Stevanovic, Andrej Shliamin

Q3 2021

Public

www.geant.org
Background

• Test IdPs exist but do not fulfil all the needs of R&E

• A test IdP focused on R&E could:
  • Be easy to use for non-technical SPs
  • Test release of R&S and other entity category
  • Encourage best practice in attributes requested
  • Provide guidance why SSO has failed
  • Help validate the SP before joining a federation
  • Collate data on SP request trends
  • Provide a sustainable and trusted service
Aims and Objectives

• Investigate what is required
  • Aim: Understand community use cases and requirements
    • Identify use cases and review with stakeholders
    • Document use cases and map to Test IdP service requirements

• Implement a Test IdP service for R&E
  • Aim: Develop and test deployment of a sustainable service
    • Investigate technical approaches and develop a solution
    • Create a test deployment and associated policies and evaluate
    • Determine how such a service could be sustained
    • Plan to handover the service to an identified operator
Activities Status

- Stakeholder feedback collected and discussed
- Functionality and requirements documented
- Technical architecture finalised
- Tests scenarios defined
- Demo service created
- Relationship to eduGAIN determined
- End-user documentation created
- Make deployment even easier
Assumed requirements

- Must be able to support many SPs who are testing
- Must be able to establish trust between SP and Test IdP
- Must be able to release various attributes including for different entity categories
- Must allow various errors types to be triggered
- Must provide admin functionality for Test IdP maintainer
- Should provide logging functionality
- May provide admin monitoring capabilities
- May be a member of eduGAIN
Stakeholder feedback

- Focus on checking SP before fed./eduGAIN membership
- Simplify operation - SPs are not sophisticated
- Provide a ‘simple’ and ‘advanced’ mode
- Encourage ‘best practice’ and provide guidance
- Take account of national and international context
- Indicate issues if SP login fails
- Assume SAML SP implementation compliance tested
- Target user configuration/semantic error types
- Consider how differentiated from other test solutions
TestIdP and eduGAIN

- eduGAIN sets baseline requirements
- SPs in eduGAIN have had metadata validated
- eduGAIN has well defined support process
- eduGAIN has a well defined metadata ingest

- Test IdP must protect against rogue usage
- Needs own metadata validation process
- May need to provide support to the SP
- May require separate ingest scheme

Feedback indicated TestIdP should not be a part of eduGAIN
Any decision left for eduGAIN Steering committee
Test categories

Test IdP provides pre-defined test categories

- R&S Entity category tests
- Behavioural tests
- Generic Attribute profile tests
- REFEDS Assurance Framework profile tests
- Error scenario tests
- Experimental profile tests
Test IdP proposed architecture
Test IdP workflow

Login / Register via SP metadata
Paste your SP metadata into the text field below:

```xml
<wsdl:definitions xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
                  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
                  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                  targetNamespace="urn:oasis:names:tc:SAML:2.0:metadata">
  <wsdl:service name="SP">
    <wsdl:port name="SP_Port">
      <soap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>
      <wsdl:operation name="Login"/>
      <wsdl:operation name="Register"/>
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

https://testidp.incibator.geant.org/
Test IdP Portal

GEANT Test IdP is a SAML 2.0 SP testing service based on SimpleSAMLphp and focused on the needs of R&E. Please register for the service by uploading your SP metadata which will then be validated.

Once registered you can login to your Test IdP instance and select a user test profile. User test profiles check different success and error scenarios for your SP and may be edited.

Then login to your SP as usual and any issues resulting from the test will be indicated. Detailed logs are available to assist further investigation of any issues.

Register a new IdP
Paste your SP metadata into the text field below.

Or upload your SP metadata xml file:

Edit your IdP
Login to your account via Token

Login

-> Each and every SP will get its own unique test IdP
Demo

A service has requested you to authenticate yourself. Please select a profile and optionally which attributes to release from the information below.

Choose Test Scenario

- Research and Scholarship
  - Display name
  - Surname + givename
  - Name and affiliation
ePPN and pseudonymous epTID identifiers
  - Display name, ePPN and transparent epTID identifiers
  - Surname + givename, ePPN and transparent epTID
  - Surname + givename, ePPN and epTID identifier
  - Surname + givename, ePPN and epTID identifier

Choose attributes

Released attributes

Log in
Deployment

• Module for SimpleSAMLphp

• Docker deploy WIP

• Available from the GÉANT gitlab: https://gitlab.geant.org/TI_Incubator/test_idp
Account configuration

```json
{
  "message": "Research and Scholarship (R&S) profiles<br/>R&S has been designed as a simple and scalable way to release minimal amounts of research data.<br/>
  "profiles": {
    "account1": {
      "explanation": "This profile provides a R&S compatible attribute bundle with the name of the user name being provided<br/>
      "display": "Display name",
      "eduPersonPrincipalName": "jrockefeller@idp.example.org",
      "displayName": "John D. Rockefeller",
      "mail": "John.D.Rockefeller@idp.example.org"
    },
    "account2": {
      "explanation": "This profile provides a R&S compatible attribute bundle with the name of the user name being provided<br/>
      "display": "Surname + givenname",
      "eduPersonPrincipalName": "g_ohm@idp.example.org",
      "givenName": "Georg",
      "sn": "Ohm",
      "mail": "georg.ohm@idp.example.org"
    },
    "account3": {
      "explanation": "This profile provides a R&S compatible attribute bundle with the name of the user name being provided<br/>
      "display": "Name and affiliation",
      "eduPersonPrincipalName": "jweeler@idp.example.org",
      "givenName": "Joseph",
      "sn": "Weeler"
    }
  }
}
```
Conclusions and next steps

- Test IdP is very flexible and easy to deploy
- Provides very extensive capabilities for testing, which may need to be simplified for novice SPs
- Integration w/ eduGAIN not a good idea
- Investigated integration with eduGAIN Access Check

Feedback and suggested improvements so far:

- Editable attribute values (esp. entitlements and isMemberOf)
- Allow operation as test IdP for National federation test fed, can metadata handling be simplified?
- Registration API (to integrate w/ existing portals)
- Allow SP to see IdP logs
- Docker deployment (WIP)
Thank you