Idea for GN4

Purpose: This NIF form is to be used for the submission of New Ideas suggested for inclusion in the GN4 Phase1 and beyond proposals. Budget estimates, information about objectives, impact, benefits, etc. as well as scope must all be supplied.

Submit to: pmo@GÉANT.net by January 31st, 2014 with the subject label starting: GN4Input

Overview

Project Name:	OpenID Connect Federations	**Project Proposer:**	UNINETT, Andreas Åkre Solberg

Project Type: GN4 Phase1 or longer term	Longer term	**Estimated Project Costs (best effort!)**	
Duration proposed	2Y	Manpower in person-months also identifying specific expertise required	25MM Expertise with OpenID, SAML, Federations, Identity and trust frameworks.
Deliverables proposed (If any can be defined at this stage)	Final report.	Hardware and equipment:	Provided by participating partners.
Milestones proposed (If any can be defined at this stage)	Operational pilot	Other costs	Travel: 3500€

1 Background and Reasoning

In more recent time the NRENs community has shown increasing interest in OAuth, the open standard for authorisation. OAuth allows users to grant third-party access to their resources without sharing their passwords. OAuth 1 is an IETF RFC and the new protocol OAuth 2 is being standardised within the IETF.

A new technology, **OpenID Connect** has recently emerged; this technology integrates OAuth and OpenID 2.0 and offers a framework to share identities using RESTful APIs.

Compared to SAML 2.0, OpenID Connect is easier to integrate for Service Providers, and better support the more modern application architecture based upon HTTP APIs, mobile applications and cloud services.

OpenID Connect lacks the supporting protocols needed to build scalable federations, but supports the interfaces allowing it to be extended, and the idea is to propose such a trust framework with the necessary scalability.

2 Objectives, Impact and Benefits

Provide and implement a framework and necessary protocols to build federations using the OpenID Connect, allowing it to possibly replace the existing.

Learn from the experiences within GEANT of buidling the eduGAIN metadata service, and design a better more flexible framework.

Ensure that the framework is generic to involve more than just authentication, and support the generic nature of trusted HTTP APIs, including extension points.

Implement a proof of concept pilot that demostrates the scalability.

Document new use cases allowed to be realized by this new emerging standard given the new scalable trust framework.

3 Scope

Describe the areas expected to be covered or impacted by the proposed activity, such as organisational areas, systems, processes, resources.. i.e. what is 'in scope'. This is not a list of what will be done but identifying the services, areas or what, will be affected.

Also please enumerate specific items which although they could perhaps be related are intentionally not addressed by your proposal ("Out of Scope").

1. In Scope

- Simple implementation of a service, making use of existing software components
- Documentation and specifications of technical protocol / framework
- Contact and dialogue with the OpenID community and possible IETF about best effort

2. Out of Scope

- Integration with existing SAML 2.0 federations are out of scope
- Possible use of and extensions SAML 2.0 metadata for backward compatability is out of scope
- Any real services are out of scope. Proof of concept only.

4 General Information

OpenID Connect is a rather new technology involved with the obvious risks of the uncertain future. There are a lot of indicators that OpenID Connect has a future within the NRENs, and it also supports most NRENs increasing support and focus on APIs and cloud.

There has already been work within GEANT on OpenID Connect, and it would be reasonable to make use of the already established expertise, experience and contact with the OpenID Community.