

APNIC Resource Certification Service

Tuan Nguyen

APNIC

Issue Date: [31 May 2014]

Revision: [4]



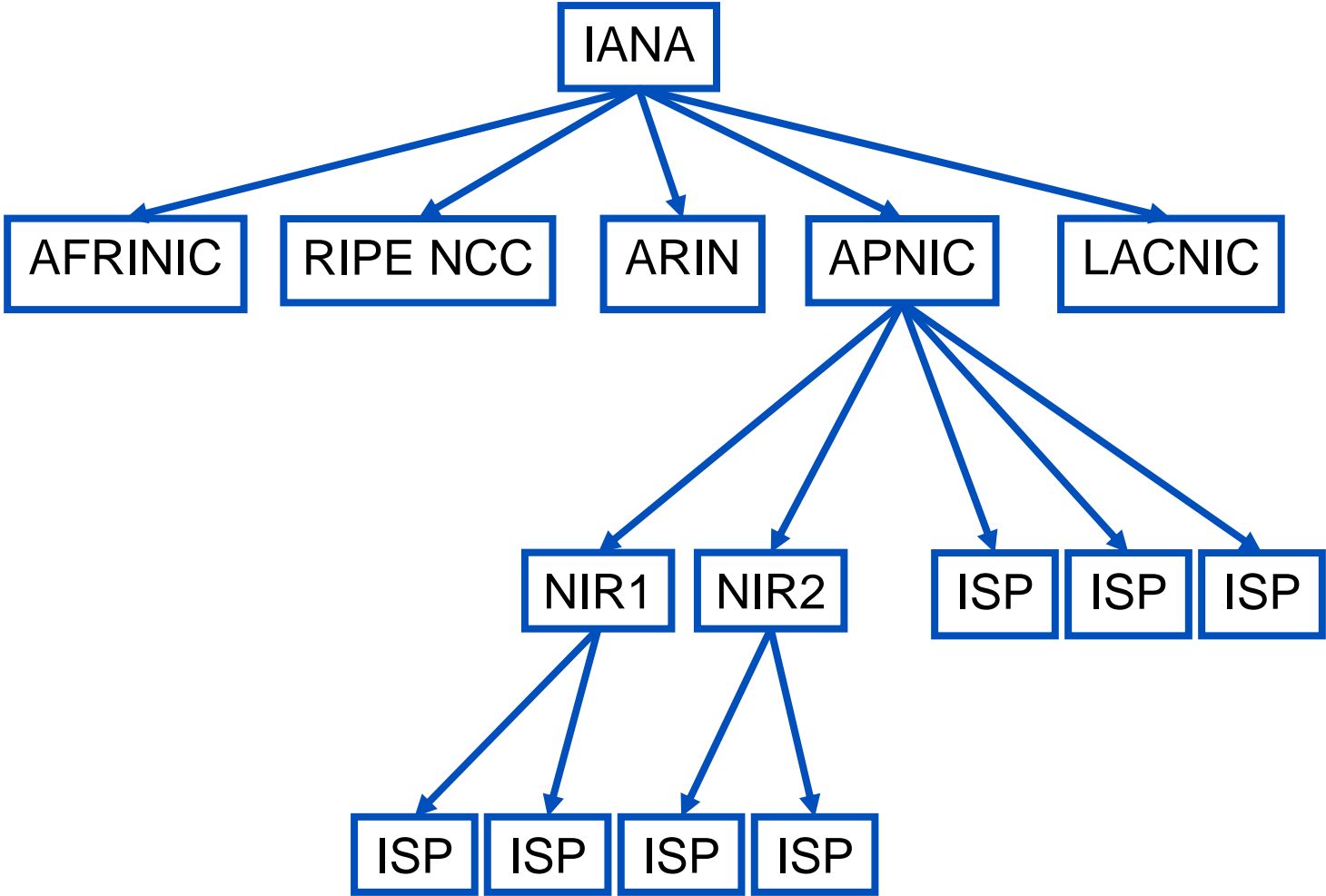
Internet Routing Security

- Routing security is essential to integrity of the Internet
 - Need to improve security of inter-domain routing
- Who has the authority to advertise information into the routing system?
- The majority of network relationships are based on system of mutual trust
 - Each party trusts that routes used to transmit information are safe
- The trust model is increasingly open to potential abuse and attack

About RPKI

- An architecture to support improved security of Internet routing using PKI infrastructure
- A robust security framework for verifying the association between resource holders and their Internet resources
 - “Cryptographically verifiable attestations” for IP address delegations and their use
- This architecture is called Resource Public Key Infrastructure (RPKI)

Resource Delegation Hierarchy



About RPKI

- “Trustable authority” mirrors the administrative resource allocation hierarchy with certificates that match current resource delegations
- A resource holder operating a sub-delegation registry (for example, an LIR) may use an RPKI system to generate certificates that correspond to these delegations
 - Grant a unique “right-of-use” for the associated set of IP resources

About RPKI

- These certificates are called resource certificates and they conform to X.509 PKIX standards
- RPKI is not used to validate attestations of an individual's identity or that individual's role, but as a means to **validate** that person's **authority** to use IP address resources
- An RPKI resource certificate is required to enable a resource holder to issue "Route Origination Authorizations" (ROAs)

What is a ROA?

- It is a digital object that contains a list of address prefixes and one AS number
- It is an authority created by a prefix holder to authorize an AS number to originate one or more specific route advertisements
- It does not contain any routing policy information, nor does it convey whether or not the AS holder has even consented to actually announce the prefix(es) into the routing system

APNIC's RPKI Service

- Enhancement to the RIRs
 - Offers verifiable proof of resources holdings
- Resource certification is an opt-in service
 - Resource holders choose to request a certificate and provide their public key to be certified
- APNIC has integrated the RPKI management service into MyAPNIC for APNIC Member use

What you need to know

- You are encouraged to experiment, test, play and develop
 - For example, you can create your ROAs
- RPKI standards are still being developed, and the operating environment for RPKI use is still fragile
- It's ready for testing and prototyping, but is probably not ready for production use just yet
- Please tell us what you find but don't rely on it in your network yet

MyAPNIC - Resource Certification Service

MyAPNIC-Resource Certification

MyAPNIC

APNIC

[Login](#) [Register](#)

MyAPNIC

MyAPNIC

Please enter your username and password below to access your membership information online.

Login

Username: *

Password: *

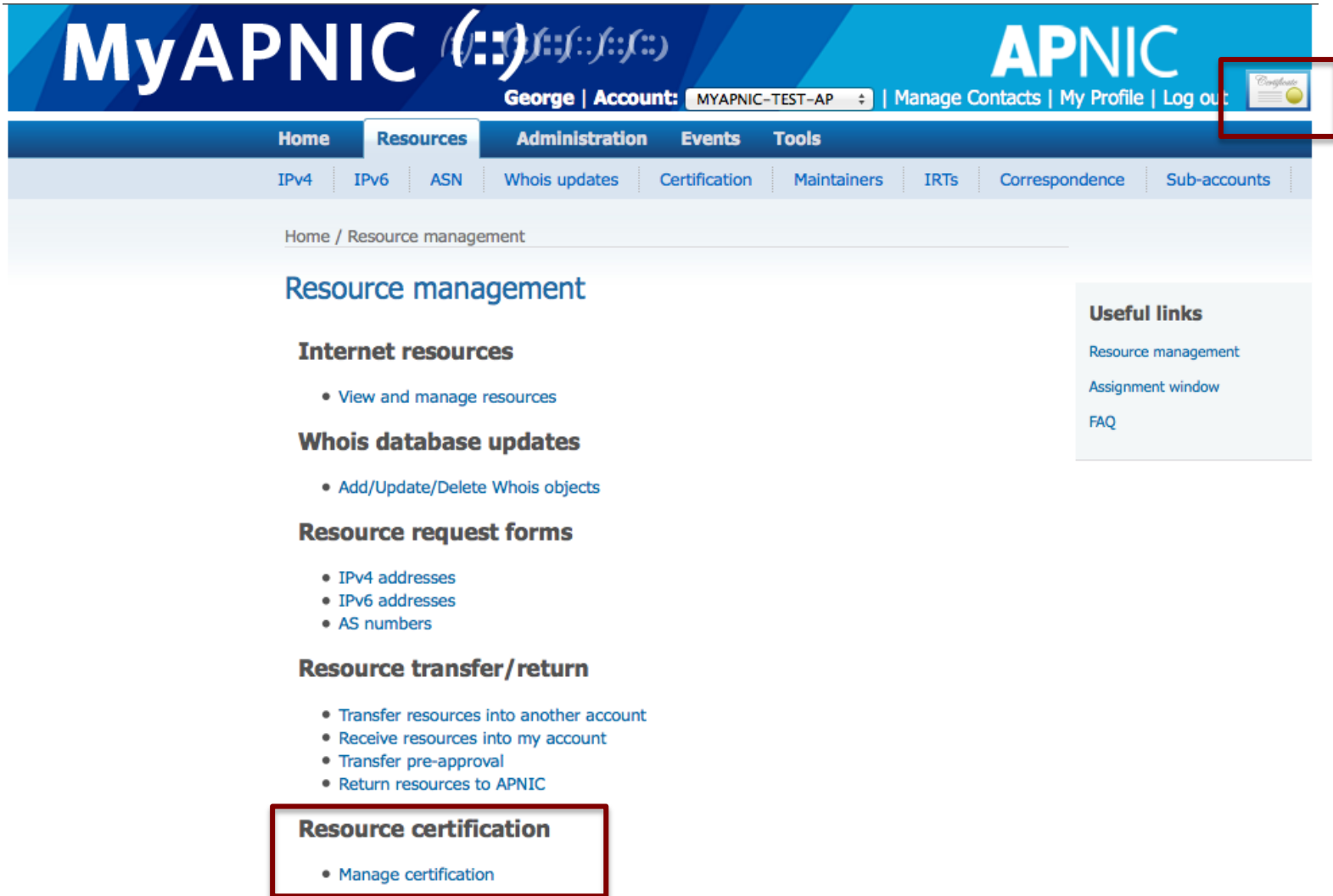
[Sign In](#)

[Forgot your login information? click here](#)

Don't yet have access to MyAPNIC?
[Click here](#) to register.

© Tuesday, 08-Apr-2014 15:16:15 EST APNIC | [Feedback](#) | [About MyAPNIC](#) | [Need help?](#)

MyAPNIC-Resource Certification



The screenshot shows the MyAPNIC website interface. At the top, the MyAPNIC logo is on the left and the APNIC logo is on the right. The user's name 'George' and account 'MYAPNIC-TEST-AP' are displayed in the center. Navigation links include 'Manage Contacts', 'My Profile', and 'Log out'. A small profile picture icon is highlighted with a red box in the top right corner.

The main navigation menu includes 'Home', 'Resources', 'Administration', 'Events', and 'Tools'. The 'Resources' menu is expanded to show 'IPv4', 'IPv6', 'ASN', 'Whois updates', 'Certification', 'Maintainers', 'IRTs', 'Correspondence', and 'Sub-accounts'. The 'Certification' link is highlighted.

The breadcrumb trail reads 'Home / Resource management'. The main heading is 'Resource management'. Underneath, there are several sections:

- Internet resources**
 - View and manage resources
- Whois database updates**
 - Add/Update/Delete Whois objects
- Resource request forms**
 - IPv4 addresses
 - IPv6 addresses
 - AS numbers
- Resource transfer/return**
 - Transfer resources into another account
 - Receive resources into my account
 - Transfer pre-approval
 - Return resources to APNIC
- Resource certification** (highlighted with a red box)
 - Manage certification

On the right side, there is a 'Useful links' section with links to 'Resource management', 'Assignment window', and 'FAQ'.

MyAPNIC-Resource Certification

Home / Resources / RPKI

RPKI

Enable Resource Certification

Currently, you have not enabled resource certification for your registry.

- I want to operate in the MyAPNIC RPKI portal.
- I want to host my own certification authority and run an RPKI engine myself.

Next

MyAPNIC-Resource Certification

Home / Resources / RPKI

RPKI

Enable Hosted Resource Certification

Currently, you have not enabled resource certification for your registry.

Terms and Conditions of APNIC Certification Authority

Introduction

APNIC publishes all Certificates, Certificate Revocation Lists (CRLs), and RPKI-signed objects in the Certification Repository ("**Repository**"). The Repository is available to anyone under these Terms and Conditions.

Article 1 - Definitions

In the Terms and Conditions, unless the context requires otherwise, the following terms have the meanings assigned to them below:

[I accept. Create my Certification Authority](#)

MyAPNIC-Resource Certification

[Home](#) / [Resources](#) / [RPKI](#)

RPKI

Activating engine, please wait...



MyAPNIC-Resource Certification

Home / Resources / RPKI

RPKI

ROA Configuration

Origin ASN Prefix Max Length

61.45.248.0/23

All Changes Items per page Search by AS or IP...

Origin AS	Prefix	Max Length
No data available in table		

Showing 0 to 0 of 0 entries

Certified Resources

- 61.45.248.0/23
- 61.45.251.0/24
- 61.45.252.0/22

More RPKI Information

- Securing BGP
 - *The Internet Protocol Journal, Volume 14, No. 2*
- An Infrastructure to Support Secure Internet Routing
 - *RFC6480*
- A Reappraisal of Validation in the RPKI
 - labs.apnic.net/blabs
- An Introduction to Routing Security (and RPKI tools)
 - labs.apnic.net/presentations/store/2013-05-13-rpki.pdf
- MyAPNIC Resource Certification Guide
 - www.apnic.net/myapnic

Questions or Comments?

THANK YOU



www.facebook.com/APNIC



www.twitter.com/apnic



www.youtube.com/apnicmultimedia



www.flickr.com/apnic



www.weibo.com/APNICrir