Resource Certification (RPKI)

Marco Hogewoning
RIPE NCC
(marcoh@ripe.net)

MENOG 10, Dubai UAE

Resource Certificates – The Goal

- Issue digital certificates along with the allocation of Internet Resources

- Two main purposes:
  - Make the Registry more robust
  - Make Internet routing more secure

- Validation is the added value

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

Discussion in Tech Community since 1990s

- Aug 1998: IDR Working Group at IETF 42
  - BGP is vulnerable to attacks due to the lack of a scalable means of ensuring the authenticity and legitimacy of BGP control traffic
- Feb 2000: Secure Border Gateway Protocol
  - Real World Performance and Deployment Issues; paper by S. Kent, C. Lynn, J. Mikkelson, and K. Seo
- Sept 2003: IETF Internet Draft
  - X.509 Extensions for IP Addresses and AS Identifiers

Digital Resource Certificates

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

- Certificate does not list any identity information

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

How to Secure Routing

- Using the resource certificate the holder can make a statement on how those resources should be routed:

“I, the certified holder, authorise this Autonomous System to announce the route for these prefixes”

Route Origin Authorisations

- Only the registered holder of a Internet number resource can create a valid ROA
- A ROA affects the RPKI validity of a route announcement:
  - VALID: ROA found, authorised announcement
  - INVALID: ROA found, unauthorised announcement
  - UNKNOWN: No ROA found (resource not yet signed)

Publication of Cryptographic Objects

- Publication is distributed by design
  - Publish yourself or publish through a 3rd party
- Each RIR has a public repository
  - Holds Certificates, ROAs, etc.
  - Refreshed at least every 24 hrs
- Accessed using a Validation tool
  - Communication via rsync
  - Builds up a local validated cache

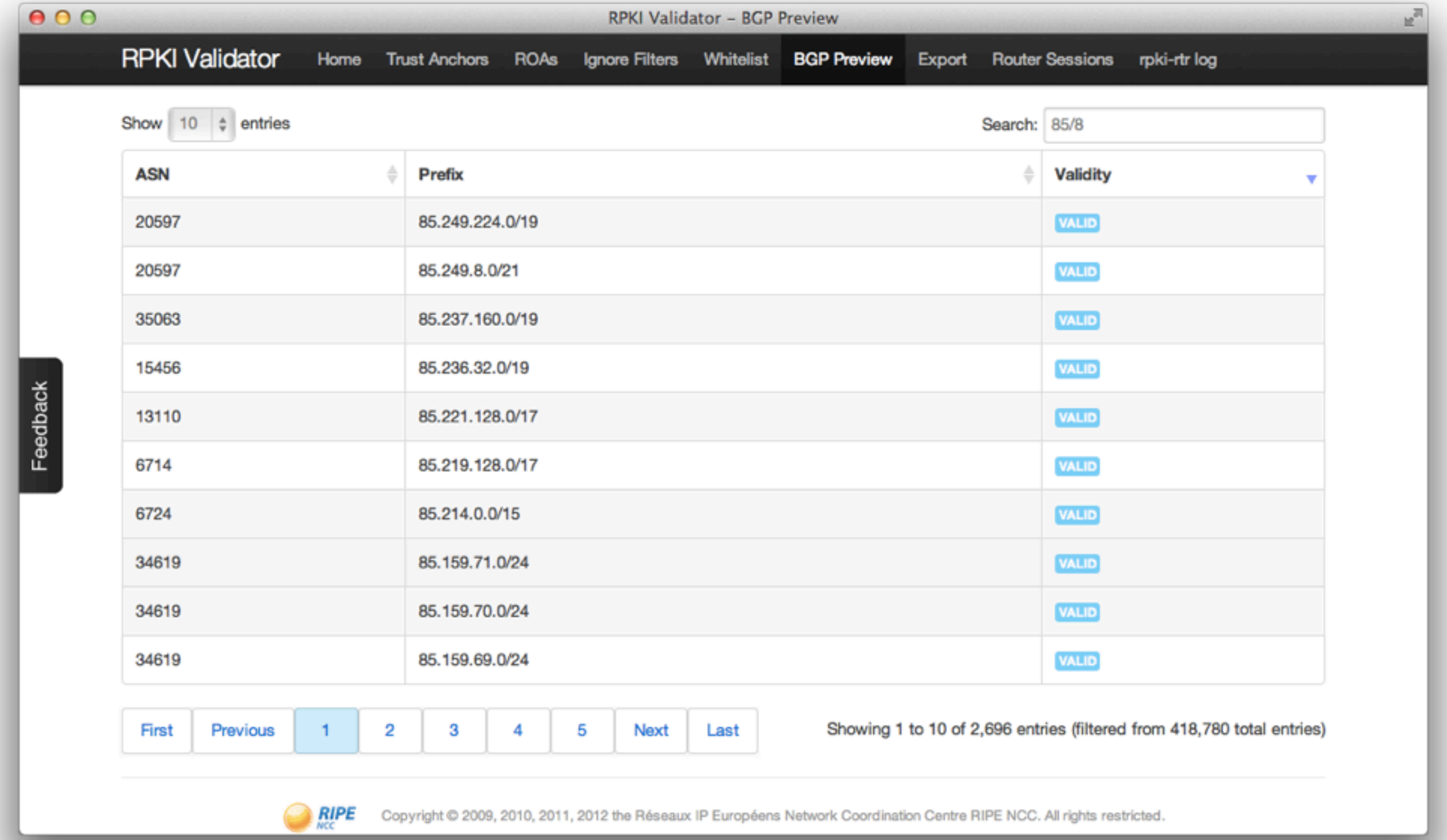
RIPE NCC RPKI
Validation tool

RIPE NCC RPKI-RTR Validator

- Web-based user interface
- Periodically validates all ROA repositories
  - Downloads and processes changes automatically
- Ignore Filters (Apply RPKI status ‘Unknown’)
- Whitelist (Apply RPKI status ‘Valid’)
- RPKI-Router Support
  - Cisco, Juniper, Quagga...

Open source, BSD License

RIPE NCC RPKI Validator 2.0.3



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
```

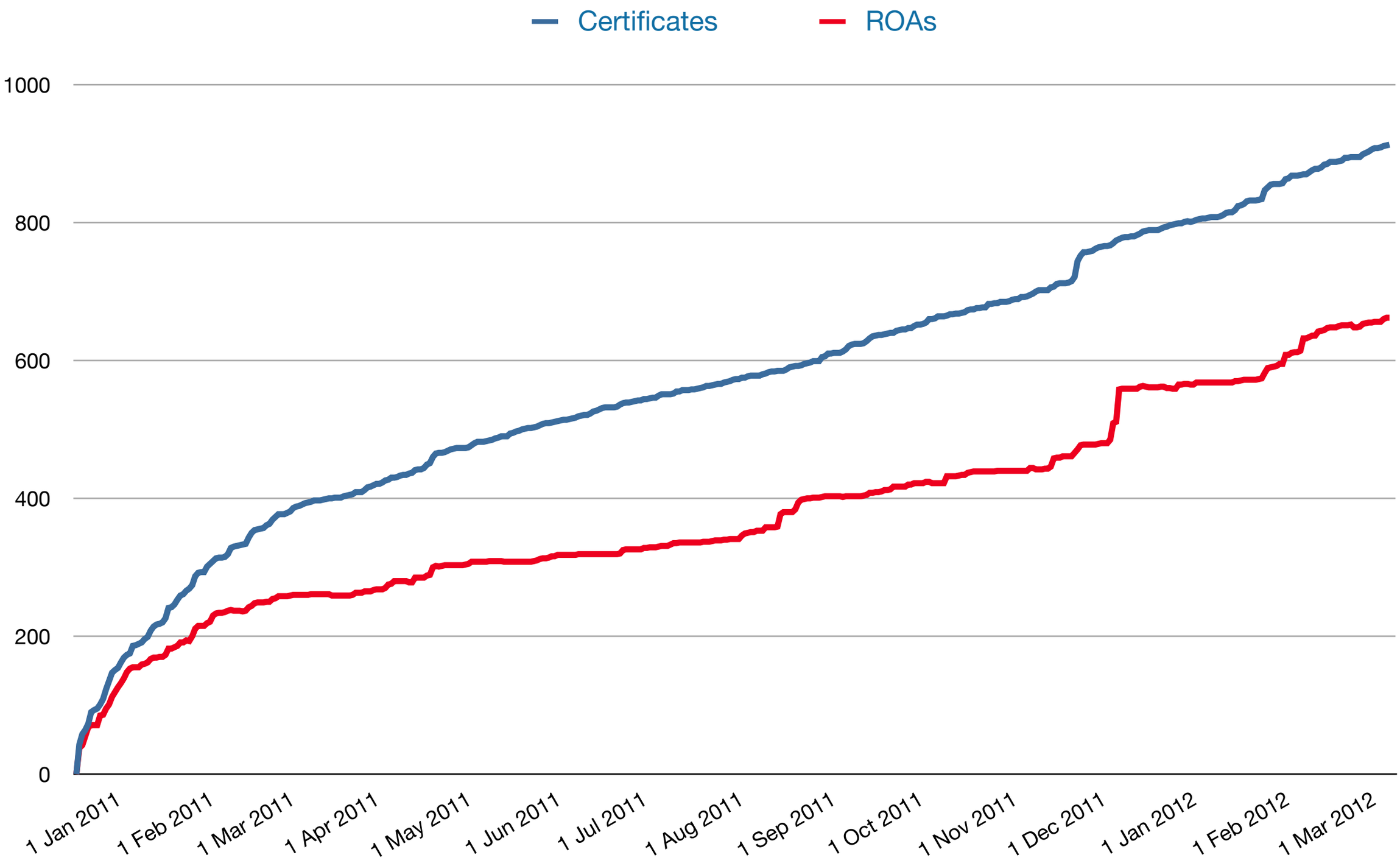
Router Configuration – Juniper

```
policy-options {
    policy-statement route-validation {
        term valid {
            from {
                validation-state valid;
            }
            then {
                local-preference 110;
                validation-state valid;
                accept;
            }
        }
        term invalid {
            from {
                validation-state invalid;
            }
            then {
                local-preference 90;
                validation-state invalid;
                accept;
            }
        }
        term unknown {
            from {
                validation-state unknown;
            }
            then {
                local-preference 100;
                validation-state unknown;
                accept;
            }
        }
    }
}
```

RPKI Capable Test Routers

- Cisco
  - rpki-rtr.ripe.net
  - telnet username: ripe, no password
  - “sh ip bgp 193.0.24.0/21 (or your prefix)”, “sh ip bgp rpki table”, “sh ip bgp ipv6 unicast rpki table”, “sh ip bgp rpki server”
- Juniper
  - juniper.rpki.netsign.net
  - telnet username: rpki, password: testbed
  - “show validation session detail”, “show validation statistics”, “show validation database”, “show route protocol bgp validation-state valid”

Resource Certification Adoption



Latest News

- RIPE NCC Validator 2.1.0 released 24-04-2012
  - Interface improvements
- Cisco has production releases for RPKI
  - 7600, ASR 1000, ASR 901, ASR 903
  - IOS 15.2(1)S or XE 3.5
- Early Field Trial for other platforms
  - CSR 1, CSR 3, ASR 9000, c12K (IOS-XR)
  - Contact Cisco or RIPE NCC when interested

Information and Announcements

http://ripe.net/certification

#RPKI