About

Resource Certification is a security framework for verifying the association between Internet number resources (Internet addresses and/or Autonomous System Numbers) and their rightful holders.

It is aimed to add a verifiable form of a holder's current right to use those resources over the Internet. An important component of the resource certification framework is the resource Public Key Infrastructure (RPKI) based on the Internet resources management hierarchy.

Since 2006, AFRINIC has been working with other RIRs on the resources certification activity, while also following the development of the standards in the Secure Inter-Domain Routing (SIDR) Working Group at
the IETF.. http://tools.ietf.org/wg/sidr/

AFRINIC is providing a system with basic features, to be expanded over time in a phased deployment plan. Certification will be offered through a hosted environment via the MyAfriNIC portal. Members are able to sign ROAs and view their certificates. The system takes care of all the crypto operations such as certificate requests and renewals, re-keys and objects publication in the repository (rsync://rpki.afrinic.net). Access to the resource certification sub-section requires a Business Public Key Infrastructure (BPKI) certificate.

What can you do with your RPKI certificate?

Resource certificates can be used for various purposes:

- Prove the right to use resources
- Sign Route Origin Authorisations
- Sign Internet Routing Objects
- Prove ownership of Internet number resources in the context of IPv4 transfer after the exhaustion of the IPv4 pool of the RIR
- Help to secure the inter-domain routing protocol by conveying the right-to-use of the resources and to validate routing information

Technical background

Resource Certificates are based on the X.509 certificate format (RFC 5280). The format has been extended by the IETF standard, (RFC 3779) to include IP address and AS numbers in a critical certificate extension. These certificates are then published and bound together in a verifiable way in the RPKI. The resource certificates are not identity certificates and can only be

used by specialised applications and services that are related to verification of an entity's rights to use an IP address or AS number.

AFRINIC has invested significant resources in the developement of its own in house system based on the APNIC RPKI code. A basic version of the system will evolve during the year in phases. These phases include the extension of the "up/down" protocol, the sub-certification, and the migration to a single Trust Anchor (TA).

To use the system

1. Activate your account on MyAFRINIC if you have not done so before.

2. Enroll your BPKI certificate.

3. Navigate to Resources Certification under Resources.

RPKI codes and tools

AFRINIC RPKI repository:
rsync://rpki.afrinic.net
https://rpki.afrinic.net

Statistics
Global statistics
Daily validation details of objects in AFRINIC RPKI repository

Validators
RIPE NCC Validator
RPKI.net rcynic Validation Tool
RPSTIR - BBN Validation Tool

Implementation of RPKI tools
RPKI.net Open Source

Related links
BGP Secure Routing Extension (BGP-SRx) – RPKI for Quagga
RPKI Origin Validation Looking Glass

Resource certification at other RIRs

- APNIC: http://www.apnic.net/services/services-apnic-provides/resource-certification.
- RIPE NCC: http://www.ripe.net/certification/
- LACNIC: http://lacnic.net/en/rpki/index.html
- ARIN: https://www.arin.net/resources/rpki.html

Questions

If you have any questions, please send a mail to rpki-help[at]afrinic.net.

There is a mailing list rpki-discuss[at]afrinic.net to discuss RPKI services.