Simplified NIF for GN4 Input

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:	Affiliation Authority	**Project Proposer:**	Leif Johansson (SUNET), Per Nihlen (SUNET), Valter Nordh (SUNET)
Project Type: GN4 Phase1 or longer term	GN4 Phase1	**Estimated Project Costs (best effort!)**	
Duration proposed	6 months	Manpower in person-months also identifying specific expertise required	2 months of project management 6 months of software development (1-2 persons)
Deliverables proposed (If any can be defined at this stage)	An operational service for affiliation verification using eduGAIN.	Hardware and equipment:	Cloud hosting.
Milestones proposed (If any can be defined at this stage)	Service deployed and ready for use.	Other costs	Budget for 2 physical meetings: 4k EUR

1 Background and Reasoning

Provide background information and the context of the project. Explain the reason for the project. What do you want to be different? What do you hope to improve? Why is the project needed? This should be the reason for the project, not the solution.

The eduGAIN service provides a technical infrastructure for interfederation – connecting multiple federations to a common set of service providers - but for some specific use-cases connecting to eduGAIN is overly complex

compared to the problem being addressed.

Some of the most important use-cases are services that only want to verify the “studentness” of a user – the property of being an active student at an institution of higher learning. Examples of consumers of this attribute include Microsoft Dreamspark, student discount card companies (eg Mecenat), travel agents, etc.

Another possible use-case is the proposed mobile voice/data service consession being developed by GN3+ SA7 T5 which will need to provide a simple way for a mobile operator to verify that a prospective customer is a student.

This NIF proposes developing and operating a common service that can assert the “studentness” property over multiple technical interfaces including (but not limited to) regular SAML2int attribute assertions. The ***Affiliation Authority*** service is an interfederation (eduGAIN) relying party and a proxy identity provider.

In the GN3+ SA7T5 case the mobile operator would perform an authentication request to the Affiliation Authority and get a a successful authentication response with no attributes (!) only if the subject is a student or faculty member. It is possible to extend the service to release non-PII attributes in order to attest to (say) employee status. In essense this is a service that hides all attributes except the eduPersonScopedAffiliation.

There are several benefits of doing this:

1. Drive interfederation uptake by presenting a simple “killer app” service.
2. Make life easier for vendors offering discounts and other offers to the NREN sector.
3. One place to assign value to the “studentness” attribute.

The Affiliation Authority should be operated on a managed cloud service to ensure capacity and availability. The development work involved is very light. A simple service could be based on any of the SAML stacks that include proxy support (eg simpleSAMLphp or pysaml2).

2 Objectives, Impact and Benefits

Provide one or more bullet points to briefly describe the primary objective(s) of the project in terms of the desired outcomes. This should be expressed in the form: 'To ensure…', 'To implement…', 'To service...', 'To improve...', 'To innovate...', 'To optimize...', 'To save...', etc. For each objective mention the benefits to identified stakeholders (e.g. end-users, NRENs, large international research projects, industrial research partners, high level education, etc.) should be mentioned. A description of the expected overall impact must also be provided.

- to provide a single simple interface to the "studentness" attribute
- to enable collaboration with vendors that provide discounted services to students

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

- Software development

2. Out of Scope

- Any work on eduGAIN is out of scope – eduGAIN is basic infrastructure which is required by this service.
- Inventing new federation protocols.

4 General Information

Outline any potential issues, risks, dependencies, assumptions, constraints and limitations or any other points that may be useful to help assess the proposal.

The main risk is that IdPs don't release attributes to the Affiliation Authority. However since the only attribute needed is eduPersonScopedAffiliation which is not PII, this risk should be fairly low. Getting IdPs to configure attribute release will probably be helped by having a set of valuable services depend on the Affiliation Authority. We believe that it will be possible to get at least MSFT DreamSpark and Mecenat onboard as early adopters.

The goal is to produce something quick that is useful for key discount offerings. Future projects can develop the service depending on user need. This should probably turn into a service activity in SA2.