

# 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

<b>Project Name:</b>	RPKI BCP for NRENs	<b>Project Proposer:</b>	Leif Johansson and Per Nihlen (SUNET)
<b>Project Type:</b> GN4 Phase1 or longer term	GN4 Phase1	<b>Estimated Project Costs (best effort!)</b>	
<b>Duration proposed</b>	1 year (Year 1)	<b>Manpower in person-months also identifying specific expertise required</b>	Total of 14 person-months: 4 months of project management/Chair  10 months of security and network engineering expertise (6 persons)
<b>Deliverables proposed (If any can be defined at this stage)</b>	Workshop at the GN4 symposium to inform our community  Reference RPKI validation infrastructure  RPKI operational BCP documentation for NRENs	<b>Hardware and equipment:</b>	
<b>Milestones proposed (If any can be defined at this stage)</b>	Month 1: Kickoff meeting and project plan ready. Identify at least 6 pilot NRENs for enabling RPKI validation.  Month 3: Reference installation ready	<b>Other costs</b>	Travel budget for 4 project meetings: 30k EUR

	<p>Month 6: At least 3 pilot NRENs with at least 80% signed with RIPE</p> <p>Month 9: At least 6 pilot NRENs with at least 80% signed with RIPE</p> <p>Month 12: BCP documentation completed.</p>		
--	---	--	--

## 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.*

“RPKI provides a way to connect Internet number resource information (such as Autonomous System numbers and IP Addresses) to a trust anchor. The certificate structure mirrors the way in which Internet number resources are distributed. That is, resources are initially distributed by the IANA to the Regional Internet Registries (RIRs), who in turn distribute them to Local Internet Registries (LIRs), who then distribute the resources to their customers. RPKI can be used by the legitimate holders of the resources to control the operation of Internet routing protocols to prevent route hijacking and other attacks. In particular, RPKI is used to secure the Border Gateway Protocol (BGP) through BGPSEC, as well as Neighbor Discovery Protocol (ND) for IPv6 through the Secure Neighbor Discovery Protocol (SEND).” -- From Wikipedia

The objective of this activity to setup and configure a reference infrastructure for RPKI relying party (validation) suitable for the NREN community as well as providing operational Best Current Practice documentation. We also foresee that this task will provide RPKI expertise to help pilot NRENs enable RPKI validation.

## 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 deliver a reference architecture for RPKI validation and operational BCP documentation which will benefit the security of the NREN network connectivity services.

## 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

As RPKI is established technology there should be little need for development work. Therefore the scope is limited to:

- Documentation and best-practice work.
- Developing operational experience with RPKI validation technology.

### 3.2 Out of Scope

- As RPKI is established technology there should be little need for development work.
- Operating root CAs is also out of scope – it is expected that this work will focus on using the existing RIPE CA to sign our ROAs

## 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 RPKI is stable technology that is being deployed to protect the global routing system. Unfortunately the NREN community has been very slow in deploying RPKI. This is doubly problematic since some NRENS are very old entities and therefore have so called “legacy” (eg pre-RIPE) delegations. These delegations is the focus of debate in the NRO (number resource organization) community and arguably RPKI is an added axes of control that will influence the way legacy delegations are managed in the future. The NREN needs to be on top of this in order to maintain control over our very valuable resources, the ipv4 delegations. Deploying technologies like RPKI is an important part of being active in the Internet community. This work should probably be organized as part of a network-related service-activity or as part of a new security service or research activity.

