

AUTHORS' DATA:

Name: Roque Gagliano

e-mail: rogaglia@cisco.com

Organization: Cisco

PROPOSAL DATA:

Policy Proposal Title: Requirement to sign up for RPKI when requesting additional resources

Policy Proposal Type: LACNIC

Id: LAC-2012-11

Version: 2

PROPOSAL SUMMARY:

This proposal seeks to require that any organization requesting additional resources from LACNIC must previously have signed up their resources in the RPKI system. To meet this requirement, the organization must have one or more certificate authorities registered in LACNIC's system; one or more RPKI certificates covering all its resources; if applicable, one or more ROAs covering all non delegated resources; and one or more public repositories where this information is freely available.

RATIONALE:

The current RPKI implementation requires members to complete a series of minimum steps in LACNIC's management system. The RPKI adoption process often faces operational issues. Typically, for instance, the person operating the network can not be the same person that uses LACNIC's system.

In addition, as with any registration system, RPKI suffers from the issue of the aging of stored information. This proposal provides the registration system with a tool that allows requiring an assessment of RPKI information each time an organization contacts LACNIC to request additional resources. Similar tools already exist in LACNIC's policy manual for Whois and reverse DNS registration.

This policy proposal will achieve several objectives:

- It will alleviate the issue of the aging of the information contained in the RPKI registry.
- It will encourage the production of cryptographic material in RPKI.
- It will educate on RPKI and security in the global routing system.

Provided that they have an information management system in place, the cost for operators will be insignificant (a few clicks on LACNIC's system).

Costs for LACNIC should be minimal, as the implementation of this policy does not require changes in its management systems.

PROPOSAL TEXT:

Section 2.3.4.

(The text below would be added as paragraph 8 and the following paragraph renumbered as number 9)

8- Applicants' RPKI certification system records must be up to date. For this they must have:

- a. one or more certifying entities registered in LACNIC's RPKI system;
- b. one or more valid RPKI certificate authority (CA) certificates (according to RFC 6487) covering all its resources.

If applicable, applicants will be required to verify that they have:

- c. one or more well-formed ROAs (according to RFC 6482) covering all non-delegated resources;
- d. one or more public repositories that satisfy RFC 6481 where this information is freely available.

IPv6: Section 4.5.2.1. Subsequent Allocation Criteria

The following text would be added:

Applicants' RPKI certification system records must be up to date. For this they must have:

- a. one or more certifying entities registered in LACNIC's RPKI system;
- b. one or more valid RPKI certificate authority (CA) certificates (according to RFC 6487) covering all its resources.

If applicable, applicants will be required to verify that they have:

- c. one or more well-formed ROAs (according to RFC 6482) covering all non-delegated resources;
- d. one or more public repositories that satisfy RFC 6481 where this information is freely available.

ADDITIONAL INFORMATION:

Timetable: Immediate implementation.

References:

Changes since previous version:

- Requesting ROAs and repositories is no longer mandatory, as reasons may exist for not publishing ROAs (e.g., non-public networks).
- Added normative references as agreed on the mailing list.
- Added the motivation having to do with the aging of the information.