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:	Open HW HSM	**Project Proposer:**	Leif Johansson and Per Nihlén (SUNET)

Project Type: GN4 Phase1 or longer term	GN4 Phase 1 (with possible 1 year extension)	**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 (1 Person) 6 month of software development (1-2 persons) 6 months of hardware engineering expertise (1-2 persons)
Deliverables proposed (If any can be defined at this stage)	Prototype HSM Documentation	Hardware and equipment:	FPGA boards and Novena boards for prototyping and development work: ca 20k EUR
Milestones proposed (If any can be defined at this stage)	Month 1: Kickoff meeting and project plan ready Month 8: Have a working hardware setup Month 10: Version 0.5 of HSM software & hw Month 12: Version 1.0 of HSM software & hw.	Other costs	Travel budget for 4 physical project meetings: ca 20kEUR

	Documentation ready.		

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.

Recent revelations have called into question the integrity of some of the implementations of basic cryptographic functions and devices used to secure communications on the Internet. There are serious questions about algorithms and about implementations of those algorithms in software and particularly hardware.

The algorithmic issues are in the domain of the heavy math cryptography folk. But we must also deal with the implementation issues. The project is embarking on development of an open-source hardware cryptographic engine that meets the needs of high assurance Internet infrastructure systems that use cryptography. The open-source hardware cryptographic engine will be of general use to the broad Internet community, covering needs such as secure email, web, DNS, PKIs, etc.

The intent is that the resulting open-source hardware cryptographic engine can be built by anyone from public hardware specifications and open-source firmware. Anyone can then operate it without fees of any kind.

Leveraging on the work from the cryptech group we suggest building a prototype open HSM (Hardware Security Module) with the goal of integration with eduGAIN but also with other Identity Federations.

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 innovate a system to be used to increase the security in eduGAIN and other ID federations. Besides benefiting our whole community this work can be reused by our industrial partners.

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

- Software and (some) hardware development.

3.2 Out of Scope

- Developing client software for use with the HSM. All access will be based on PKCS11 standards. It is expected that this work with dovetail with cryptech development which means that most of the core FPGA coding will be done in cryptech. This implies that hardware work will mostly be limited to work on interfaces with the crypto FPGA cores.

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 could be organized either as part of the JRA3 identity research activity or as part of a new security research activity.