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:	Incident Response for Federations	**Project Proposer:**	Per Nihlén and Leif Johansson (SUNET)

Project Type: GN4 Phase1 or longer term	GN4 Phase1	**Estimated Project Costs (best effort!)**	
Duration proposed	1 year (Year 1)	Manpower in person-months also identifying specific expertise required	Total of 16 person-months: 4 months of project management/Chair 6 months of ID Federation expertise (3 persons) 6 months of IRT expertise (3 persons)
Deliverables proposed (If any can be defined at this stage)	Architecture for Incident response handling in Federations	Hardware and equipment:	None
Milestones proposed (If any can be defined at this stage)	Month 1: Kickoff meeting and project plan ready. Month 3: First draft architecture document ready Month 6: Second draft architecture document ready Month 9: Validate architecture by deploying a small Proof of	Other costs	Travel budget for 4 project meetings (6 persons): 24k EUR

	Concept Month 12: Documentation and recommendation for further steps completed.		

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.

Identity federations are distributed virtual organizations operating shared, security-sensitive infrastructure. This begs the question of how Incident Response is done. To date incident response is typically not within the remit of even some large federations. This project will collaborate with the REFEDS-community to produce a common architecture for incident response and incident information sharing among federation operators. The project will collaborate with international emerging communities focused on information sharing and inter-CERT communications.

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 improve security and incident response in ID federation for consumers of high-assurance identities
- To identify key technical components (eg protocols and formats) that can be used to enable cross-federation information sharing related to security incidents.

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").

3.1 In Scope

- Profiling existing protocols (eg XMPP and IODEF) for transport of and expression of security incidents.

3.2 Out of Scope

- Changing federation policy & (inter)federation operations is explicitly out of scope. The project must design and develop solutions that can work with existing federation operational and policy practices.

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.

It is expected that this work will be organized as part of the JRA3 identity research activity.