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:	Smartcards & Second Factor Tokens	**Project Proposer:**	Per Nihlen och 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 15 person-months: 3 months of project management/Chair (1Person) 6 months of software engineering expertise (split over at most 3 people) 6 months of architecture expertise (split over 6 people)
Deliverables proposed (If any can be defined at this stage)	Contributions to existing opensource software. 2nd factor architecture for the R&E community.	Hardware and equipment:	Small budget for buying tokens (< 5k EUR)
Milestones proposed (If any can be defined at this stage)	Month 1: Kickoff meeting and project plan ready. Month 3: Identify key	Other costs	Travel budget for 6 project meetings: 60k EUR

	software gaps, First draft architecture document ready. Month 6: PoC ready using at least 2 2nd factor tokens types (separate vendors) w. http, Kerberos & ssh authentication. Month 12: Software gaps closed. Documentation finished. Reference architecture done.		

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 NREN community operates several services where key management for client access is becoming a critical factor. In the enterprise community 2nd factor tokens are typically deployed as a site- or enterprise-wide homogeneous infrastructure. In the R&E community the deployment of 2nd factor tokens have been hindered by the fact that most vendors in this space are focused on single-vendor solutions and vendor lock-in.

We have to recognize that it is impossible and not even desirable for the R&E sector to “pick a vendor” and that we must therefore find ways to break vendor-dependence and establish common infrastructure for 2nd factor tokens.

The goal of this task is to identify and close key technology gaps and arrive at a reference architecture for the use of 2nd factor tokens in the NREN community.

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 identify key technology gaps limiting the deployment of 2nd factor authentication for web, ssh and Kerberos (esp. MS Active Directory)
- to close the important technology gaps by implementing middleware, enabling software & services as open source
- to develop a reference architecture for the use of 2nd factor for web, ssh and Kerberos (esp. MS Active Directory)

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

- open source software & library development for MIT Kerberos, Heimdal, Microsoft Windows, OpenSSH and related tool chains.
- service specification and documentation
- reference architecture

3.2 Out of Scope

- picking a single vendor solution for 2nd factor tokens is to be avoided at all cost since the objective is to

avoid vendor lock-in!

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.

- There are very few people in the world who understand and can do the work needed. The project depends on access to these critical resources. These people are available in the R&E community so there is no need to look for external resources.

- This work should probably be organized either as part of the JRA3 identity research activity or as part of a new security research activity.