Resource Certification (RPKI)

Alex Band – Product Manager

RIPE 64, Ljubljana

RIPE 63: Members Voted on Certification

- The RIPE NCC will continue working on RPKI
  - Offer resource certificates on an opt-in basis
  - Offer a platform for BGP Origin Validation
- A close vote
- A clear message

Proceed with caution!

Concerns That Were Raised

1. Operator Autonomy
   - RIR could be forced to tamper with the certificate tree (court order)

2. Security
   - The system could get compromised (hack, error, etc.)

3. Resilience
   - The system could suffer from a failure
   - Data cannot be maintained or retrieved (affecting BGP)

Summary

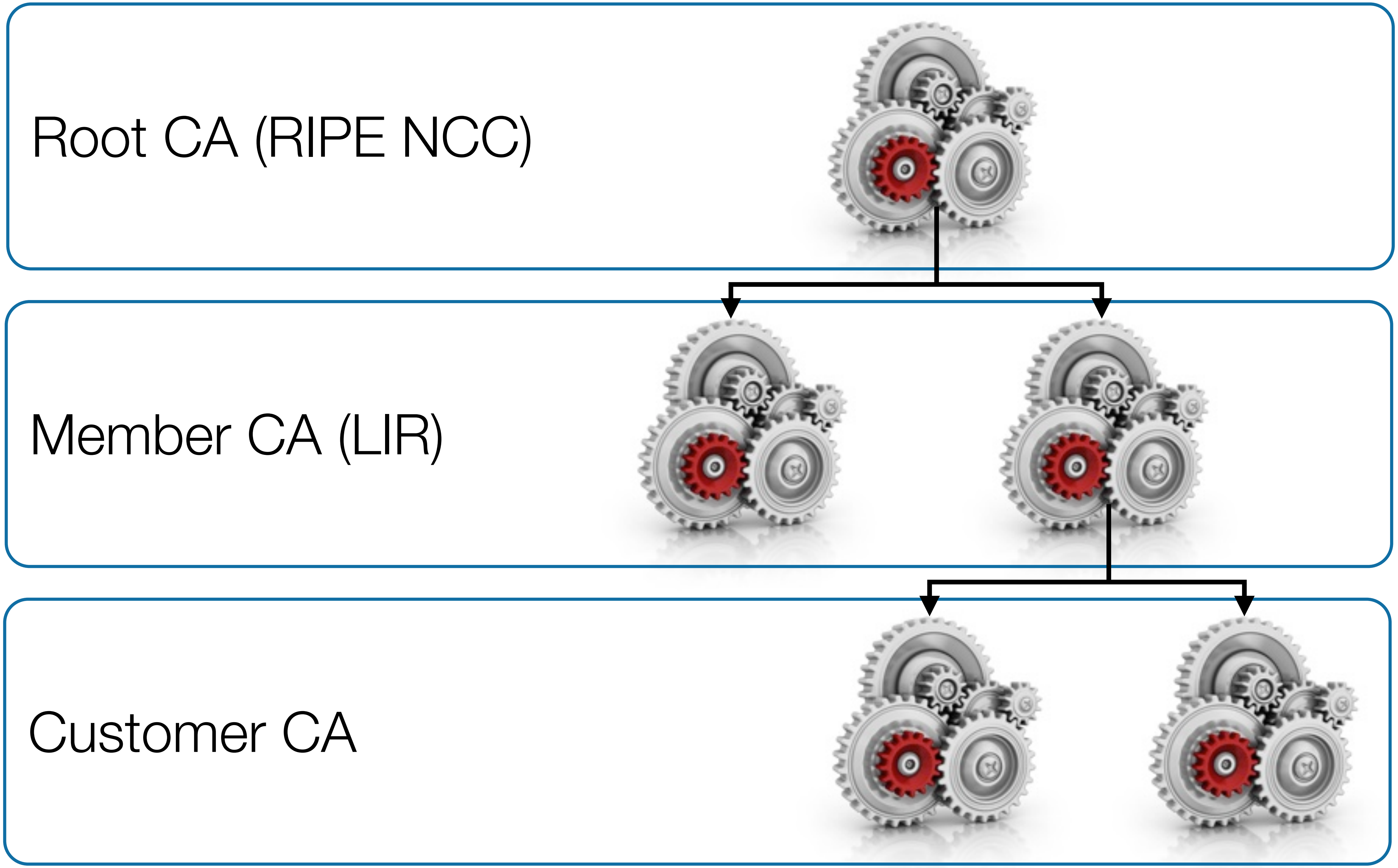
- Members have expressed their support for:
  - A service that offers validatable proof of holdership
  - The possibility to perform BGP Origin Validation
    - Prevent (unintentional) hijacks
    - Have a stepping stone to BGPSEC (Path Validation)
- Those advantages must outweigh potential risks:
  - Diminished operator control of BGP routing
  - An RPKI failure results in unreachable networks

Quick Recap

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

Certificate Authority (CA) Structure



Root CA (RIPE NCC)

Member CA (LIR)

Customer CA

Using RPKI for BGP Origin Validation

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 ROAs in LIR Portal

Certification to Secure Internet Routing

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

Route Origin Authorisation (ROA):

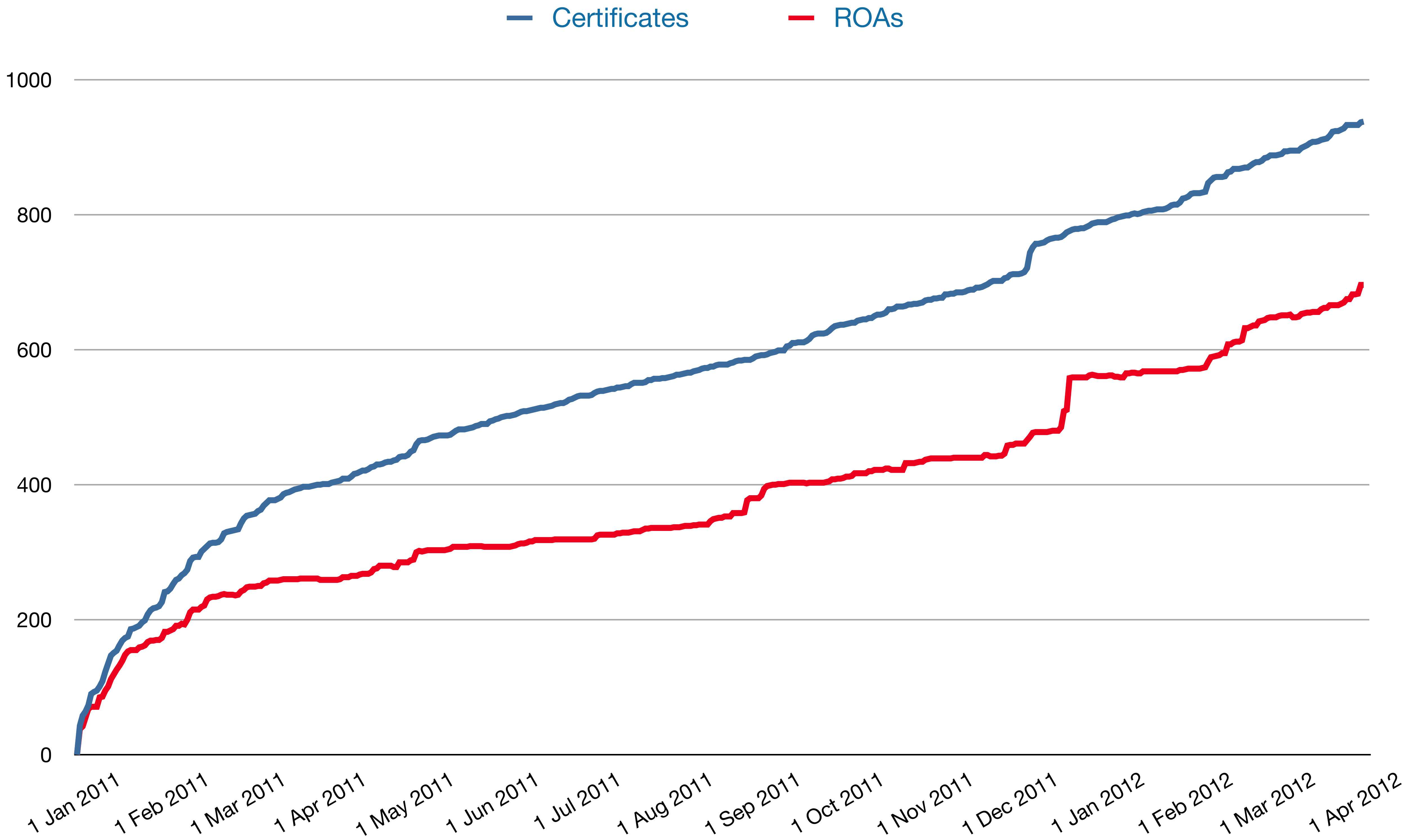
“I authorise this Autonomous System to originate these IP prefixes”

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 BGP route:
  - VALID: ROA found, authorised announcement
  - INVALID: ROA found, unauthorised announcement
  - UNKNOWN: No ROA found (resource not yet signed)

Resource Certification Adoption



The Relying Party – That's YOU!

- Anyone can base any routing decision on the RPKI data set
- Three variables: VALID, INVALID, UNKNOWN
  - Treat them as you wish
  - Override specific parts locally

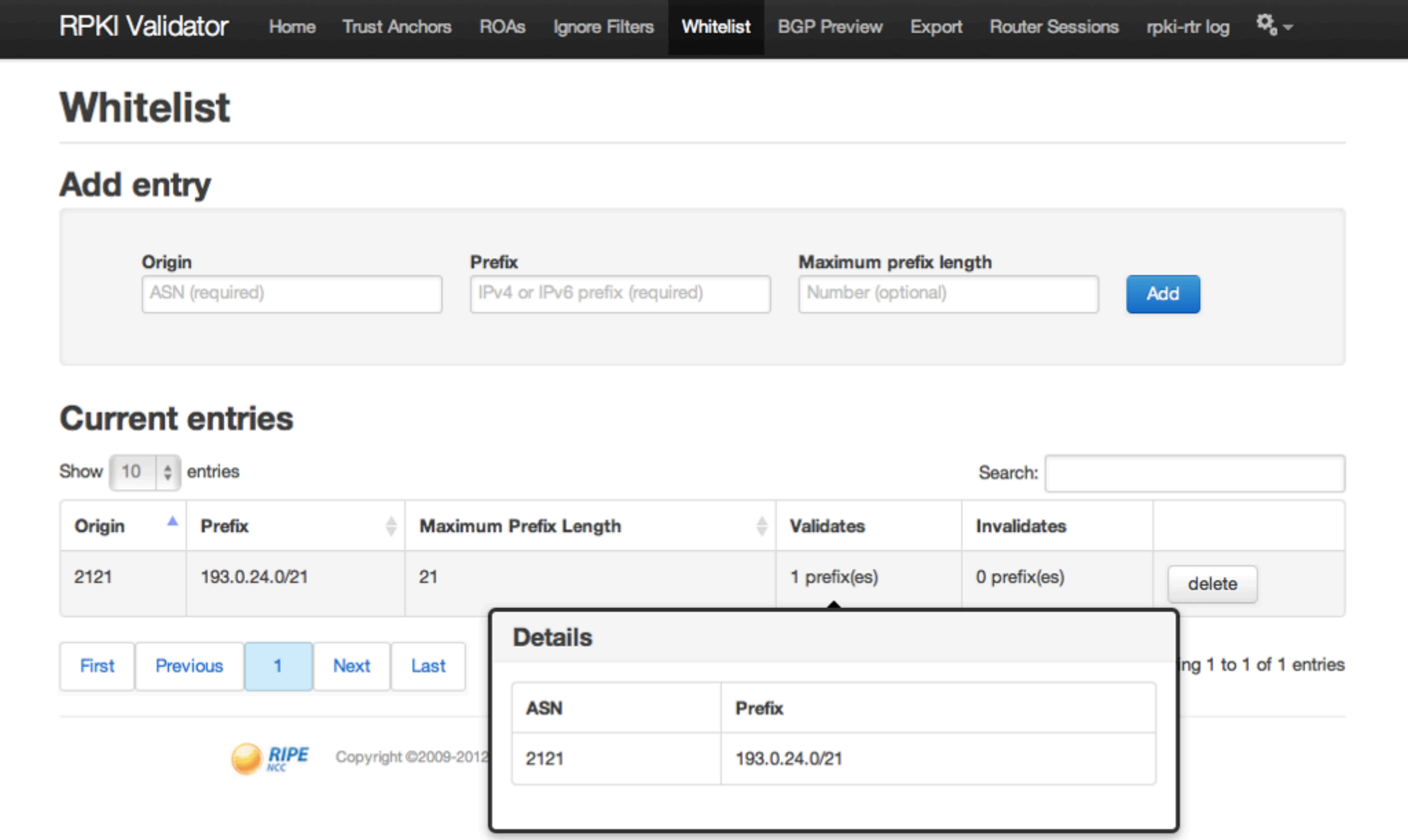
The decision making power is in your hands!

Operator Autonomy

Enhance Relying Party Autonomy

- The relying party is in the driver’s seat:
  - You can choose to rely on any Trust Anchor
  - Data set is the sum of all configured Trust Anchors

- RIPE NCC RPKI Validator has additional controls:
  - You can ignore or override any RPKI data point:
    - White List (Apply RPKI status ‘Valid’)
    - Ignore Filter (Apply RPKI status ‘Unknown’)



Whitelist

Add entry

Origin: ASN (required)

Prefix: IPv4 or IPv6 prefix (required)

Maximum prefix length: Number (optional)

Current entries

Show 10 entries

Search:

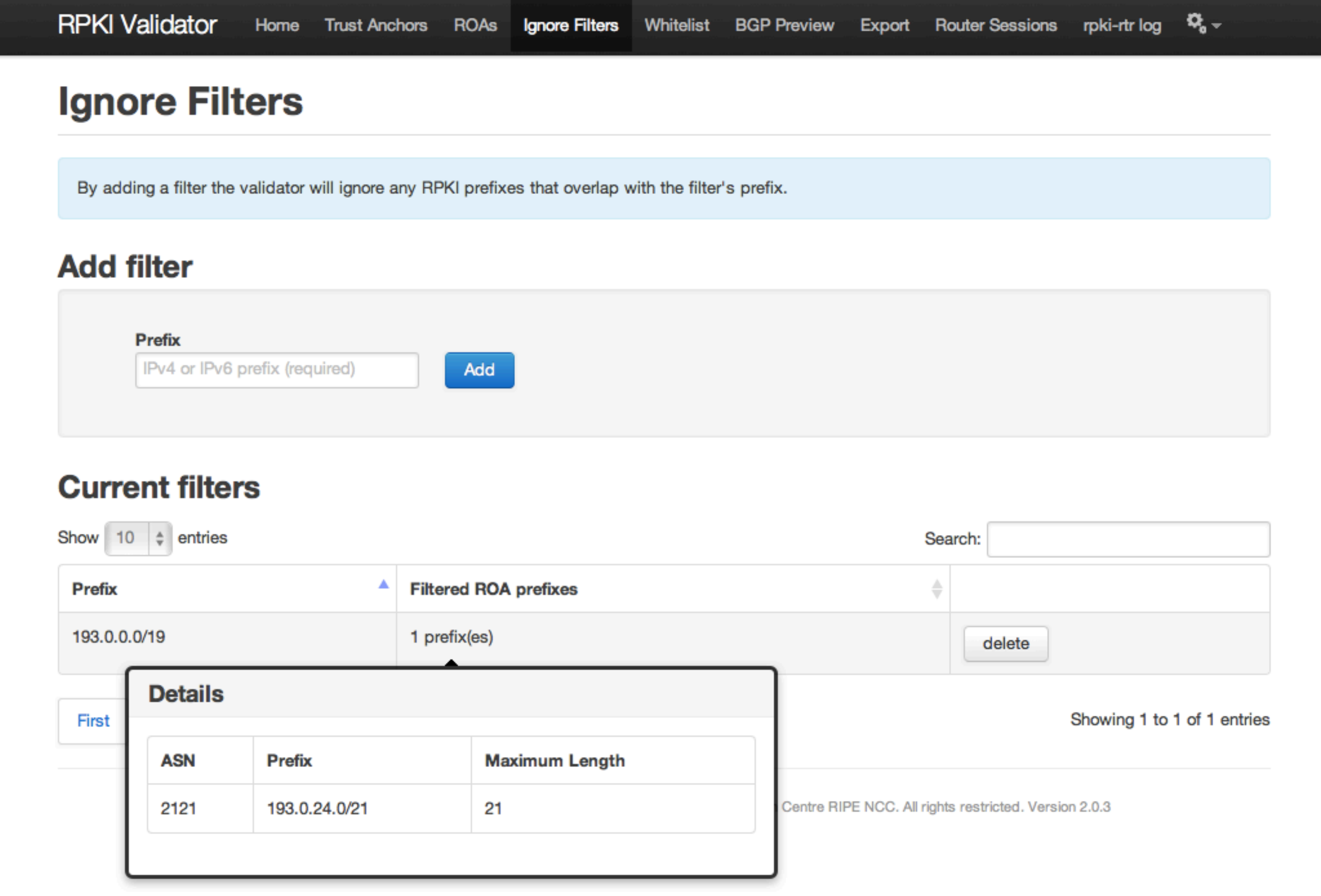
Origin	Prefix	Maximum Prefix Length	Validates	Invalidates	
2121	193.0.24.0/21	21	1 prefix(es)	0 prefix(es)	delete

ing 1 to 1 of 1 entries

Details

ASN	Prefix
2121	193.0.24.0/21

Copyright ©2009-2012



Ignore Filters

By adding a filter the validator will ignore any RPKI prefixes that overlap with the filter's prefix.

Add filter

Prefix

IPv4 or IPv6 prefix (required)

Current filters

Show 10 entries

Search:

Prefix	Filtered ROA prefixes	
193.0.0.0/19	1 prefix(es)	delete

Details

ASN	Prefix	Maximum Length
2121	193.0.24.0/21	21

Showing 1 to 1 of 1 entries

Centre RIPE NCC. All rights restricted. Version 2.0.3

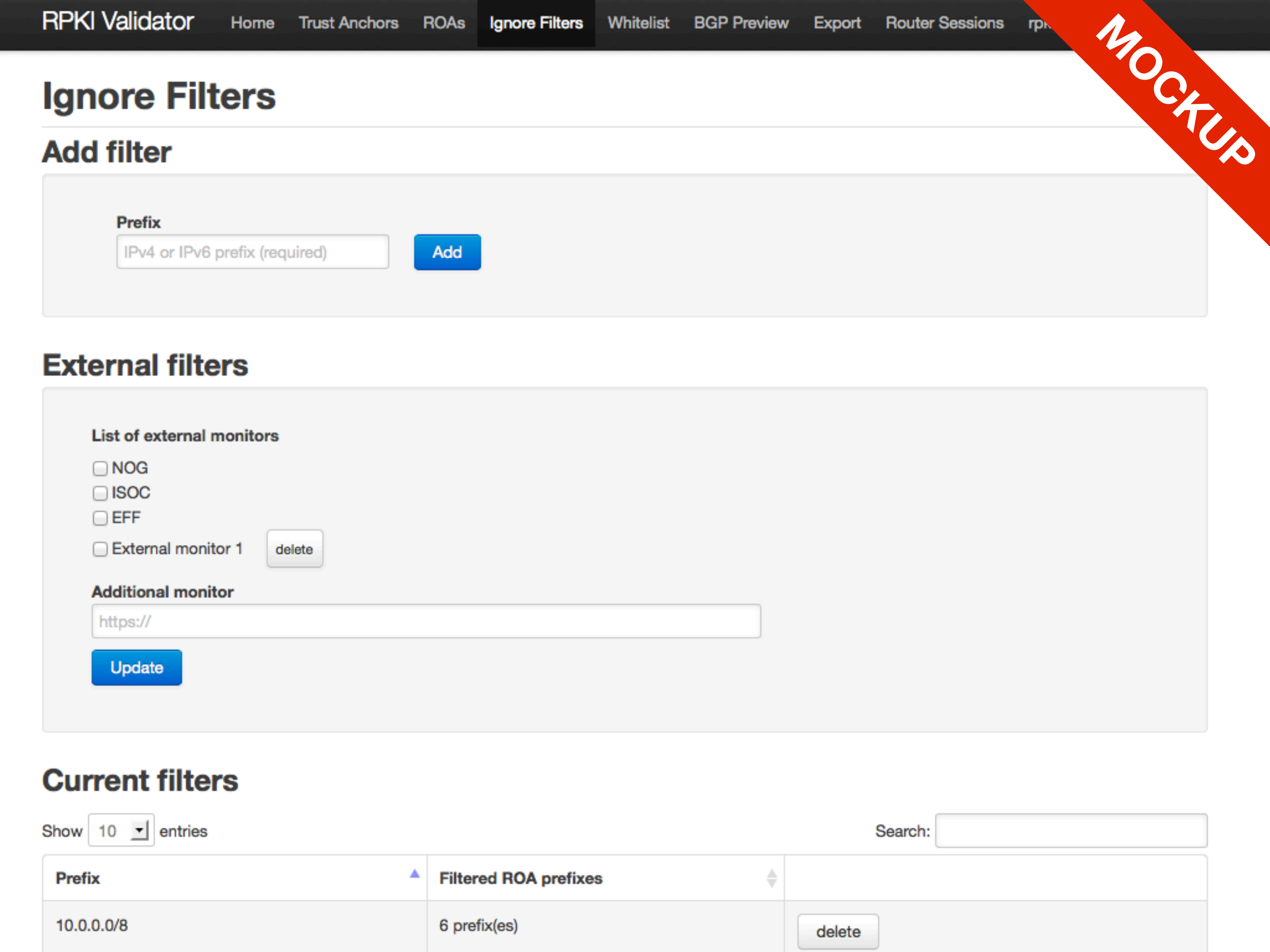
Using The Overrides Practically

- If a ROA is not trusted:
  - it can be ignored or white listed in the RPKI Validator
  - overrides can be applied directly on the router
- In a fully deployed RPKI world, this requires >8000 RIPE NCC members to take action

That doesn’t scale

Proposal: Using Independent Monitors

- External, independent monitors can publish a list of address space that is disputed or untrusted
- NOGs, ISOC, EFF?
- RPKI Validator can import these lists and feed the ignore filter
  - Automatically ignore or send alert



Ignore Filters

Add filter

Prefix

IPv4 or IPv6 prefix (required)

External filters

List of external monitors

☐ NOG
☐ ISOC
☐ EFF
☐ External monitor 1

Additional monitor

https://

Current filters

Show 10 entries

Search:

Prefix	Filtered ROA prefixes	
10.0.0.0/8	6 prefix(es)	delete

Considerations

- Potential monitors need to have broad support
  - Open process, transparent
  - Impartial, community driven
  - Outside RIPE NCC jurisdiction
- Ignore only if certain amount of monitors agree
- Possible attack vector on monitors
- No IETF Standards cover this
  - Data format to be determined

Security, Resilience, Service Expansion

Enhance Security

- Enhance LIR Portal two-factor authentication
  - Solution that works for >8000 members in 72 countries
  - Looking at mobile phones (SMS)

- Independent audits of code and CA operation
  - Get Certificate Authority Accreditation?

Enhance Resilience

- Make all elements of the system more resistant to failure and attack:
  - Hosted Certificate and ROA management
    - LIR Portal
  - Non-hosted Parent Certificate system
    - up/down
  - Data retrieval
    - RIPE NCC ROA Repository

Expand Eligible Address Space

- Incrementally add:
  - Certification access for Direct Assignment Users
  - Certification access for PI End Users
    - Direct access, or
    - Grant access to sponsoring LIR
  - Certify ‘Minority’ address space
    - Get child certificate from ‘Majority’ RIR
  - Legacy space

The Roadmap

The Roadmap

- Q1/Q2: Test system, better Validator, better UI
- Q2/Q3: Strengthen Operator Autonomy
  - Build monitoring infrastructure prototype
- Q3/Q4: Strengthen Security
  - Authentication, periodic auditing
- Q4/Q1: Strengthen Resilience
  - Service and data set distribution
- Gradual: Expand eligible address space

Information and Announcements

http://ripe.net/certification

#RPKI

Questions?

✉ alexb@ripe.net

@alexander_band