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:	Federation Operational Good Practices	**Project Proposer:**	Mikael Linden, Manne Miettinen – Funet
Project Type: GN4 Phase1 or longer term	Phase 1 and 2	**Estimated Project Costs (best effort!)**	
Duration proposed	Y1: preparations Y2: community consultation Y3 & Y4: adoption in federations and Home Organisations	Manpower in person-months also identifying specific expertise required	Preparing and community consultation: 18 (1 person editor 50% 5 persons support team 20%) Adoption: 18 (1 person flywheel 50% 10 persons deployment team 10%)
Deliverables proposed (If any can be defined at this stage)	Reference model for Federation operational good practices	Hardware and equipment:	none
Milestones proposed (If any can be defined at this stage)	None defined at this point	Other costs	Training and dissemination: € 10 000

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 services whose access identity federations are protecting are getting more sensitive (such as biomedical samples) and expensive (expensive research equipment that have an on-line interface). The service owners need to pay more attention to the information security requirements and risks related to their service's access control.

The service provider communities are getting more aware of this: "A pragmatic risk analysis of the use of identity federation from the point of view of a research infrastructure provider will be necessary to reassure the security officers at participating sites… Such a risk analysis should prioritise the various risks and hence focus available effort." [Eiroforum FIM4R group: Federated Identity Management for Research Collaborations. 23rd April 2012]

How the user identities are managed in the home organisation (Level of Assurance) is certainly part of those security considerations. However, also the operations of the identity federation is a potential security bottleneck, and a security breach in the federation operations can compromise the integrity and/or availability of access control in all connected Identity and Service Providers, including those connected via an interfederation service such as eduGAIN.

So far there has been no comprehensive good practice for information security for a federation operations. There are well-known practices for narrowly scoped topics, such as, how strong cryptographic keys should be used for federation configuration data (SAML2 metadata) signing, and how the availability of the service (such as SAML2 metadata delivery) can be quaranteed. However, integrity, availability and confidentiality of federation operations is a much wider topic and requires more holistic approach, covering also issues such as ensuring adequate resources and training the federation operational staff, having appropriate verification in place when registering Identity and Service Providers (SAML2 metadata updates), using appropriate measures to ensure the integrity of the federation operational environment (SAML2 metadata management) etc. The work item could also include an appropriate audit framework for the federation operations.

For public key infrastructure (PKI), there is a well-established industry practice of developing a Certificate Policy and Certification Practice Statement (CP/CPS) for operations of a Certificate Authority (CA). This work item proposes a similar approach for federation operations.

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 ensure that the integrity, availability and confidentiality of the NREN-operated identity federations meets the security requirements of international research infrastructures

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

- Developing and documenting practices necessary to guarantee integrity, availability and confidentiality of the federation operations service provided by the national identity federation
- Definin related audit framework
- Deploying the practices for pilot federations in the GÉANT community

2. Out of Scope

- Good practices for Home Organisations/Identity Providers (LoA)

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 proposed work item completes the proposed LoA work item
- There is a proposed related work item in the REFEDS workplan 2014: https://refeds.terena.org/index.php/REFEDS_Planning_Documents_2014
-

1.