



GEANT Trust and Identity Incubator

Niels van Dijk (SURF)

REFEDS townhall, Oct 11, 2023

Public (PU)

Incubator activities

- Activity Cycle 1 (completed)
 - **Further improve the personal profile page**
 - geteduroam Linux client
 - OIDCfed support on SimpleSAMLphp
 - Passkeys - Use and Deployment for R&E Services
- Activity Cycle 2 (current)
 - **Automation of deployment and configuration of initial set of SPs for new federations**
 - **Scalable testing for insecure SAML signature validation**
 - Trust fabric for wallets
 - Webwallet for research and education use case

Scalable testing for insecure SAML signature validation (Call for participation)

Niels van Dijk (SURF)

REFEDS townhall, Oct 11, 2023

Public (PU)

Scope of the activity

- SP signature validation is paramount to the SAML federation security model
- We have seen incidents, among other with commercial vendors

-> Can we test *at scale* if services are indeed validating

Open Questions

- **Which test are needed, which are doable?**
 - Partial signatures, Multiple signatures, Modified message, etc
 - Do we need user accounts?
- **What deployment model is preferred?**
 - Role of FedOPS (and/or federation policy)
 - Timing of the testing (bulk or when onboarding)
 - As-a-Service?
- **How can we protect against potential legal action?**
 - Involve & invite SP
 - Share results between federations?

Invite for participation

- **Workshop:** We seek participation of FedOPS for a workshop to discuss and collect input (date & time: tbd)
- **Test and Deploy:** we seek participation of **max 5** FedOPS to test and deploy a solution (beginning 2024)

Automation of deployment and configuration of initial set of SPs for new federations (Call for feedback & participation)

Niels van Dijk (SURF)

REFEDS townhall, Oct 11, 2023

Public (PU)

3 seemingly alike use cases:

- Provide a ready to roll set of SPs for new federations
- “What I am basically looking for is a set of (fairly simple) ‘collaboration tools’ which nearly every collaboration needs.”
- Support institutions who want to streamline deployment of services at their campus

Scenario 'deployment scripts'

- Integrate Services directly into federation
-> Create set of deployment scripts to roll out services

We know this can be done, it's 'just' work

But how to maintain?

Not a 'fundamental' improvement

Scenario 'Proxy model'

- Leave federating and containerizing to the SP vendor
- 'Create' a proxy solution
 - which has 'standardized' interaction with IdP
 - provides a few default 'patterns' for SP authN and provisioning
 - SAML R&S
 - OIDC
 - LDAP
 - auto generated config documentation[1]
 - and has *per SP config modules to integrate* with backend SP
- Facilitate automated deployment of proxy
- Facilitate automated deployment of SPs (based on *existing* dockers)

[1] like e.g.: <https://perun-proxy-aai.gitlab-pages.ics.muni.cz/sp-docs/>

Invite for participation

- **Workshop:** We seek stakeholders for a workshop to discuss and collect input (date & time: tbd)
 - Pro's and Con's of proposed direction
 - Services which should be included
 - Usecases you have
 - Contributions you might be able to make

IdP User Profile Page

Niels van Dijk (SURF)
Mihály Héder (KiFu / SZTAKI)
Marko Ivančić (SRCE)
Janne Lauros (CSC)

REFEDS townhall, Oct 11, 2023








Public (PU)

Goals of this activity

A user profile page for **Shibboleth IdP** and **SimpleSAMLphp**

- enable end users to gain insight into **where their personal data is used** and **when it was last released** to various services, as far as the IdP is aware.
- Provide **personal data export** (GDPR)
- Data includes **OIDC tokens**, with the possibility of revocation
- **Starting point** for further interaction wrt personal data

What we have achieved

-  Common design in Figma
-  shibboleth implementation
 - Personal data page, connected services page, activity page, all services
-  simpleSAMLphp implementation
 - Personal data page, connected services page, activity page
-  Refresh and Access Token visualization (both IdPs)
-  Refresh and Access Token revocation (both IdPs)
-  SSP OIDC module to 2.0.x line
-  Good feedback from several fronts



Demo

www.geant.org



Co-funded by
the European Union

- Personal Data
- Connected Services
- Activity Page
- All Services
- Log Out

Personal Data

Attribute	Your value	Actions
Given name	Ted	
Surname	Tester	
Principal name	tedte@acme.com	
Assurance level	https://refeds.org/assurance/IAP/low	https://refeds.org/assurance/ID/eppn-unique-no-reassign https://refeds.org/assurance
Entitlement	http://example.com/myentitlement	
Affiliation	student member	
Common name	Ted Phileas Tester	
E-mail	ted.tester@acme.com	
Display name	Ted Tester	

Expected Future work

- Future
 - **Maintenance:** some working hours for both main developers in the GN5 Outreach task
 - Potential future features
 - *custom design for an attribute value, ie. group info*
 - *proxy awareness*
 - *Logos*
 - *Integration with SATOSA/other AAI stacks*
 - in-situ consent revocation
 - History download & Delete
 - Evolving look & feel
 - still leftovers in from our figma design

Thank you! Questions?

Incubator Sprint demo results:

<https://wiki.geant.org/display/GWP5/Incubator+demos>

User profile page links

SimpleSAMLphp

<https://github.com/cicnavi/simplesamlphp-module-accounting>

Shibboleth

<https://github.com/GEANT/shib-idp-profile>



ABOUT TIIME

PROGRAMME

JOURNEY AND STAY

SPONSORSHIP

HOST AND ORGANISERS

CONTACT

TIIME Unconference

31. Jan - 01. Feb 2024

Copenhagen

<https://tiime-unconference.eu/>

111

Days

:

12

Hours



41

Minutes

:

03

Seconds



Further screenshots BOTH SSP and SHIB

www.geant.org



Co-funded by
the European Union

 Personal Data

 Connected
Organizations

 Activity

 Log out

This is what we know about you...

Attribute	Your value
hrEduPersonUniqueID ⓘ	testuser@primjer4.hr
User ID ⓘ	testuser
Common name ⓘ	TestName TestSurname
Surname ⓘ	TestSurname; TestSurname
Given name ⓘ	TestName
Mail ⓘ	testusermail@primjer.hr; testusermail2@primjer.hr
hrEduPersonPersistentID ⓘ	da4294fb4e5746d57ab6ad88d2daf275-1
Display name ⓘ	testname123

 Personal Data Connected
Organizations Activity Log out

Name	All access	Last access	
Renner, DuBuque and Schaden	59	December 18, 2022 05:06	▼
Bogan-Marvin	40	December 25, 2022 11:06	▼
Hermann-Farrell	39	January 11, 2023 22:06	▼
Fahey-McKenzie	36	January 14, 2023 10:06	▼
Bradtke-Emmerich	30	December 25, 2022 03:06	▼
Marks LLC	28	January 6, 2023 00:06	▼
Gleason-Beier	27	December 30, 2022 01:06	▼
Tillman-Kunze	27	January 12, 2023 09:06	▼
Lang Group	27	January 14, 2023 18:06	▼

Crucial in case of account theft

 Personal Data

 Connected
Organizations

 Activity

 Log out

Time	Access	Sent data
January 15, 2023 04:06	Ullrich-Hartmann	hrEduPersonUniqueID, User ID, Common name, Surname, Given name, Mail, hrEduPersonPersistentID, Display name
<p>Information transferred to service: hrEduPersonUniqueID: testuser@primjer4.hr User ID: testuser Common name: TestName TestSurname Surname: TestSurname, TestSurname Given name: TestName Mail: testusermail@primjer.hr, testusermail2@primjer.hr hrEduPersonPersistentID: da4294fb4e5746d57ab6ad88d2daf275-1 Display name: testname123</p> <p>IP address: / Authentication protocol: SAML2</p>		
January 14, 2023 23:06	Pfannerstill-Conn	hrEduPersonUniqueID, User ID, Common name, Surname, Given name, Mail, hrEduPersonPersistentID, Display name
January 14, 2023 20:06	Hermiston and Sons	hrEduPersonUniqueID, User ID, Common name, Surname, Given name, Mail, hrEduPersonPersistentID, Display name
January 14, 2023 18:06	Lang Group	hrEduPersonUniqueID, User ID, Common name, Surname, Given name, Mail, hrEduPersonPersistentID, Display name
January 14, 2023 17:06	Corwin, Hayes and Smitham	hrEduPersonUniqueID, User ID, Common name, Surname, Given name, Mail, hrEduPersonPersistentID, Display name
January 14, 2023 12:06	Marquardt, Gutmann and	hrEduPersonUniqueID, User ID, Common name, Surname, Given name, Mail, hrEduPersonPersistentID,

- Personal Data
- Connected Services
- Activity Page
- All Services
- Log Out

What would be released if you used the service (running AttributeResolvers)

Available Services

E-SCIENCE.PL

SLAC Identity Services Dev

German Cancer Research Center: Medical Informatics in Translational Oncology

sciencedata.dk [NEW]

CLARIN CMDI metadata (prod)



Principal name: tede@acme.com
Surname: Tester
Display name: Ted Tester
Common name: Ted, Phileas, Tester
Given name: Ted
subject: ODX7VZGNLTJEMXVHGVPUGFGYJFKDCIMB
Affiliation: student, member

[Show attributes](#)

[Show attributes](#)

[Show attributes](#)

[Show attributes](#)



Personal data

Connected organizations

Activity page

Personal data

ⓘ Lorem ipsum dolor sit amet, consectetur adipiscing elit. Senectus id mattis ac adipiscing tempus eget. Sed at nec tincidunt pellentesque nunc sit. Aliquam sit pellentesque tempor elementum imperdiet aliquet consectetur. ✕

Attribute ▾	Your value ▾	⬇
Full name ⓘ	John Doe	
Surname ⓘ	Doe	
First name ⓘ	John Doe	
Display name ⓘ	John Doe	
Affiliation ⓘ	student	
User ID ⓘ	johny25	
Email Address ⓘ	john.doe@surfnet.nl john.doe@surfnet.nl	
Mobile ⓘ	+31 65 134 7657 +31 65 134 7657	
Institution User ID ⓘ	johny25@surfnet.nl	


Previous design

Personal data

Connected organizations

Activity page

Connected organizations

 Lorem ipsum dolor sit amet, consectetur adipiscing elit. Senectus id mattis ac adipiscing tempus eget. Sed at nec tincidunt pellentesque nunc sit. Aliquam sit pellentesque tempor elementum imperdiet aliquet consectetur.

+ Add filter

Sent: Surname, Entiy ID, Email First access: 2021.10.01-2022.5.22. 

Name	All access	Last access	Data requested
 Surf	2	6 May, 2022 14:43:35	surname  given name  email  username 
 HEXAA	6	6 May, 2022 14:43:35	surname  given name  email  username  entitlements 
 AAI Attributes Viewer	6	6 May, 2022 14:43:35	surname  given name  email  username  entitlements 
 Book-It Membership Software	6	6 May, 2022 14:43:35	email  username 
 ProClass	6	6 May, 2022 14:43:35	surname  given name  email  username  entitlements 
 Vaave	6	6 May, 2022 14:43:35	surname  given name  email 
 Example	6	6 May, 2022 14:43:35	surname  given name  email  username 

1-8/52

< Previous 1 2 3 .. 7 Next >

Previous design

Restart

- Personal data
- Connected organizations
- Activity page

All activity

Search... + Add filter Sent: Surname, Entiy ID, Email X First access: 2021.10.01-2022.5.22. X

Time	Organization	Sent data
6 May, 2022 14:43:35	example.org	surname ⓘ given name ⓘ email ⓘ username ⓘ entitlements ⓘ
6 May, 2022 14:43:35	surf.nl	surname ⓘ given name ⓘ email ⓘ username ⓘ
Information transferred to the service		
Surname ⓘ Doe		
Given name ⓘ John		
Email Address ⓘ john.doe@surf.nl		
Username ⓘ John Doe		
Entitlement regarding ⓘ urn:mace:dir:entitlement:common-lib-terms the service		
6 May, 2022 14:43:35	example.org	surname ⓘ given name ⓘ email ⓘ username ⓘ entitlements ⓘ
6 May, 2022 14:43:35	surf.nl	surname ⓘ given name ⓘ email ⓘ username ⓘ
6 May, 2022 14:43:35	hexaa.eu	email ⓘ username ⓘ
6 May, 2022 14:43:35	surf.nl	surname ⓘ given name ⓘ email ⓘ username ⓘ entitlements ⓘ

Previous design



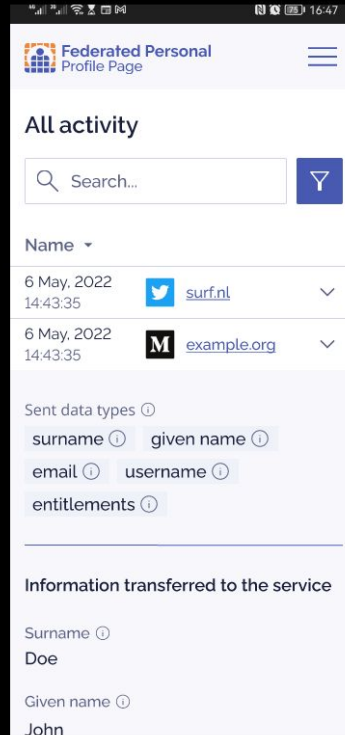
Flows



Desktop view

✓ Mobile view

No description



Previous design