T&I Incubator Test IdP

Sprint demo #4.3 – 1st June 2021

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

Q2  2021

Public

www.geant.org
• Test IdPs exist but do not fulfil all the needs of R&E
  • Aim: Understand community use cases and requirements
    • Identify use cases and review with stakeholders
    • Document use cases and map to Test IdP service requirements

• A free Test IdP focused on R&E would be highly useful
  • 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
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
Planned activities

Test IdP

Use cases and requirements
- Setup stakeholder meetings
- Capture and replay feedback
- Capture requirements

Design and Implementation
- Investigate platforms
- Define architecture
- Create PoC platform

Test and Deployment
- Create Test SP(s)

Sustainability and handover

You are here

Activities status

Status

- Stakeholder feedback summarised and replayed
- Technical architecture and approach agreed
- SimpleSAML front-end PoC platform created
- Back-end SP admin GUI created
- Initial set of use cases and scenarios detailed
- End-to-end PoC system demo
- eduGAIN inclusion resolution
- A comprehensive solution is quite hard
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
What can/should we test?

- SAML s/w implementation is outside scope
- Invalid SP metadata
- Best practices
- Successful login flow
- Unsuccessful login flow
  - Does SP gracefully handle errors returned from IdP
  - Missing/Invalid attributes
  - SP configuration errors
    - Incorrect signing key used
    - Bad signature/encryption algorithm
Test IdP proposed architecture
SAML frontend demo

• Martin
SAML backend functionality

Login / Register via SP metadata

Paste your SP metadata into the text field below.

```
<md:IdentityDescriptor entityID="https://sp.example.com/shibboleth"
  xmlns="http://www.sit.org/2002/08/samlcore"
  xmlns:o="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:samlmeta-data"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <md:Extensions>
    <md:Display Name xsi:nil="true">Test SP</md:Display Name>
  </md:Extensions>
<br/>
```

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 3abe9eb7776848bca6734dc9377c0571.

https://testidp.incibator.geant.org/
To eduGAIN or not?

- 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
Open questions

• Should the Test IdP be a part of eduGAIN?
• Level of security needed for an eduGAIN Test IdP?
• Should national federation attributes be included?
• Are eduGAIN requirements the lcdn for Test IdP?
• What types of error should be tested?
• How important is encouraging best practice?
• What knowledge can we assume about Test IdP users?
Next steps

• Iterate Test IdP with additional error cases
• Unify front/back end and GUI approach
• Provide error logging capability
• Build Test IdP admin functionality
• Arrange further stakeholder discussions
• Investigate potential service costs
• Identify a suitable hosting partner
Thoughts, ideas, questions??
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 (GN-2).