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:	E-mail based discovery for Identity Federations	**Project Proposer:**	UNINETT Andreas Åkre Solberg

Project Type: GN4 Phase1 or longer term	Longer term	**Estimated Project Costs (best effort!)**	
Duration proposed	1Y	Manpower in person-months also identifying specific expertise required	14MM Expertise with WebFinger, SAML Protocols and Metadata, IdP Discovery.
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 2000€

1 Background and Reasoning

As Identity Federations grow and interconnect to other federations, the number of available Identity Providers for each service explodes. For technical reasons, the user will have to choose which provider to login from, before being able to provide username and password. Traditionally this user selection has been implemented as a drop-down list. This does not scale very well.

Previous attempts to approach this poor user experience of Identity federations is stilled based upon selection from a list. The rest of the Identity industry is using email based discovery. The idea is to attempt this approach in HE Identity Federations as well, although it requires some work, and some new ideas in order to work properly.

2 Objectives, Impact and Benefits

Email based discovery although require user input is much more reliable and scales far better compared to the traditional drop down list.

In the last few years, through among others, the OpenID protocol, users have started getting familiar to the fact that their email is their username, and can also be used for discovery.

In GEANT, there have earlier been efforts in Discovery, resulting in the product DiscoJuice. The idea is to further develop DiscoJuice to implement email based discovery, and at the same time introduce some new concepts that have earlier not been supported in HE Identity Federations, such as account switching, and remembering a set of user accounts earlier user. It should be investigated whether the technology behind industry solution accountchooser.com can be applied in HE in combination with email discovery.

When email is introduced in the discovery process, it should also be sent along to the Identity Providers, hinting towards the user's userid, and prefilling this, just leaving the password left to be entered. This requires further work, but will improve the user experience further.

3 Scope

1. In Scope

- Investigate the best available protocol for email to Identity Provider discovery protocol.
- Implement a fully working prototype extending the earlier produced GEANT DiscoJuice service.
- Demonstrate on a number of services that is connected to eduGAIN, demonstrating full use of the improved user experience.
- Possibly extending SAML protocol to embed email in the request, or at least some SAML software for demo purposes.

2. Out of Scope

- Legal concerns with regards to making the mapping of email to Identity Provider publicly available

4 General Information

There are a lot of alternative available protocols for generic email discovery. Not all are suited to scale up to the size of Identity Federations such as eduGAIN. DNS, XRD, OpenID, SAML 2.0 metadata and WebFinger are some of the technologies that should be considered.

In addition the DiscoJuice service should be trained, and remember mapping, and perform heuristic to improve the user experience in cases where thare are not direct match.