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

Background

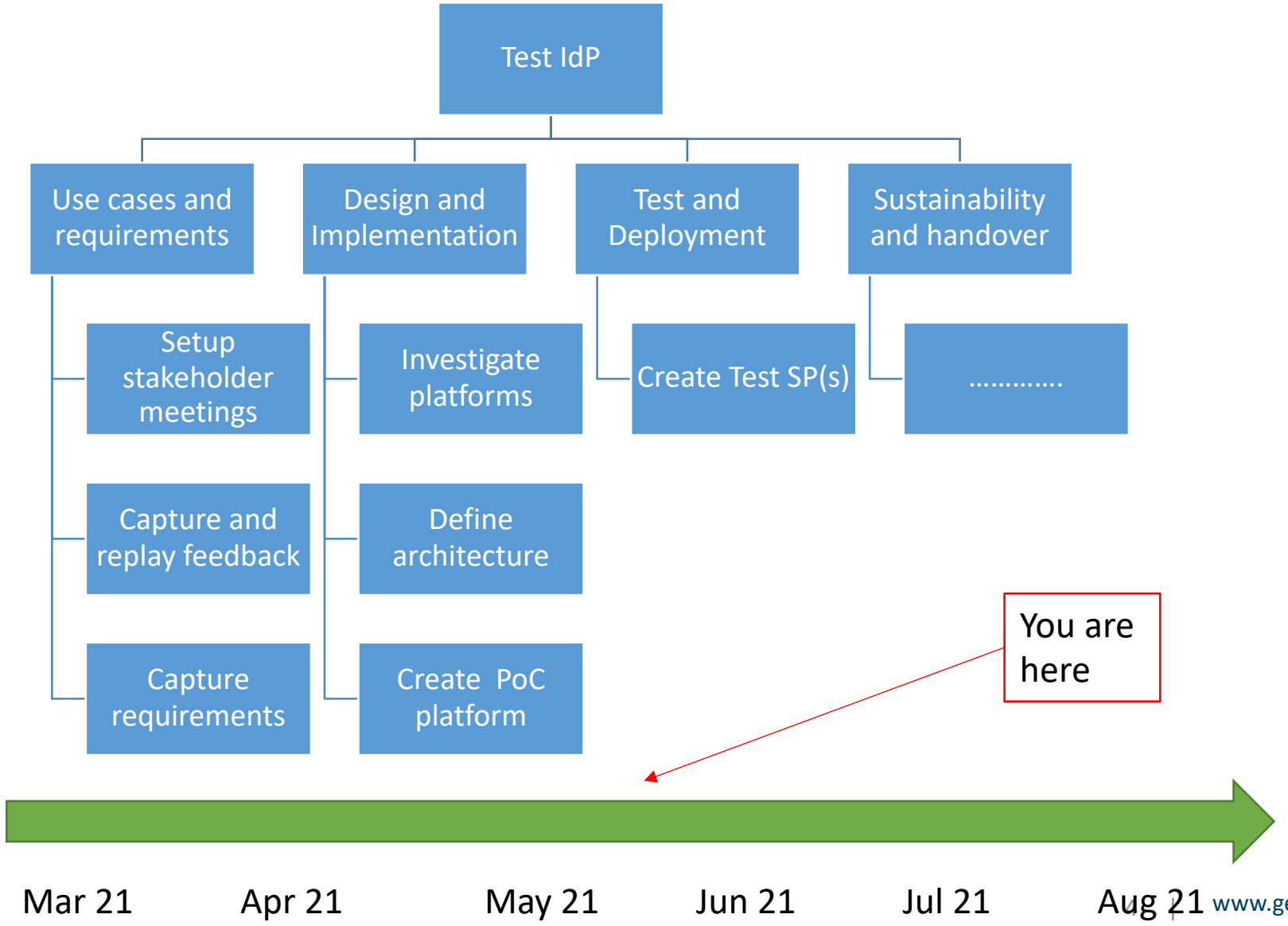
- Test IdPs exist but do not fulfil all the needs of R&E
  - Aim: Understand community use cases and requirements
    - Identify use cases and review with stakeholders
    - Document use cases and map to Test IdP service requirements

- 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

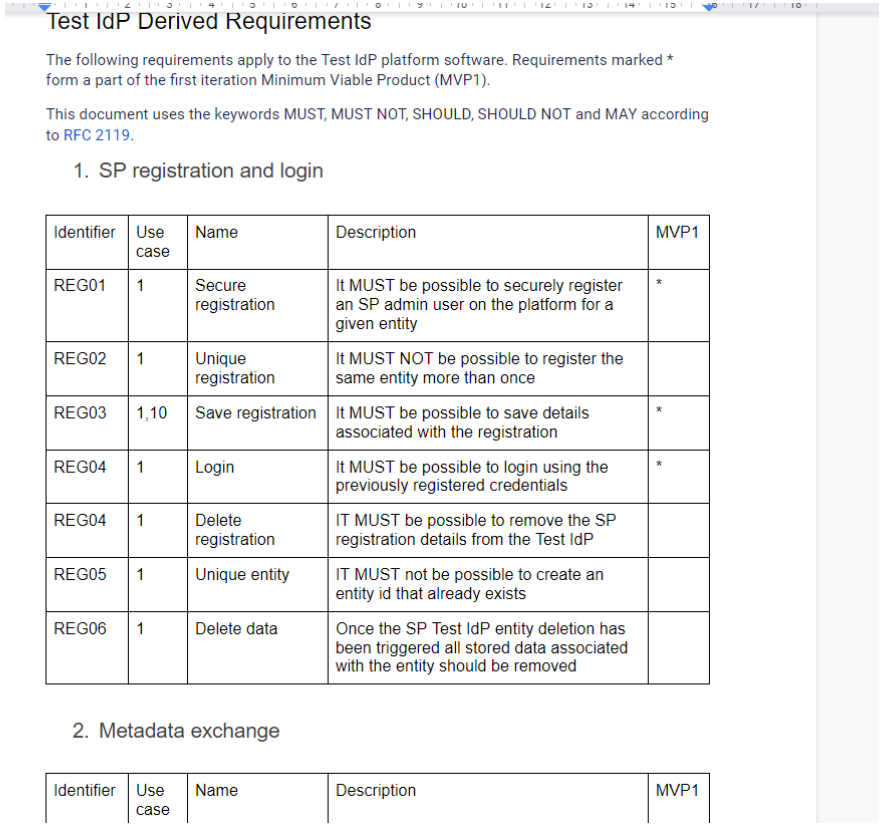
Planned activities



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 ✗



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

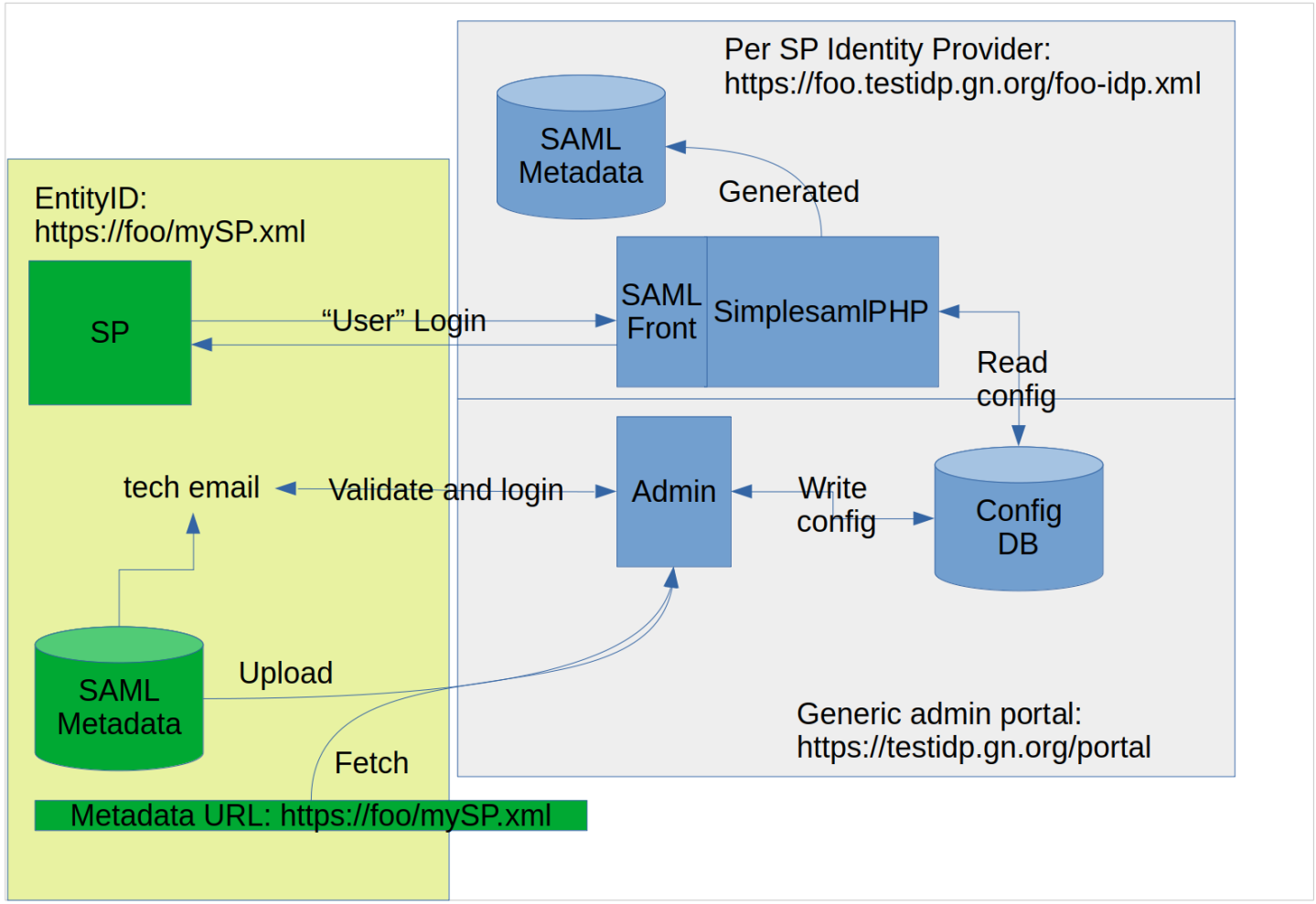
Stakeholder feedback

- 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 metatdata
- 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

GÉANT TEST IDP PORTAL

Login / Register via SP metadata

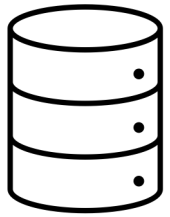
Paste your SP metadata into the text field below.

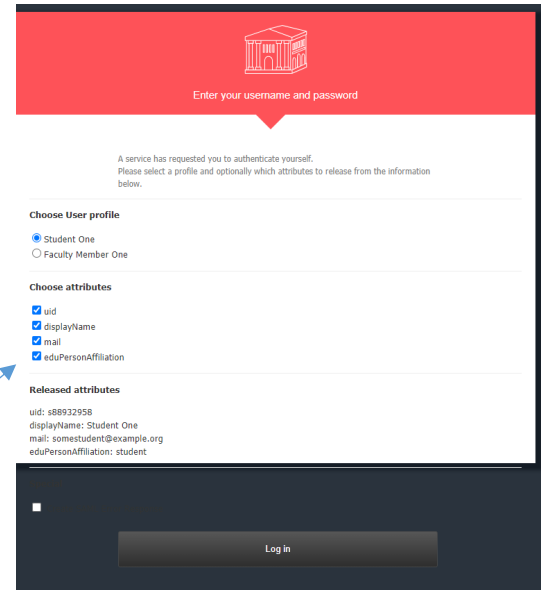
```
<md:EntityDescriptor entityID="https://sp.example.com/shibboleth"
                     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                     xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
                     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>
```

Login / Register

GÉANT TEST IDP PORTAL

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

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 lcd 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??

GÉANT
Networks • Services • People

Thank you

www.geant.org

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).