RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Developments in Routing Security

Robert Kisteleki | May 2019 | TREX/NOG.FI

Intro

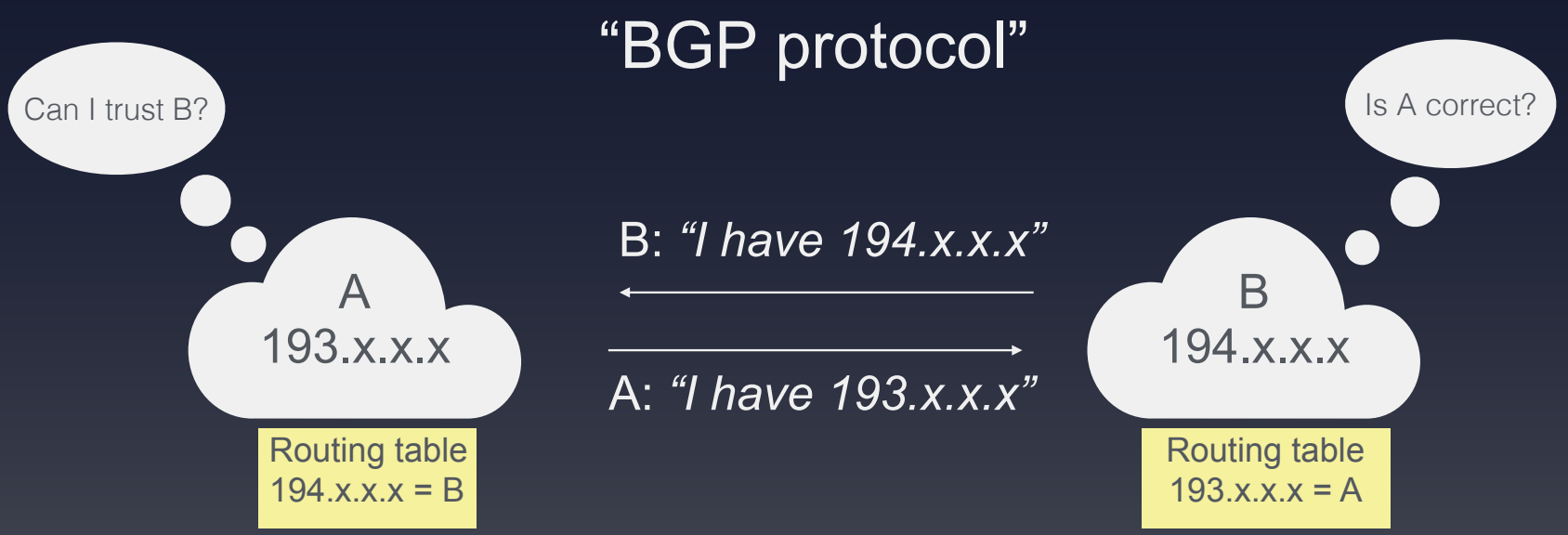
Who We Are

- We manage IP and ASN allocations in Europe, the Middle East and parts of Central Asia
  - Ensure unique holdership
  - Document holdership in the RIPE Database (whois)
  - Enable operators to document use of their address spaces

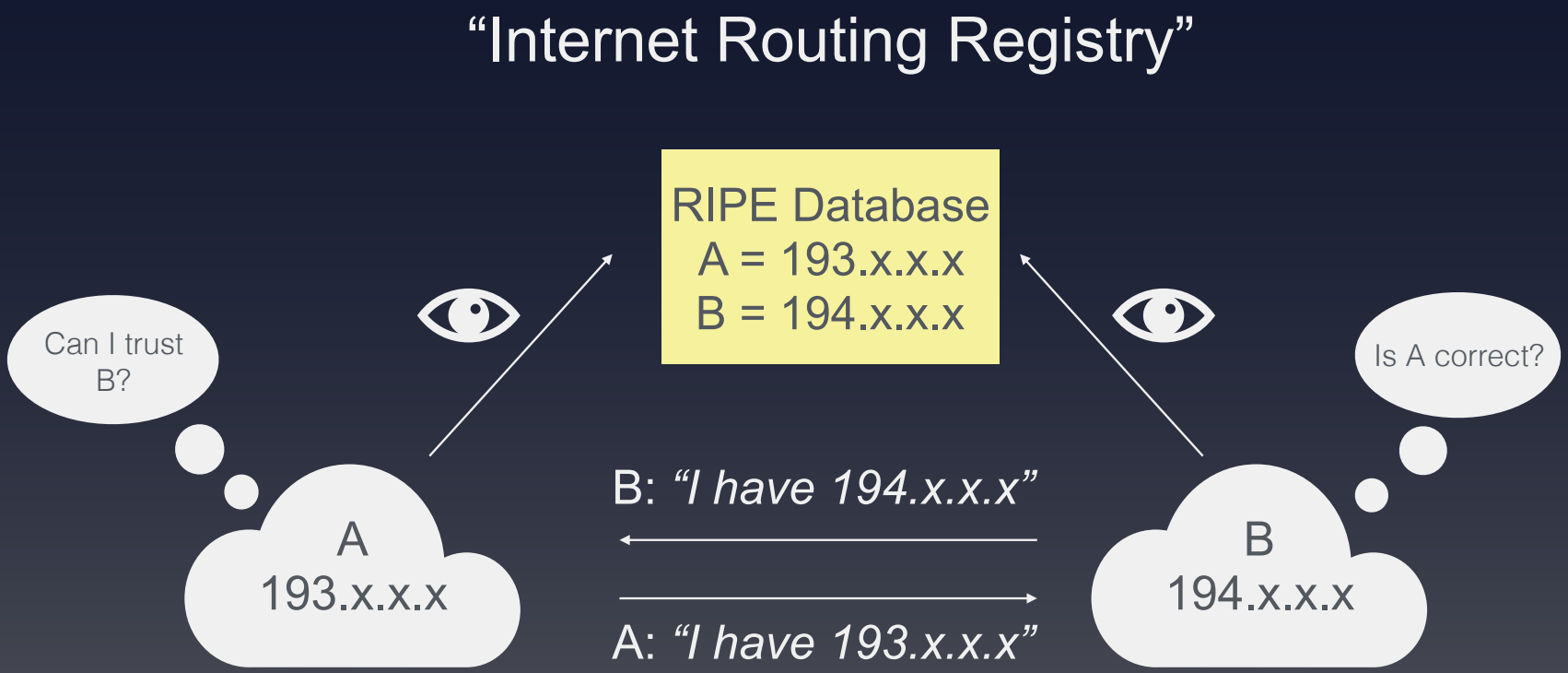
Routing Security is in Our DNA

- In 1994, RIPE-181 was the first document published that used a common language to describe routing policies
- We co-developed standards for IRR and RPKI
- We are one of the five RPKI Trust Anchors
- Our Validator tool was, until recently, the only production-grade tool to do Origin Validation

Routing on the Internet



How to Secure Routing?



Internet Routing

- Border Gateway Protocol
  - BGPv4, 1994
- The problem remains
  - No built-in security in BGP Protocol

Accidents Happen

- Fat Fingers
  - 2 and 3 are really close on our keyboards…
- Policy violations (leaks)
  - Oops, we did not want this to go to the public Internet
  - Infamous incident with Pakistan Telecom and YouTube

Or Worse…

- **April 2018**
  - BGP and DNS hijack
  - Targeting MyEtherWallet
  - Unnoticed for 2 hours

Incidents Are Common

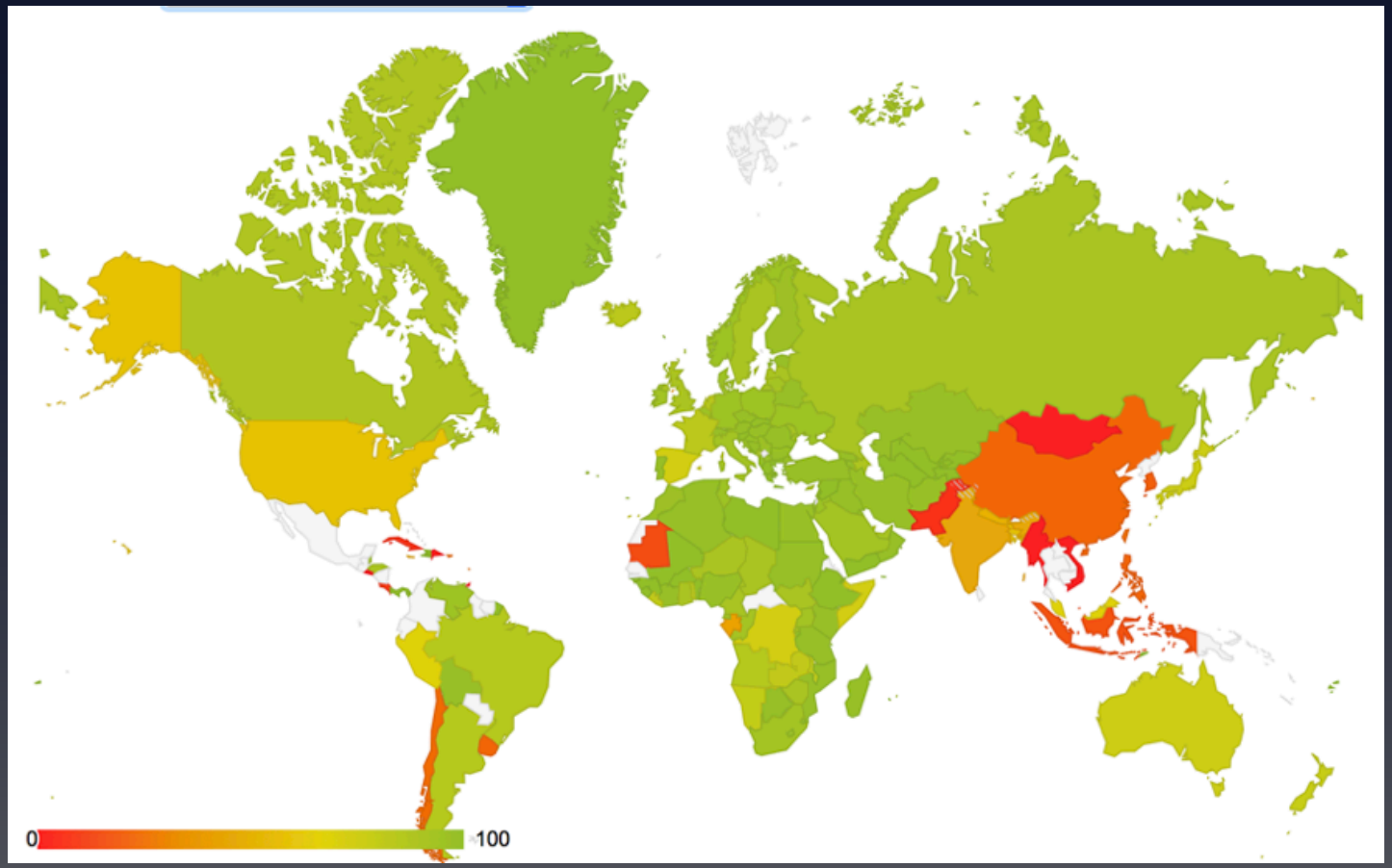
- **2018 Routing Security Review**
  - 12.6k incidents
  - 4.4% of all ASNs affected
  - 3k ASNs victims of at least one incident
  - 1.3k ASNs caused at least one incident

source: https://www.bgpstream.com/

Internet Routing Registry

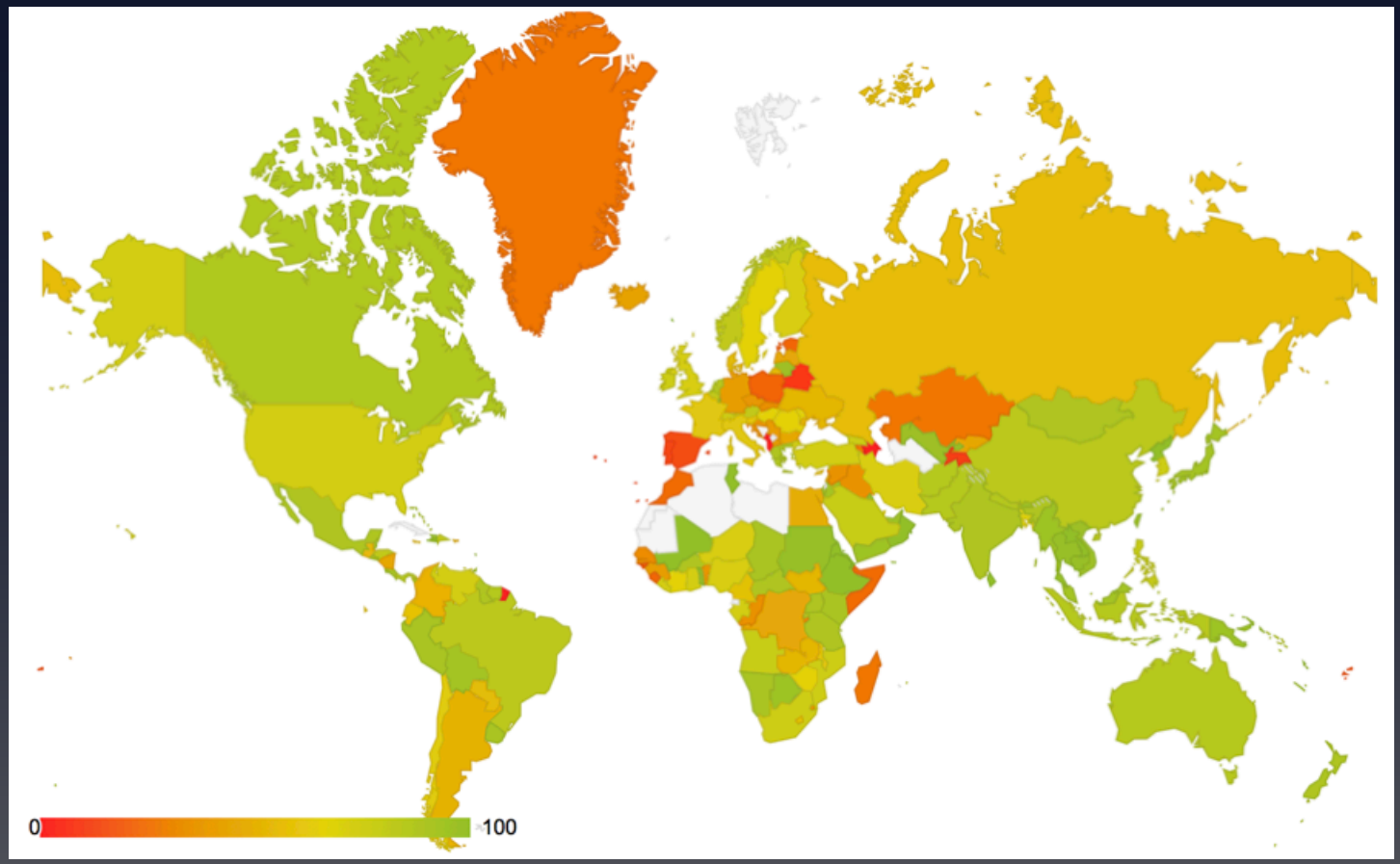
- Many exist, most widely used
  - RIPE Database
  - RADB
- Verification of holdership over resources
  - RIPE Database for RIPE region resources only
  - RADB allows paying customers to create any object
  - Lots of the other IRRs do not formally verify holdership

Accuracy - RIPE IRR



Accuracy - Valid announcements / covered announcements

Accuracy - RADB IRR



Accuracy - Valid announcements / covered announcements

Resource PKI

Resource Public Key Infrastructure

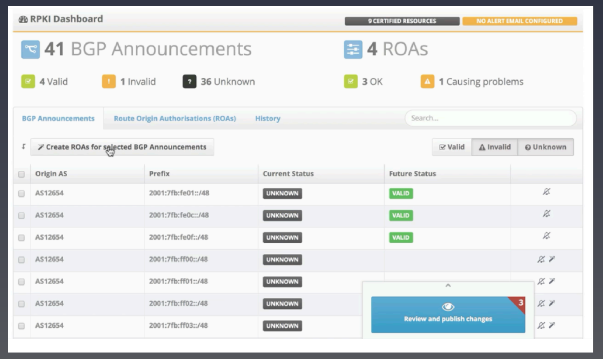
- RPKI
  - Ties IP addresses and ASNs to public keys
  - Follows the hierarchy of the registry
- Authorised statements from resource holders (ROAs)
  - ASN X is authorised to announce my IP Prefix Y
  - Signed, holder of Y

Resource Public Key Infrastructure

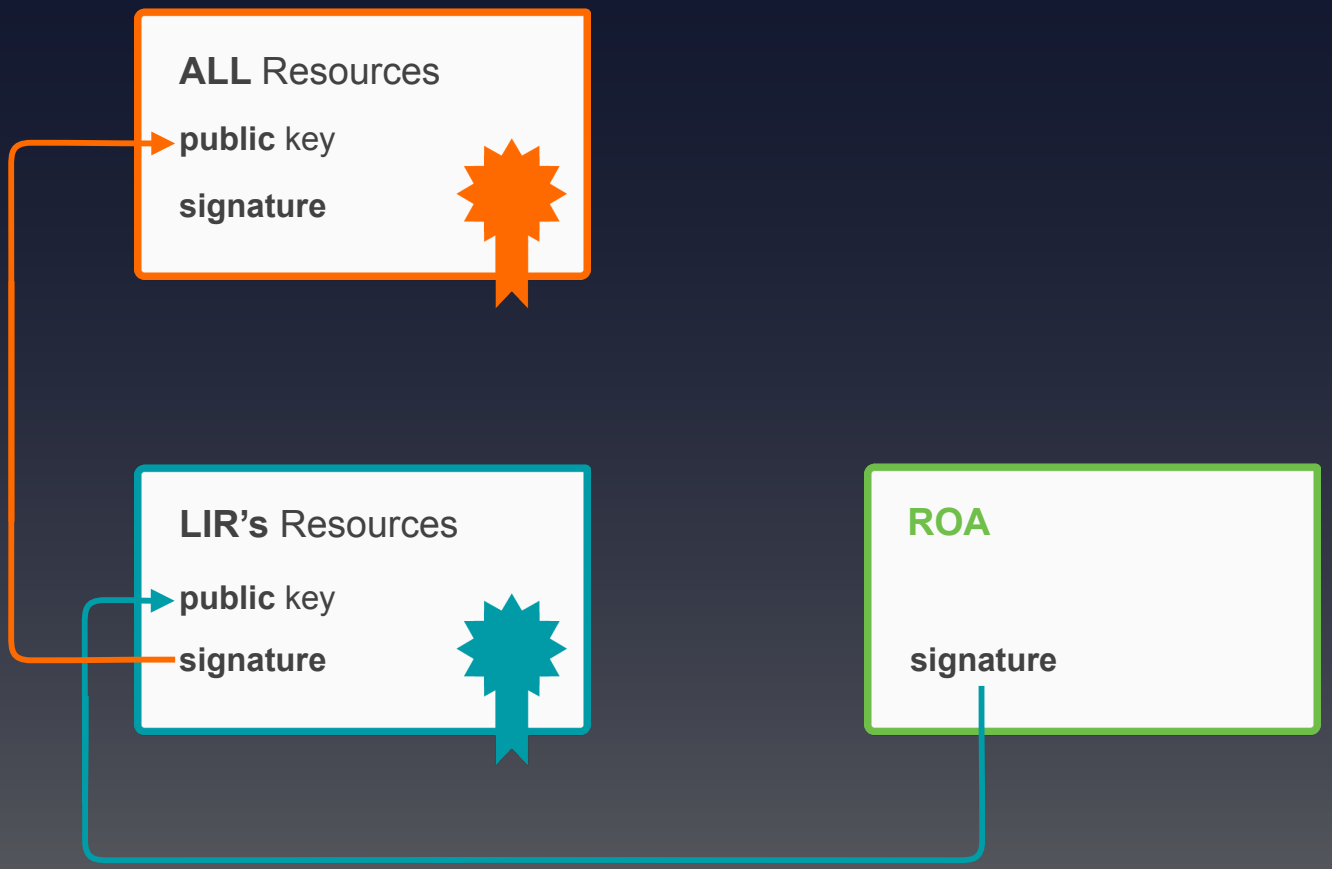
- Operated since 2008 by all RIRs
  - Community-driven standardisation (IETF)
  - IRR was not sufficient (incomplete, incorrect)
- Adds crypto-security to Internet Number Resources

Operators Are In Control

- We show member announcements (in the LIR portal)
  - Member chooses to authorise or not (via “my resources”)
  - Does not need to worry about the crypto (it’s a hosted solution)
  - It is there, but let the machines handle it…
- APNIC and LACNIC also have easy-to-use portals
  - Uptake and quality of data is a function of the interface



RPKI Chain of Trust

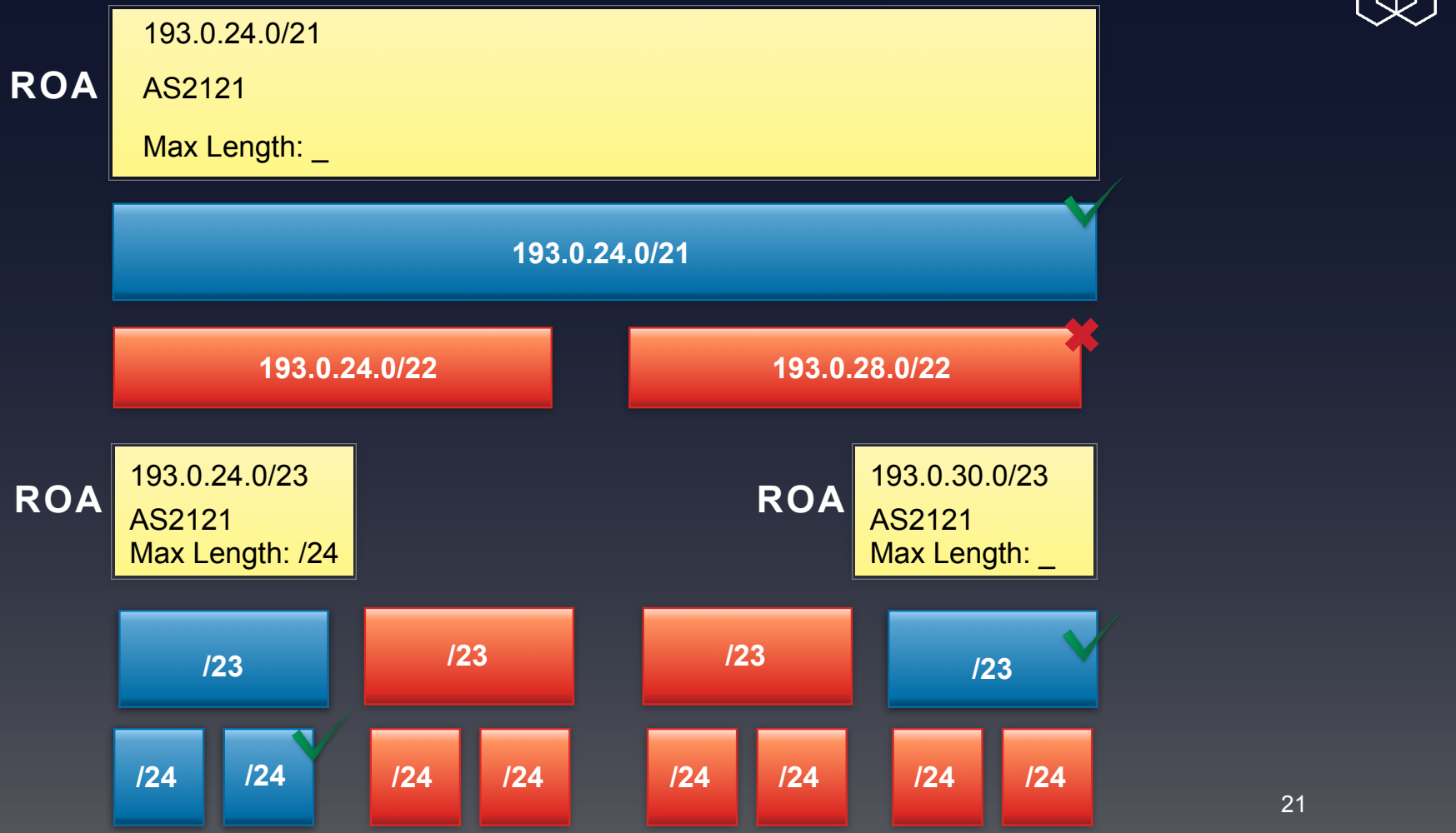


ROA (Route Origin Authorisation)

- LIRs can create a ROA for each one of their resources (IP address ranges)
- Multiple ROAs can be created for an IP range
- ROAs can overlap

What is in a ROA?

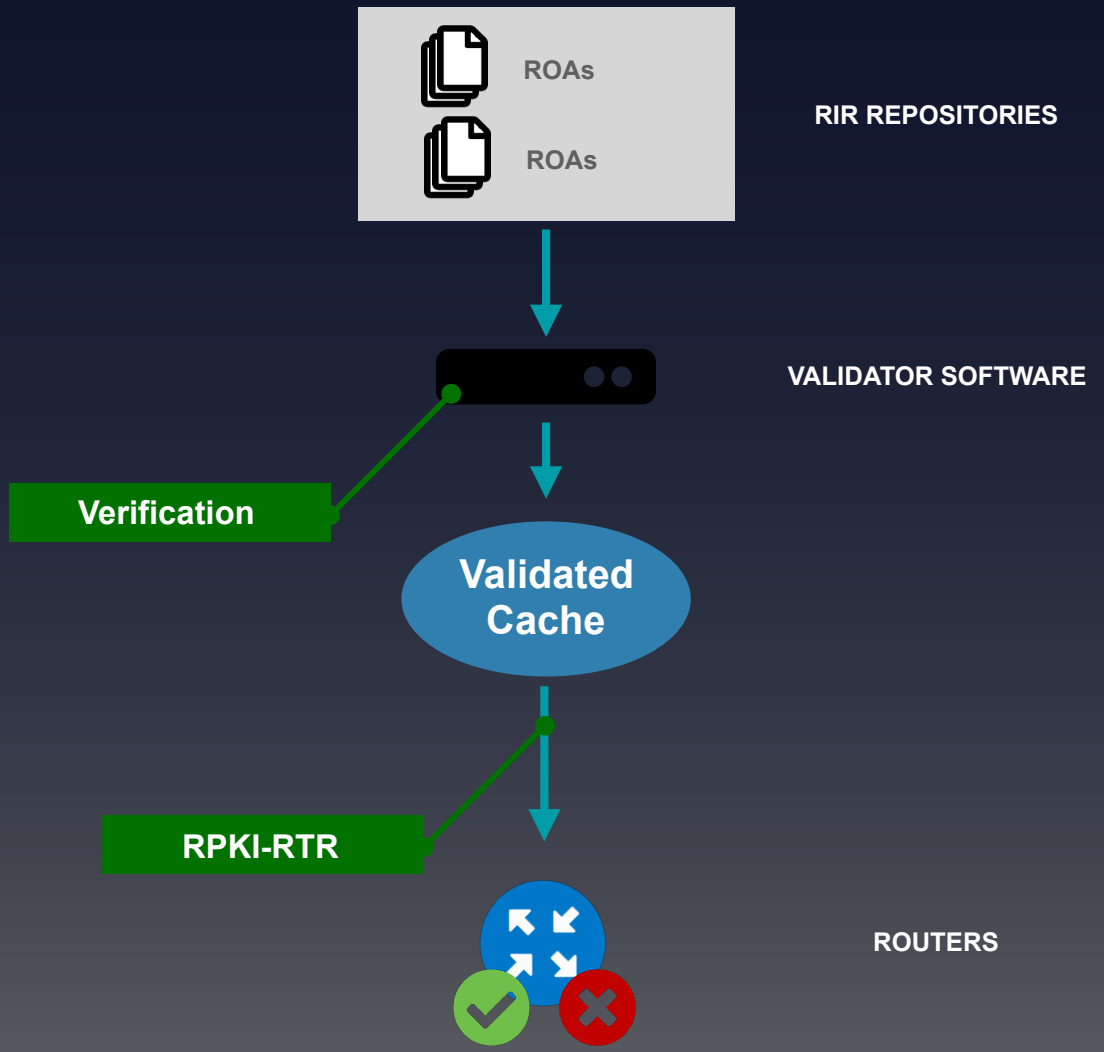
Prefix	The network for which you are creating the ROA
Origin ASN	The ASN that's supposed to be originating the BGP Announcement
Max Length	The Maximum prefix length accepted for this ROA


ROA
193.0.24.0/21
AS2121
Max Length: _
193.0.24.0/21
193.0.24.0/22
193.0.28.0/22
ROA
193.0.24.0/23
AS2121
Max Length: /24
ROA
193.0.30.0/23
AS2121
Max Length: _
/23
/23
/23
/23
/24
/24
/24
/24
/24
/24
/24
/24

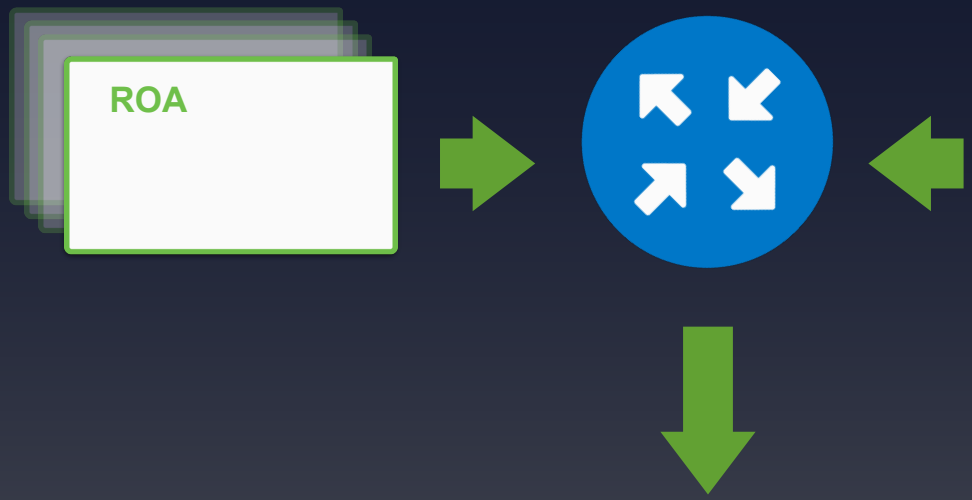
RPKI Validators

- Software that creates a local “validated cache” with all the valid ROAs
  - Downloads the RPKI repository from the RIRs
  - Validates the chain of trust of all the ROAs and associated CAs
  - Talks to your routers using the RPKI-RTR Protocol

RPKI-RTR


ROAs
ROAs
RIR REPOSITORIES
VALIDATOR SOFTWARE
Verification
Validated Cache
RPKI-RTR
ROUTERS

Route Origin Validation

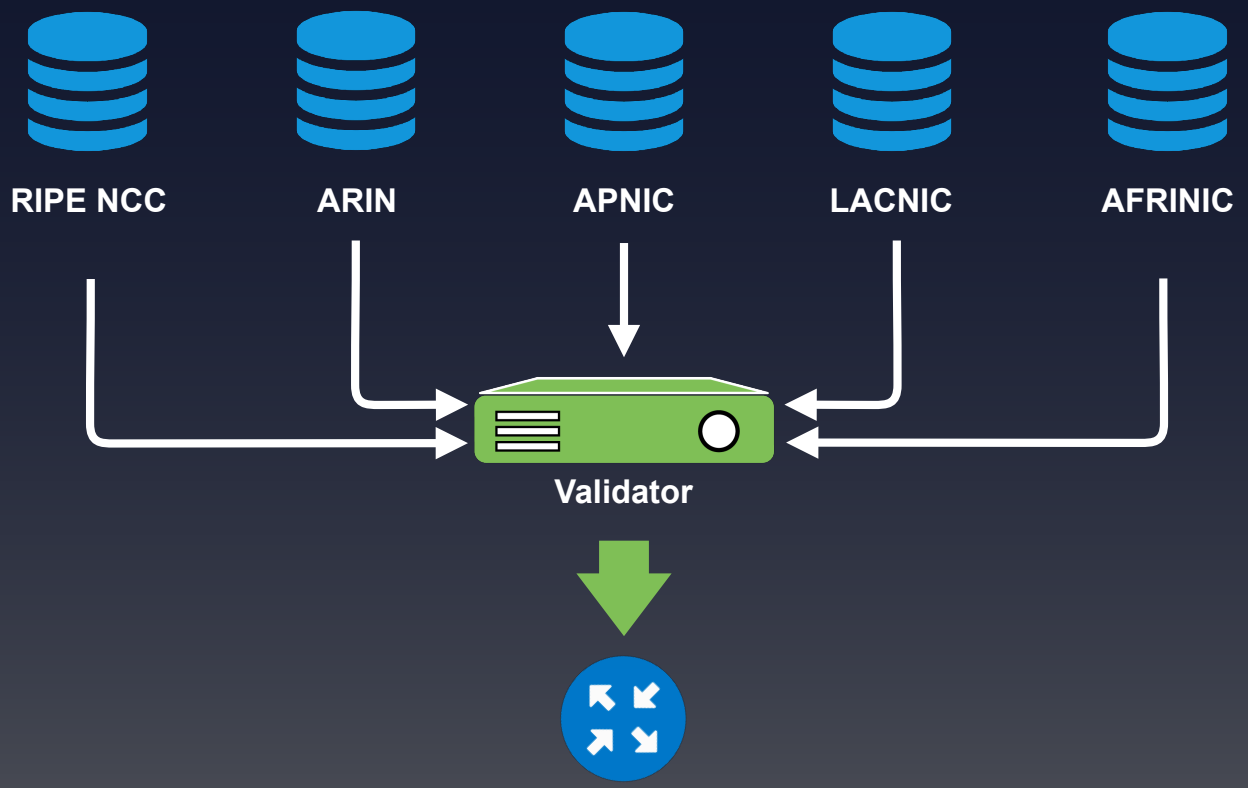


BGP Announcements

AS111	10.0.7.30/22
AS222	10.0.6.10/24
AS333	10.4.17.5/20
AS111	10.0.7.30/22
AS111	10.0.7.30/22
AS111	10.0.7.30/22

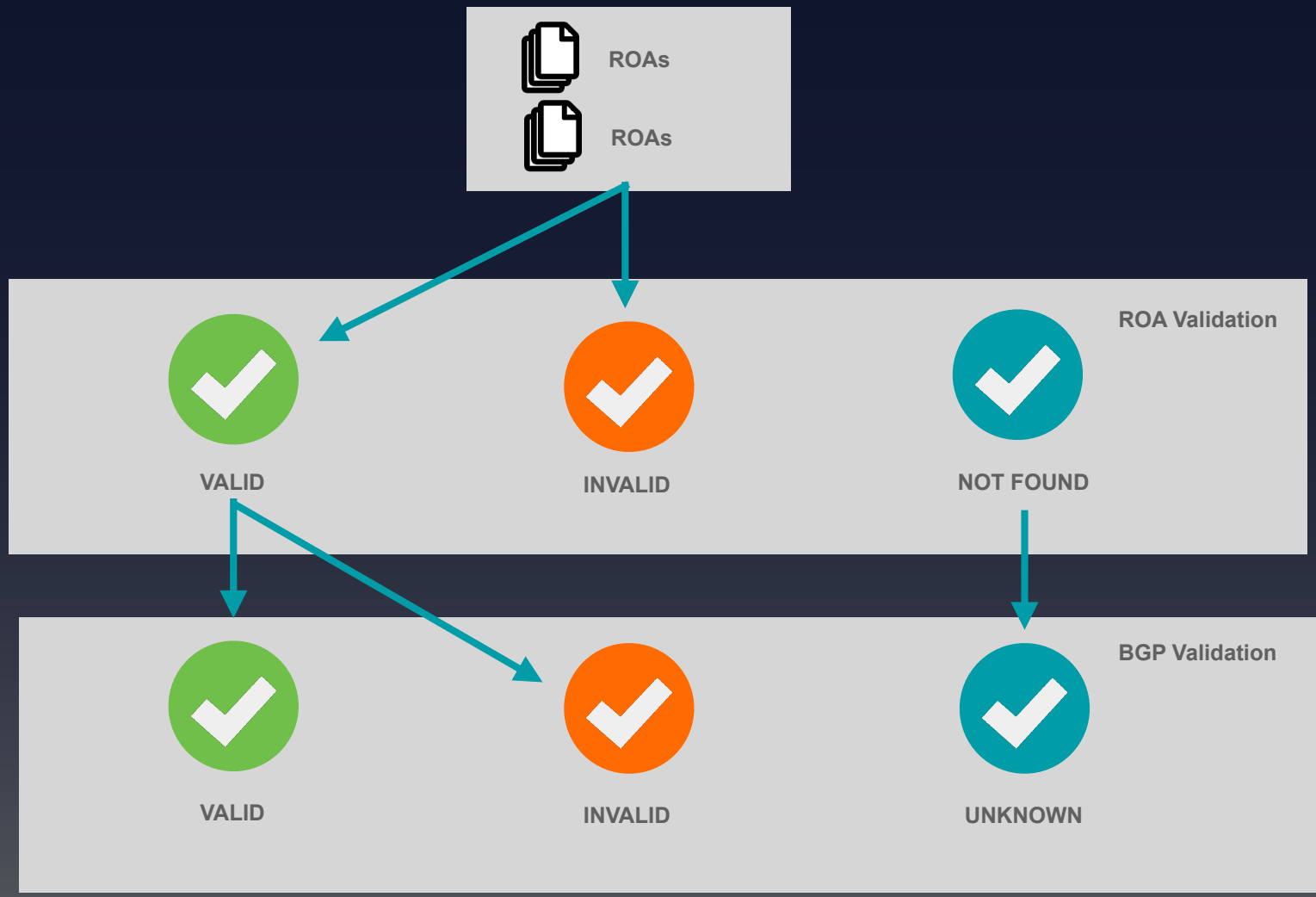
BETTER ROUTING DECISIONS

Route Origin Validation



ROA Validation

- Routers receive data from the validated cache via RPKI-RTR
- Based on this and on BGP announcements, you have to make decisions
  - Accept or discard the BGP Announcement
  - As temporary measure, you could influence other attributes, such as Local Preference


ROAs
ROAs
ROA Validation
VALID
INVALID
NOT FOUND
BGP Validation
VALID
INVALID
UNKNOWN

Invalid ROA

- Invalid ROA
  - The ROA in the repository cannot be validated by the client (ISP) so it is not included in the validated cache
- Invalid BGP announcement
  - There is a ROA in validated cache for that prefix but for a different AS.
  - Or the max length doesn’t match.
- If no ROA in the cache then announcement is “unknown”

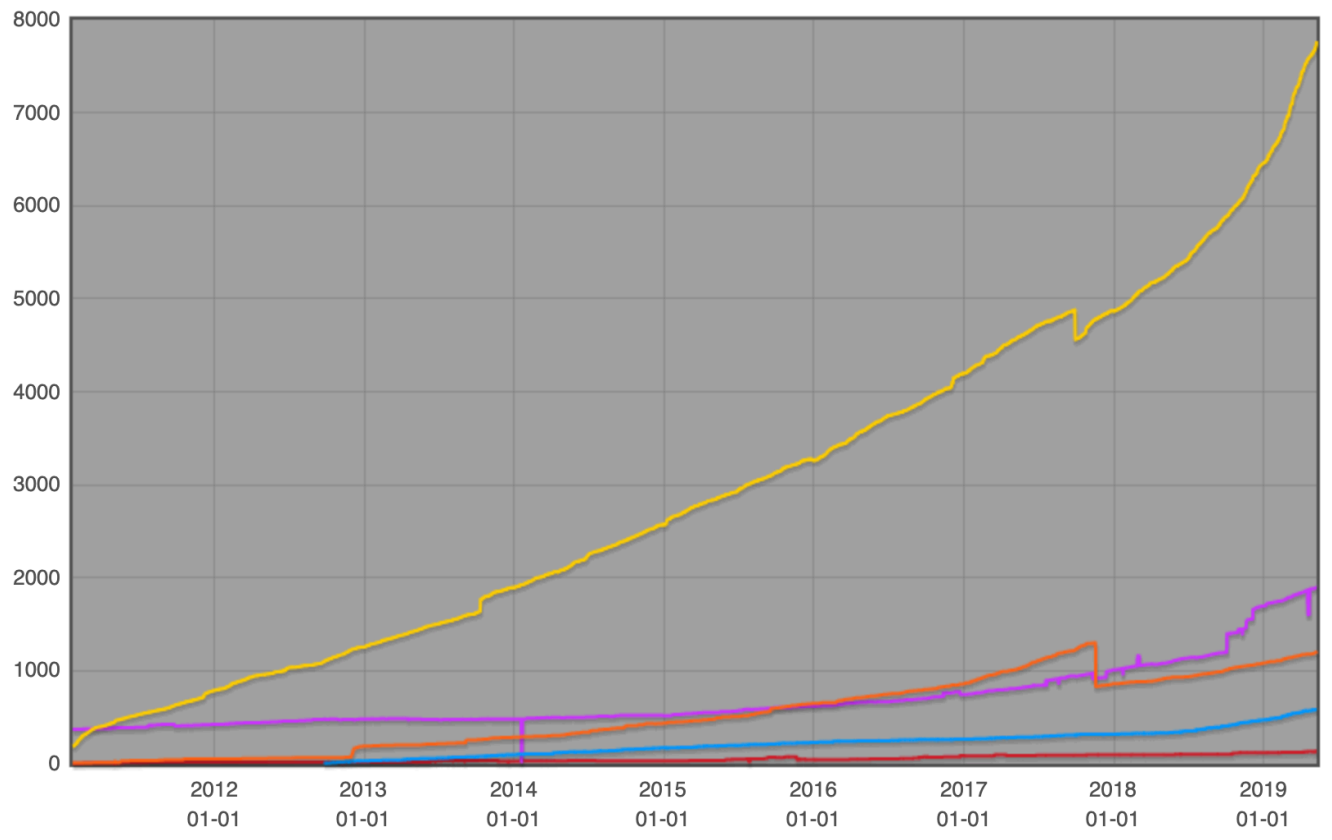
Hosted RPKI

- Automate signing and key roll overs
  - One click setup of resource certificate
  - User has a valid and published certificate for as long as they are the holder of the resources
  - All the complexity is handled by the hosted system
- Lets you focus on creating and publishing ROAs
  - Match your intended BGP configuration

Non-hosted RPKI

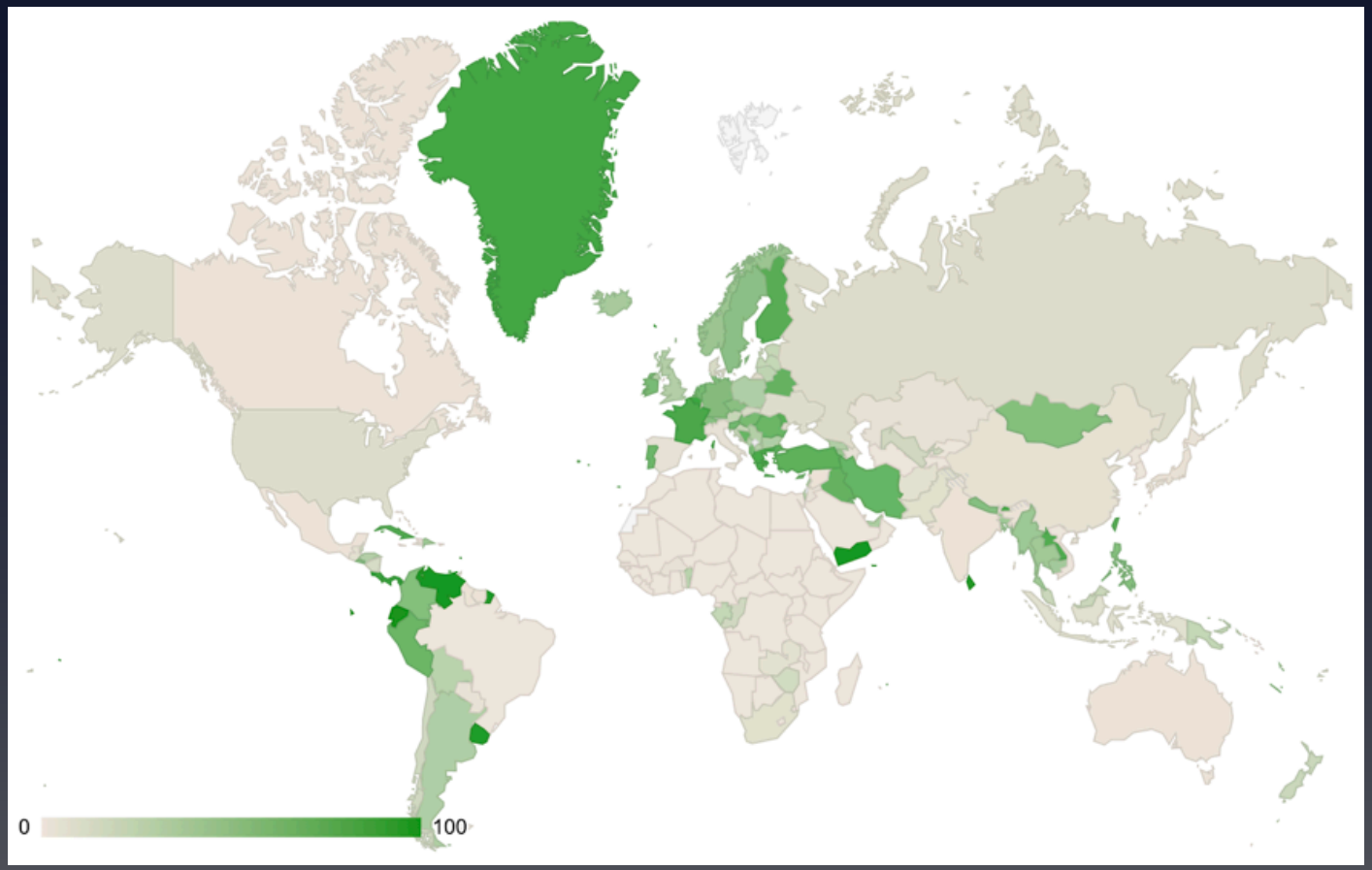
- Run your own Certificate Authority
- With your own software
- At the moment, **not advised**, because of lack of software and options
  - But the situation is improving

Number of Certificates

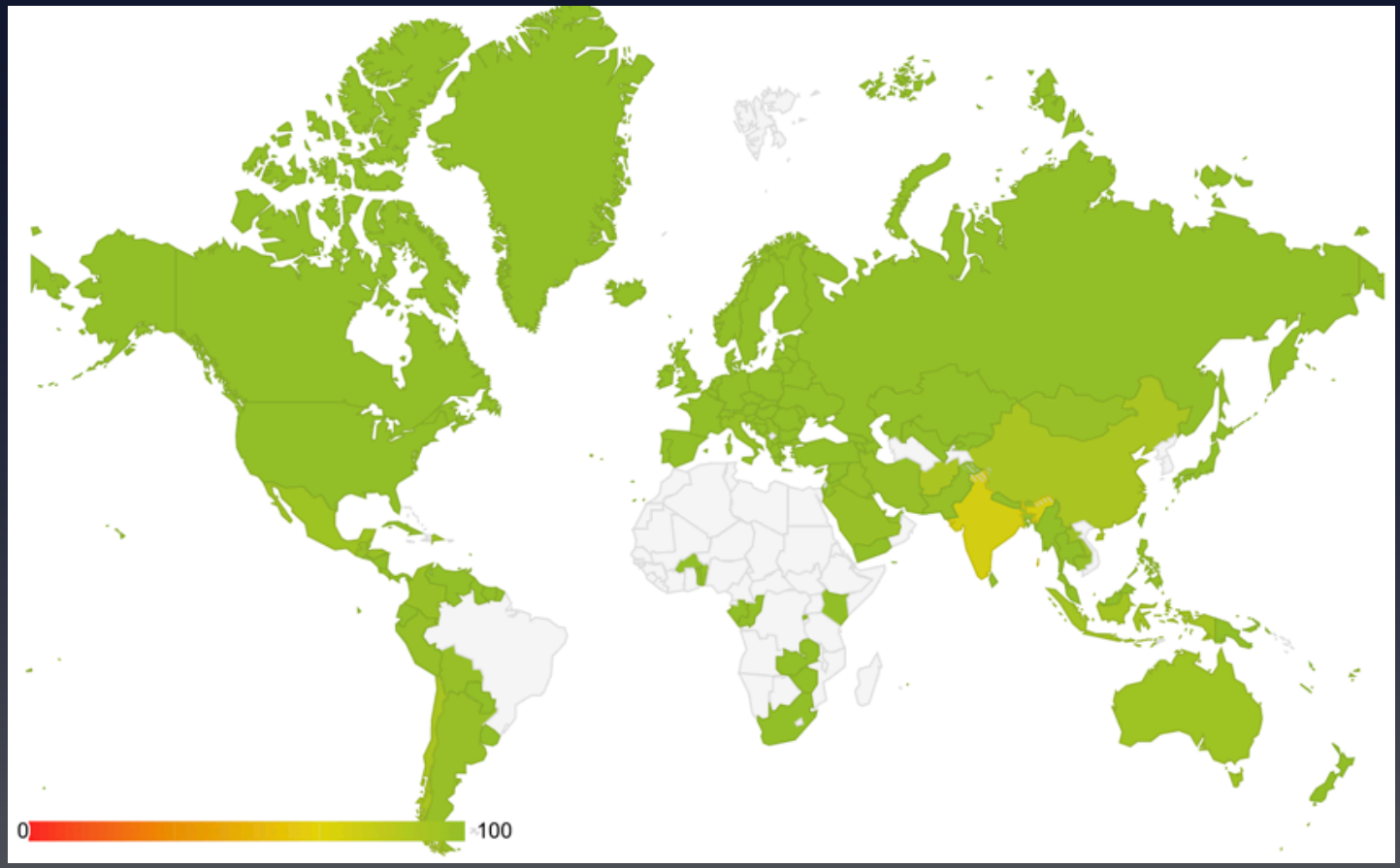


- RIPE NCC: 7770
- APNIC: 1895
- LACNIC: 1212
- ARIN: 583
- AFRINIC: 136

Coverage - RPKI (all RIRs)



Accuracy - RPKI (all RIRs)



IPv4 addresses in valid announcements / covered announcements

RPKI in Northern Europe

Country	% Addreses	Accuracy
FI	68%	100,0%
NO	41%	100,0%
SE	47%	99,9%
IS	29%	100,0%
LV	25%	99,8%
LT	20%	100,0%
EE	19%	100,0%
DK	10%	100,0%

source: https://lirportal.ripe.net/certification/content/static/statistics/world-roas.html

What’s next?

Where do we go from here?

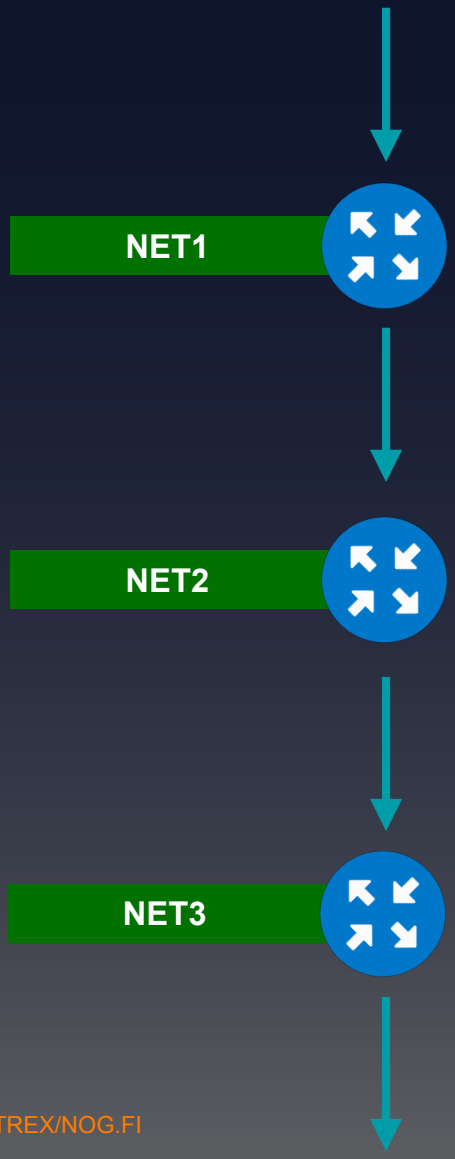
- RPKI is only one of the steps towards full BGP Validation
  - Paths are not validated
- We need more building blocks
  - BGPSec (RFC)
  - ASPA (draft)
  - AS-Cones (draft)

BGPSEC

- RPKI does not protect against path redirection attacks
- We need a way to verify the AS-Path of a given BGP Announcement
  - And understand if anyone tampered with the data on the way to our routers

BGPSEC Path Validation

- With BGPSEC, the AS-Path attribute is cryptographically signed
  - Using the operator's certificate from RPKI
- In order to validate an AS-Path, routers verify the chain of trust of all the signatures of the AS-Path



Network: 192.168.0.0/16
AS Path: NET1, …
BGPSEC: (key1, signature1)

Network: 192.168.0.0/16
AS Path: NET2, NET1, …
BGPSEC: (key1, signature1)
(key2, signature2)

Network: 192.168.0.0/16
AS Path: A
BGPSEC: (key1, signature1)

Network: 192.168.0.0/16
AS Path: NET3, NET2, NET1, …
BGPSEC: (key1, signature1)
(key2, signature2)
(key3, signature3)

Network: 192.168.0.0/16
AS Path: A
BGPSEC: (key1, signature1)

BGPSEC Operations

- New, optional, transitive attribute, to carry digitally signed route info
- Support is negotiated between routers
  - non BGPSEC router will not be burdened by big UPDATE messages
- Incremental deployment is possible

What’s next

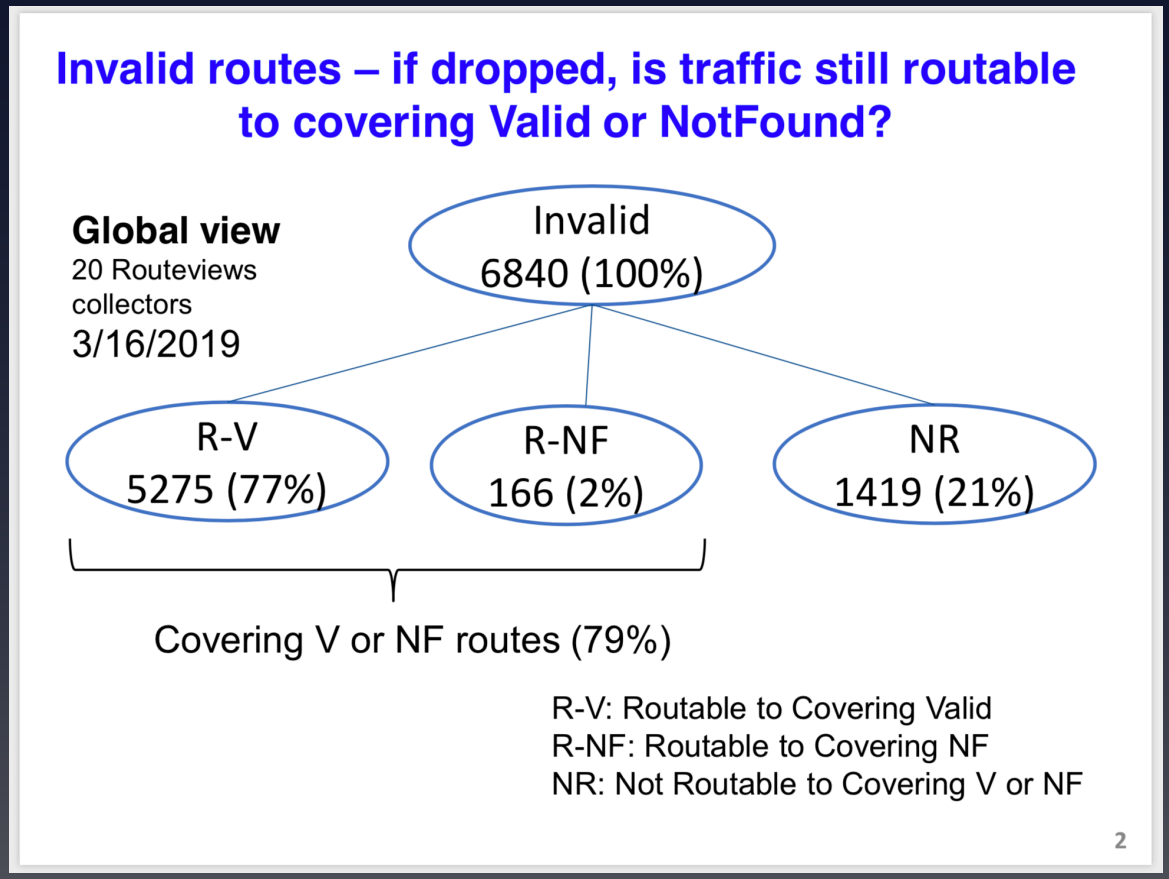
Recommendations to Get Started

- Create your ROAs in the LIR Portal
- Pay attention to the Max Length attribute
- Download and run a Validator
- In a test phase: check validation status manually, which routes are invalid?
- Set up monitoring, for example pmacct

Invalid == Reject

- **What breaks if you reject invalid BGP announcements?**
  - “Not all vendors have full RPKI support, or bugs have been reported”
  - “Mostly nothing” -AT&T
  - “5 customer calls in 6 months, all resolved quickly” -Dutch medium ISP
  - “Customers appreciate a provider who takes security seriously” -Dutch medium ISP
  - “There are many invalids, but very little traffic is impacted” -very large cloud provider

Invalids in the wild



Source: https://datatracker.ietf.org/meeting/104/materials/slides-104-sidrops-analysis-of-invalid-routes-00

Making the Difference

- Is routing security on your agenda?
- Initiate the conversation with providers and colleagues
- Are you leading by example?

Questions