

# 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](mailto:niels.vandijk@surfnet.nl)

**TRUST & IDENTITY**  
**INCUBATOR**

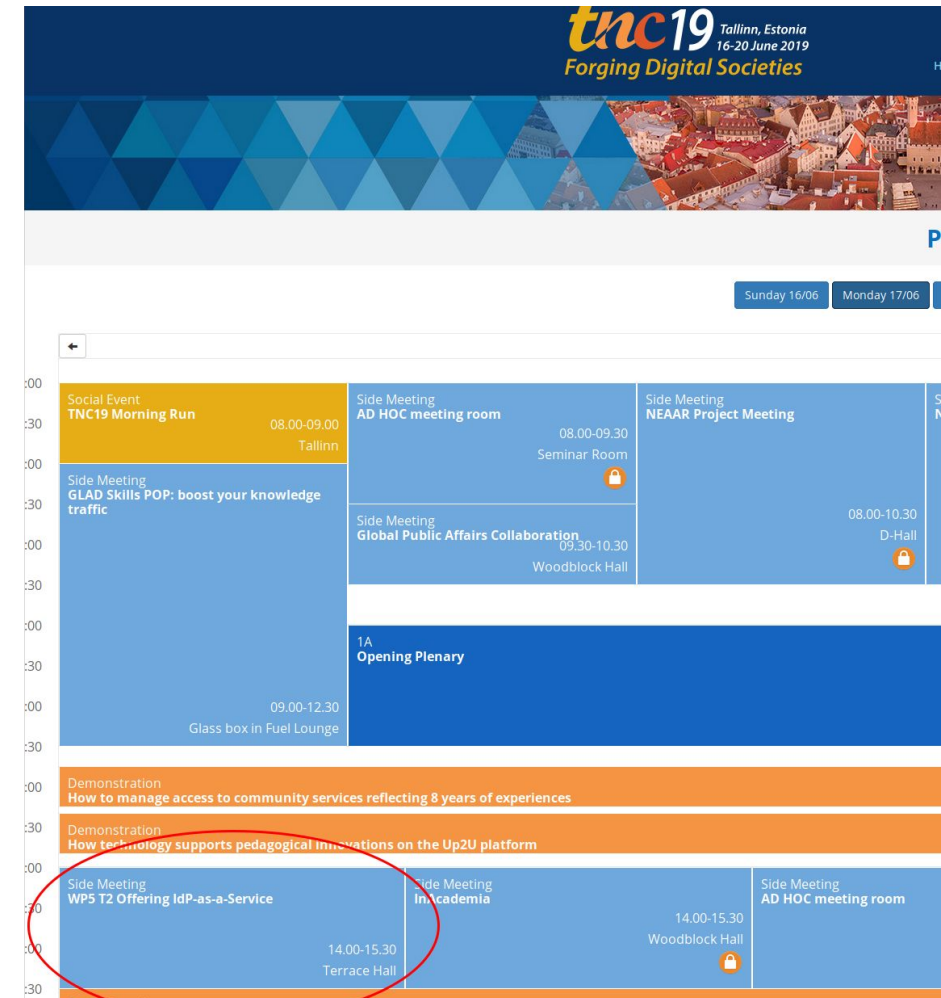


# Initial Project Goals

- 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.”



**tnc19** Tallinn, Estonia  
16-20 June 2019  
Forging Digital Societies

Sunday 16/06 Monday 17/06

Event	Time	Location
Social Event TNC19 Morning Run	08.00-09.00	Tallinn
Side Meeting AD HOC meeting room	08.00-09.30	Seminar Room
Side Meeting NEAAR Project Meeting	08.00-10.30	D-Hall
Side Meeting GLAD Skills POP: boost your knowledge traffic	09.00-12.30	Glass box in Fuel Lounge
Side Meeting Global Public Affairs Collaboration	09.30-10.30	Woodblock Hall
1A Opening Plenary		
Demonstration How to manage access to community services reflecting 8 years of experiences		
Demonstration How technology supports pedagogical innovations on the Up2U platform		
Side Meeting WPS T2 Offering IdP-as-a-Service	14.00-15.30	Terrace Hall
Side Meeting In Academia	14.00-15.30	Woodblock Hall
Side Meeting AD HOC meeting room		

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?



## 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>



- 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	<span>DONE</span>
AU2	Common standards	IdP MUST adhere to saml2int, and relevant eduGAIN profiles	No	<span>DONE</span>
AU3	No SAML1	IdP MUST NOT be able to handle SAML1 authentication	No	<span>DONE</span>
AU4	Identifier support	The IdP MUST support the following identifier types: <ul style="list-style-type: none"><li>• persistent nameid</li><li>• transient nameid</li><li>• ePPN</li><li>• ePTID</li><li>• subject ID</li></ul>	No	<span>DONE</span>
AU5	eduPerson support	The IdP MUST support the following eduPerson attributes: <ul style="list-style-type: none"><li>• DisplayName</li><li>• Email</li><li>• CN</li><li>• SN</li><li>• Name</li><li>• edupersonScopedAffiliation</li><li>• edupersonEntitlement</li></ul>	No	<span>DONE</span>
AU6	SCHAC support	The IdP MUST support the following SCHAC attributes: <ul style="list-style-type: none"><li>• schacHomeOrganisation</li></ul>	No	<span>DONE</span>
AU7	eduMember support	The IdP MUST support the following eduMember attributes: <ul style="list-style-type: none"><li>• IsMemberOf</li></ul>	No	<span>MISSING</span>
AU8	Force Authn	The IdP MUST support SAML Force authentication	No	<span>DONE</span>
AU9	SSO session time	The IdP MUST support SSO, session time must be configurable	Yes	<span>DONE</span>
AU10	Authentication Context	The IdP MUST support providing LoA information through Authentication Class Context ref	No	<span>DONE</span>

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