Trust & Identity Incubator - IdP as a Service

REFEDS @TechEx2019

New Orleans, Dec 9 2019

Niels van Dijk

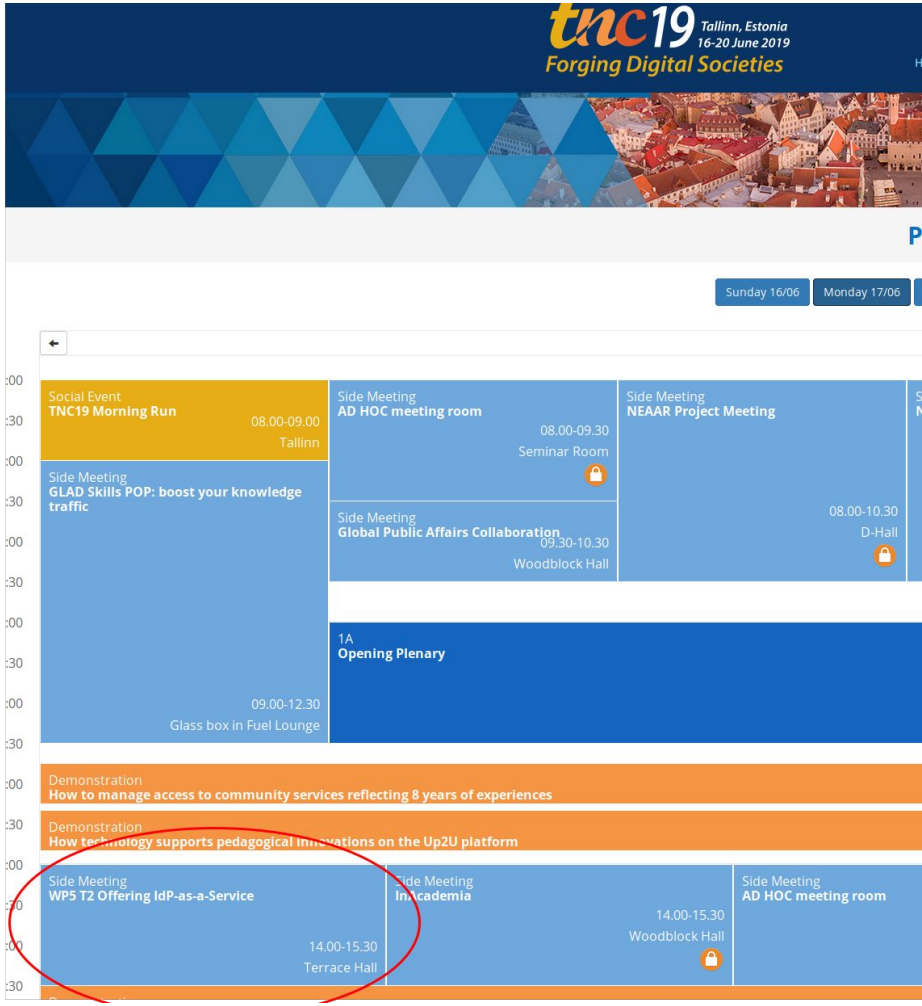
Trust & Identity Incubator lead
niels.vandijk@surfnet.nl

Initial Project Goals

- Continue work as was started in GN4-2 project
- Further develop software solution
- Work on business case for offering IdP as a Service solution
- Targeted at NREN level

Next up: Confirm with community @TNC2019

“No battle plan ever survives contact with the enemy.”



After community consultation at TNC2019

Two sets of responses:

- “Enable our institutions to make use of commercial tools”
- “Want to run a lightweight service for our institutions”

Impact on incubator:

- Current solution too heavy weight => Work terminated
- More focus needed on Minimal requirements for IdPaaS tool and the IdPs it delivers
- Is there a more lightweight solution?

IdP as a Service reference design

Platform requirements

- IdP Creation [IC]
- IdP Deletion [ID]
- IdP Management [IM]
- SP Management [SM]
- User Management [UM]
- Authentication & Authorization [AA]
- Software Deployment [SD]

IdP requirements

- Authentication [AU]
- Credential Handling [CH]
- Attribute release [AR]
- User management [UM]
- Metadata publishing [MP]
- Metadata consumption [MC]
- Logging [LO]
- Statistics [ST]
- Branding and contact data [BC]

https://wiki.geant.org/display/gn43wp5/IdP+as+a+service+reference+design

Lightweight hosted solution

- Identifier a lightweight hosted solution
- With an existing community

- Test and if needed contribute https://github.com/sitya/samlidp

Authentication [AU]

This category defines requirements for the authentication performed by the IdP.

ID	Requirement	Description	Configurable	samlidp.io
AU1	Handle SAML authentication	The IdP MUST be able to handle SAML2 authentication	No	DONE
AU2	Common standards	IdP MUST adhere to saml2int, and relevant eduGAIN profiles	No	DONE
AU3	No SAML1	IdP MUST NOT be able to handle SAML1 authentication	No	DONE
AU4	Identifier support	The IdP MUST support the following identifier types: • persistent nameid • transient nameid • ePPN • ePTID • subject ID	No	DONE
AU5	eduPerson support	The IdP MUST support the following eduPerson attributes: • DisplayName • Email • CN • SN • Name • edupersonScopedAffiliation • edupersonEntitlement	No	DONE
AU6	SCHAC support	The IdP MUST support the following SCHAC attributes: • schacHomeOrganisation	No	DONE
AU7	eduMember support	The IdP MUST support the following eduMember attributes: • IsMemberOf	No	MISSING
AU8	Force Authn	The IdP MUST support SAML Force authentication	No	DONE
AU9	SSO session time	The IdP MUST support SSO, session time must be configurable	Yes	DONE
AU10	Authentication Context	The IdP MUST support providing LoA information through Authentication Class Context ref	No	DONE

https://wiki.geant.org/display/gn43wp5/IdP+as+a+service+reference+implementation