Resource Certification (RPKI)

Making BGP more secure

SEE2 - Macedonia

The RIPE NCC involvement in RPKI

- The authority on who is the registered holder of an Internet Number Resource in our region
  - IPv4 and IPv6 Address Blocks
  - Autonomous System Numbers

- Information is kept in the Registry

- Accuracy and completeness are key

Digital Resource Certificates

- Based on open IETF standards (sidr)
  - RFC 5280: X.509 PKI Certificates
  - RFC 3779: Extensions for IP Addresses and ASNs
  - RFC 6481-6493: Resource Public Key Infrastructure

- Issued by the RIRs since 1 January 2011

- State that an Internet number resource has been registered by the RIPE NCC

Digital Resource Certificates

- Resource Certification is a free, opt-in service
  - Your choice to request a certificate
    - Linked to registration
    - Renewed every 12 months

- Enhancement to our Registry
  - Offers validatable proof of holdership

RIPE
NCC

Management: Your Choice

- Open Source Software to run a member CA
  - Use the RIPE NCC as parent CA (trust anchor)
  - Generate and publish Certificate yourself

- RIPE NCC Hosted Platform
  - All processes are secured and automated
  - One click set-up of Resource Certificate
  - WebUI to manage Certificates in LIR Portal

Using RPKI for
BGP Origin Validation

Certification to Secure Internet Routing

- Members can use their resource certificate to make statements about their BGP Routing

  Route Origin Authorisation (ROA):

  "I authorise this Autonomous System to originate these IP prefixes"

- Also in the ROA: Maximum Prefix Length
  - The smallest prefix the ASN may announce

Route Origin Authorisations

- A ROA affects the RPKI validity of a BGP route:

  - VALID: ROA found, authorised announcement

  - INVALID: ROA found, unauthorised announcement

  - UNKNOWN: No ROA found (resource not yet signed)

Every operator is free to base any routing decision on these three validity states

Demo

Using the hosted system...
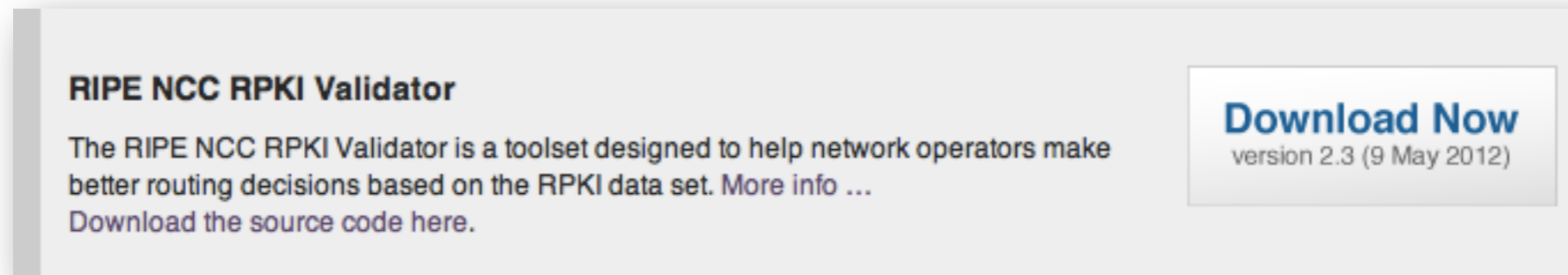
Making routing decisions

using the RIPE NCC RPKI Validator

Validation in Practice

- All certificates and ROAs are published in a repository and available for download

- Software running on your own machine will periodically retrieve and verify the information
  - Cryptographic tools check all the signatures

- The result is a list of all valid combinations of ASN and prefix, the "validated cache"

The RIPE NCC RPKI Validator toolset

- http://ripe.net/certification/tools-and-resources

RIPE NCC RPKI Validator

The RIPE NCC RPKI Validator is a toolset designed to help network operators make better routing decisions based on the RPKI data set. More info …
Download the source code here.

Download Now
version 2.3 (9 May 2012)

- Requires Sun Java 1.6 and rsync

- No installation required

  - Unzip the package

  - Run the program: `./bin/rpki-validator`

- Web-interface available on localhost port 8080

The RIPE NCC RPKI Validator toolset

Demo

Using the RPKI Validator...

RPKI support in routers

- The RPKI-RTR Protocol is an IETF Internet Draft

- Production Cisco Support:
  - ASR1000, 7600, ASR903 and ASR901

    in releases 15.2(1)S or XE 3.5

- Cisco Early Field Trial (EFT):
  - ASR9000, CRS1, CRS3 and c12K (IOS-XR)

- Juniper has support since version 12.2

- Quagga has support through BGP-SRX

Router Configuration – Cisco

```
!
route-map rpki-loc-pref permit 10
 match rpki invalid
 set local-preference 90
!
route-map rpki-loc-pref permit 20
 match rpki not-found
 set local-preference 100
!
route-map rpki-loc-pref permit 30
 match rpki valid
 set local-preference 110
```

Public Testbeds

- RIPE NCC has a Cisco:
  - Telnet to rpki-rtr.ripe.net
  - Username: ripe, no password
- Kaia Global Networks have a Juniper:
  - Telnet to 193.34.50.25
  - Username: rpki, password: testbed

- http://ripe.net/certification/router-configuration

Information and Announcements

http://ripe.net/certification

#RPKI

Questions?

✉ certification@ripe.net

✉ alexb@ripe.net

🐦 @alexander_band

RIPE NCC