

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



Test IdP Derived Requirements

The following requirements apply to the Test IdP platform software. Requirements marked * form a part of the first iteration Minimum Viable Product (MVP1).

This document uses the keywords MUST, MUST NOT, SHOULD, SHOULD NOT and MAY according to RFC 2119.

1. SP registration and login

Identifier	Use case	Name	Description	MVP1
REG01	1	Secure registration	It MUST be possible to securely register an SP admin user on the platform for a given entity	*
REG02	1	Unique registration	It MUST NOT be possible to register the same entity more than once	
REG03	1,10	Save registration	It MUST be possible to save details associated with the registration	*
REG04	1	Login	It MUST be possible to login using the previously registered credentials	*
REG04	1	Delete registration	It MUST be possible to remove the SP registration details from the Test IdP	
REG05	1	Unique entity	It MUST not be possible to create an entity id that already exists	
REG06	1	Delete data	Once the SP Test IdP entity deletion has been triggered all stored data associated with the entity should be removed	

2. Metadata exchange

Identifier	Use case	Name	Description	MVP1
------------	----------	------	-------------	------



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**



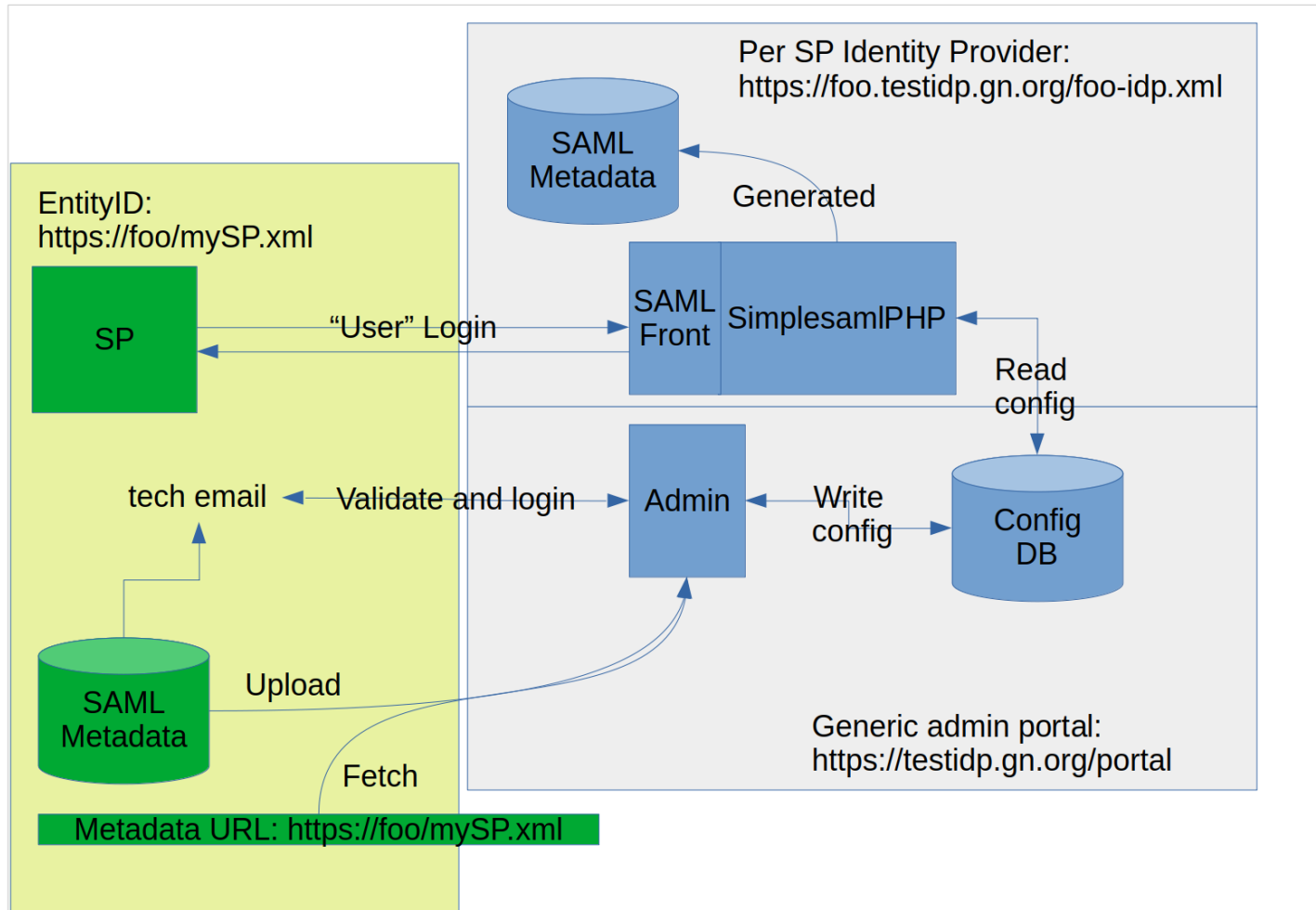
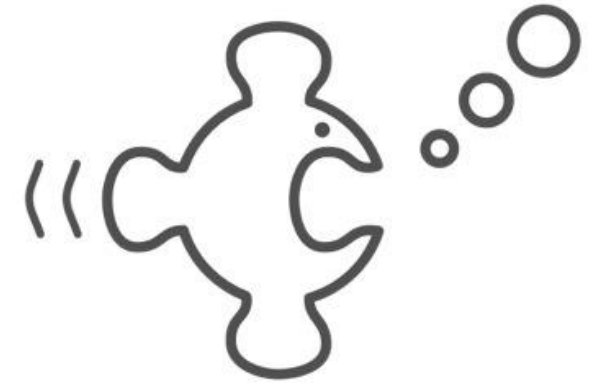
Test categories

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

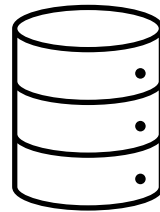
Paste your SP metadata into the text field below.

```
<md:EntityDescriptor entityID="https://sp.example.com/shibboleth"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:Extensions>
      <mdui:UIInfo>
        <mdui:DisplayName xml:lang="en">Test SP</mdui:DisplayName>
      </mdui:UIInfo>
    </md:Extensions>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Login / Register



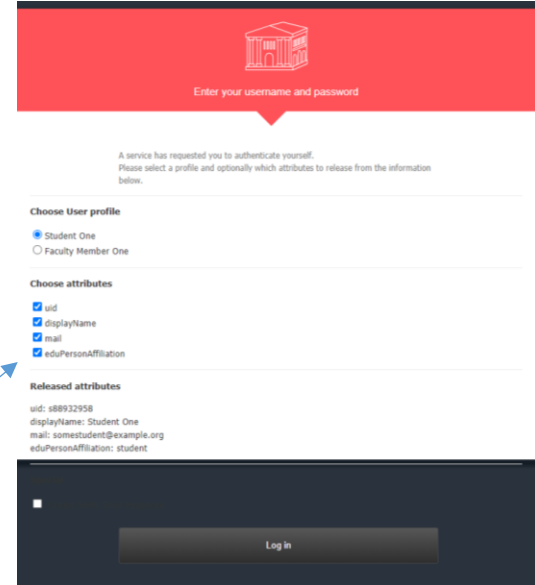
Your XML looks fine.
We have found 1 e-mail addresses provided in your metadata: <mailto:alan.l.lewis@gmail.com>.
We have sent an account activation e-mail to the first e-mail address <mailto:alan.l.lewis@gmail.com>.
If you didn't receive any e-mails, please contact our administrator and provide your token **3abe9eb777d848bca6734dc9377c0571**.



<https://testidp.incibator.geant.org/>



Token



Test IdP Portal



GÉANT 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.

<h3>Register a new IdP</h3> <p>Paste your SP metadata into the text field below.</p> <input type="text"/> <p>Or upload your SP metadata xml file.</p> <p>Select a file</p> <p>Register</p>	<h3>Edit your IdP</h3> <p>Login to your account via Token</p> <input type="text"/> <p>Login</p>
--	---

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

Demo



Enter your username and password

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 + givenname Name and affiliation ePPN and pseudonymous epTID identifiers Display name, ePPN and transparent epTID iden Surname + givenname, ePPN and transparent epT Surname + givenname, ePPN and epTID identifier Surname + givenname, ePPN and epTID identifier	Woohaa!
--	---------

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

The screenshot shows a GitLab repository page for 'test_idp' under the 'Trust and Identity Incubator' organization. The repository is on the 'master' branch. A commit by Martin van Es is highlighted with the message 'Make Error message customizable in logins.json'. Below this is a table of repository files and their commit history.

Name	Last commit	Last update
config	Make Error message customizable in logins...	1 week ago
metadata	Add subject and pairwise-id	2 weeks ago
modules/customauth	Make Error message customizable in logins...	1 week ago
.gitignore	Improve explanations	2 months ago
README.md	Improve README and add architecture pic...	2 months ago
test_idp_architecture.svg	Improve README and add architecture pic...	2 months ago
testidp.sql	Dynamic DB IDP configuration	5 months ago

The README.md file is displayed below the table, titled 'Test_IdP'. It describes the project's structure and provides instructions for enabling the custom authentication module and configuring the database.

Test_IdP

This project consists of two separate parts for simpleSAMLphp. This README assumes you know your way around in simpleSAMLphp and know how to setup a working implementation.

The authentication module is located in modules and is called customauth, and should be enabled like this:

```
config/authsources.php
```

```
+ 'custom-userpass' => [  
+   'customauth:External',  
+ ],
```

Don't forget to touch `enable` in the module directory to enable the module.

The second part are the DB based *IdP Hosted* and *SP Remote* metadata files, found in metadata. These files enable database based configuration, based on the DB structure found in testidp.sql

The Database consists of 3 tables:

- options
- idps
- config

options contains the definitions of the adjustable simpleSAMLPHP hosted IdP configuration options, this can be used to render a configuration interface. The options have a key, which is used in config to configure this option for a specific IdP.

idps contains the vhost based configuration for an IdP and the most important part is the `sp_metadata` columns, which should contain the connected SP metadata so that this IdP trusts this SP.

Account configuration

```
logins.json 31.1 KB Edit Web IDE Lock Replace Delete
1 {
2   "Research and Scholarship": {
3     "message": "<b>Research and Scholarship (R&S) profiles</b><br/>R&S has been designed as a simple and scalable way to release minimal amounts of re
4     "profiles": {
5       "account1": {
6         "explanation": "<b>R&S: displayName</b><br/>This profile provides a R&S compatible attribute bundle with the name of the user name being provi
7         "display": "Display name",
8         "eduPersonPrincipalName": "jrockefeller@idp.example.org",
9         "displayName": "John D. Rockefeller",
10        "mail": "John.D.Rockefeller@idp.example.org"
11      },
12      "account2": {
13        "explanation": "<b>R&S: surname + givenname</b><br/>This profile provides a R&S compatible attribute bundle with the name of the user name bein
14        "display": "Surname + givenname",
15        "eduPersonPrincipalName": "g_ohm@idp.example.org",
16        "givenName": "Georg",
17        "sn": "Ohm",
18        "mail": "georg.ohm@idp.example.org"
19      },
20      "account3": {
21        "explanation": "<b>R&S: name and affiliation</b><br/>This profile provides a R&S compatible attribute bundle with the name of the user name be
22        "display": "Name and affiliation",
23        "eduPersonPrincipalName": "jweeler@idp.example.org",
24        "givenName": "Joseph",
25        "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

www.geant.org



© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).
The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation
programme under Grant Agreement No. 731122 (GN4-2).