

# Background on Resource Certification

---

Alex Band  
RIPE NCC



# Internet Routing

---

- Routing is non-hierarchical, open and free
- Freedom comes at a price:
  - You can announce any address block on your router
  - Accidental errors happen frequently, impact is high
    - Entire networks become unavailable
  - Malicious attacks are relatively easy
    - Mitigation requires intervention from operators

# Discussion in Tech Community since 1990s

---

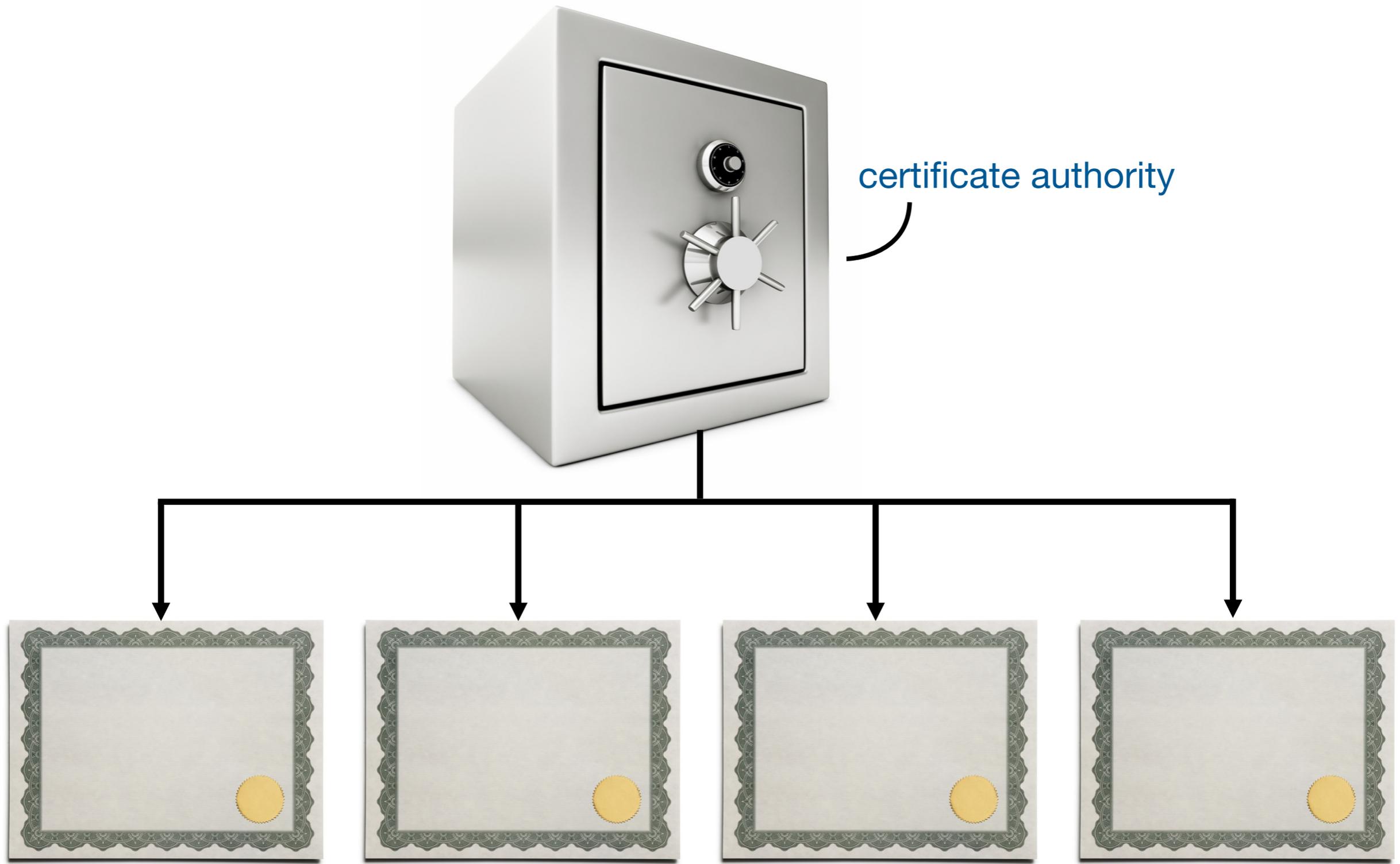
- Aug 1998: IDR Working Group at IETF 42
  - BGP is vulnerable to attacks due to the lack of a scalable means of ensuring the authenticity and legitimacy of BGP control traffic
- Feb 2000: Secure Border Gateway Protocol
  - Real World Performance and Deployment Issues; paper by S. Kent, C. Lynn, J. Mikkelsen,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

# A RIPE NCC Activity Since 2006

---

- ripe-365 – RIPE NCC Activity Plan 2006
  - “The RIPE NCC will support its members and the Internet community to better secure the inter-domain routing system. As part of this support, the RIPE NCC will improve the quality of Internet number resource distribution data.”
- ripe-364 - RIPE NCC Budget 2006
  - “the expenses for Membership Services show an increase due to the new activity to support routing security.”

# The system



# The Route Origin Authorisation (ROA)

---

- A cryptographic attestation using your resource certificate
  - A valid ROA can only be created by the legitimate holder of the IP address block
  - A ROA makes a claim about a route announcement

*“I authorise this Autonomous System to originate these IP prefixes”*

# Management of Certificates and ROAs

---

- RIPE NCC Hosted System
  - Embedded in the LIR Portal
  - RIPE NCC publishes Certificates and ROAs
- RIPE NCC Non-Hosted System
  - Run your own Certificate Authority
  - Publish objects yourself
- 3rd Party software

# After publication of the ROA, anybody can...

- Create local cache of the ROA repository
- Validate if a ROA was created by the legitimate holder of the IP Address block
- Base routing preferences on the RPKI status of a route announcement:
  - VALID: ROA found, authorised announcement
  - INVALID: ROA found, unauthorised announcement
  - UNKNOWN: No ROA found (resource not yet signed)

# RIPE NCC RPKI Validator

RPKI Validator

Home

Trust Anchors

**ROAs**

Filters

Whitelist

BGP Preview

rpki-rtr log

## Validated ROAs

Validated ROAs from APNIC RPKI Root, AfrinIC RPKI Root, LACNIC RPKI Root, RIPE NCC RPKI Root.

Download validated ROAs as CSV

Show 10 entries

Search: 85/8

ASN	Prefix	Maximum Length	Trust Anchor
1126	85.90.64.0/19	19	RIPE NCC RPKI Root
3303	85.0.0.0/13	24	RIPE NCC RPKI Root
6714	85.219.128.0/17	17	RIPE NCC RPKI Root
6724	85.214.0.0/15	16	RIPE NCC RPKI Root
9146	85.92.224.0/19	21	RIPE NCC RPKI Root
13110	85.221.128.0/17	24	RIPE NCC RPKI Root
13301	85.14.192.0/18	24	RIPE NCC RPKI Root
15456	85.236.32.0/19	19	RIPE NCC RPKI Root
15527	85.157.0.0/16	16	RIPE NCC RPKI Root
31549	85.15.0.0/18	24	RIPE NCC RPKI Root

First Previous 1 2 Next Last

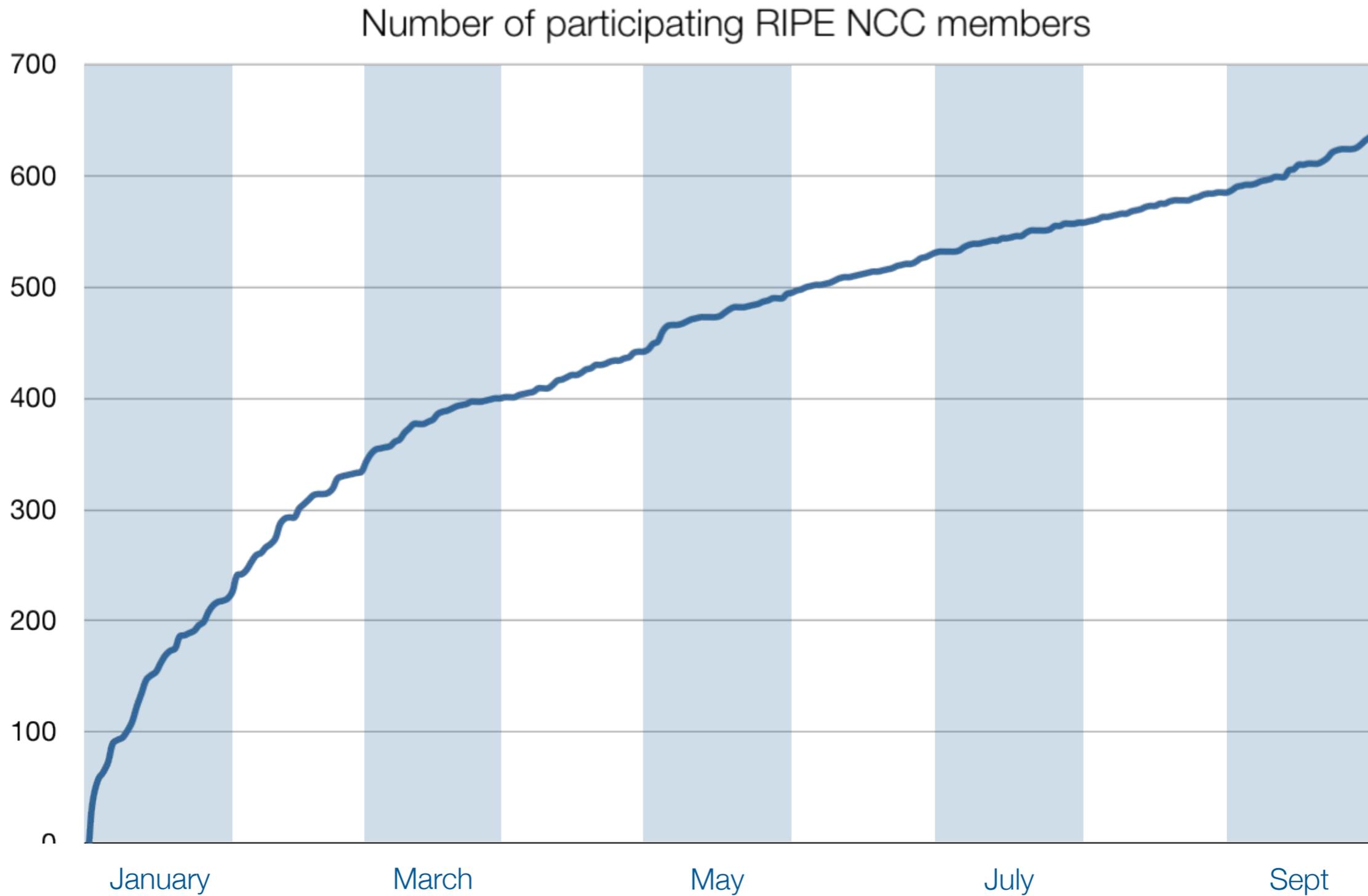
Showing 1 to 10 of 17 entries (filtered from 1,317 total entries)

# Hardware Router Support

---

- Based on open IETF Standards: RPKI-RTR
- Router talks to your local validation tool
  - Router does not do the crypto
- Set route maps and prefs based on the three RPKI states of a route announcement
  - Valid, Invalid, Unknown
- Running code on:
  - Cisco, Juniper, Quagga

# Adoption



Questions?



# Certification Resolutions

---

- Option A is approved > Certification is abandoned by the RIPE NCC
- Option B is approved > Certification continues as a RIPE NCC activity BUT without ROAs
- Neither option is approved > The RIPE NCC continues with full implementation of Certification