RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Developments in Routing Security

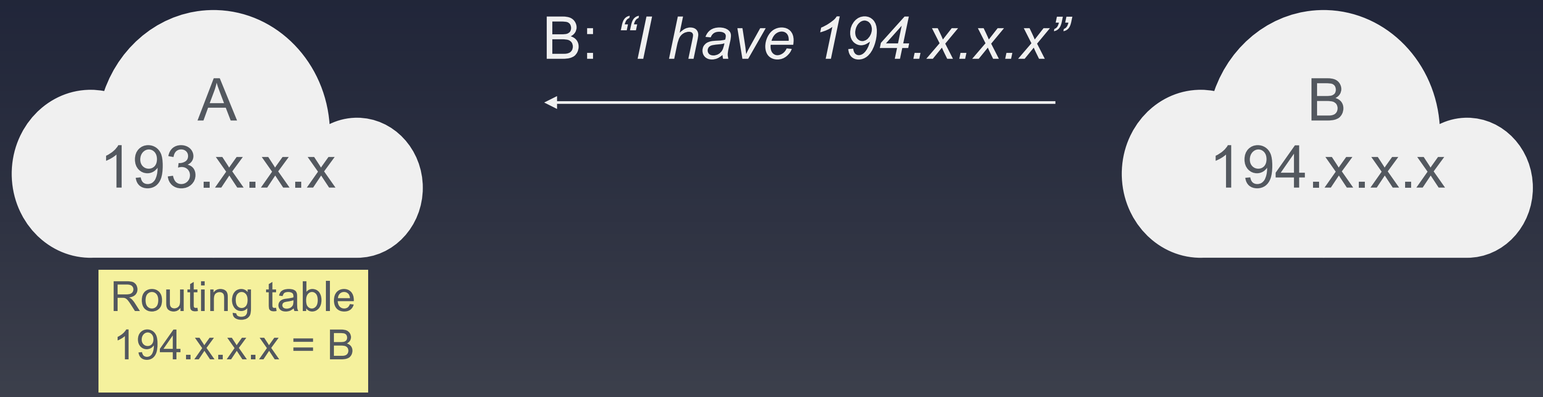
Massimiliano Stucchi | May 2019 | SWINOG

Routing Security is in Our DNA

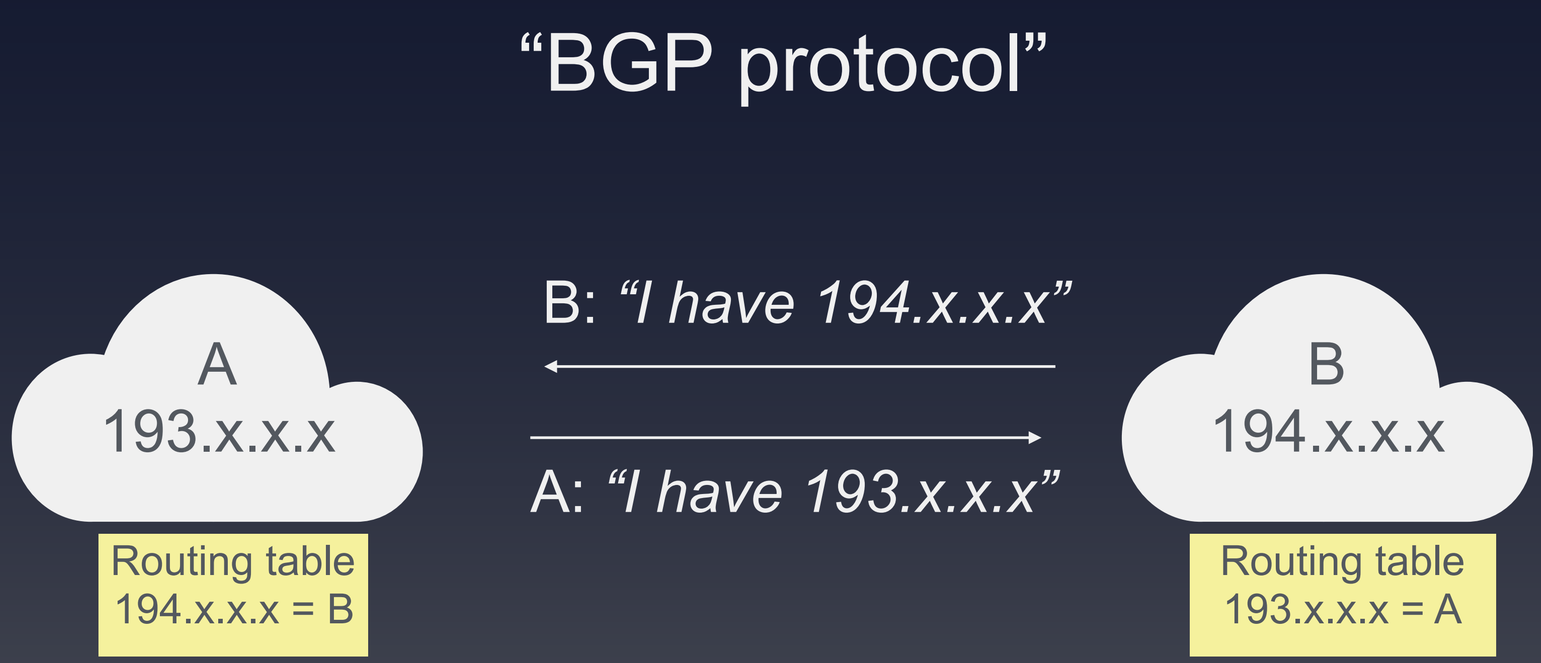
- In 1994, RIPE-181 was the first document published that used a common language to describe routing policies
- We co-developed standards for IRR and RPKI
- We are one of the five RPKI Trust Anchors
- Our Validator tool was, until recently, the only production-grade tool to do Origin Validation

Routing on the Internet

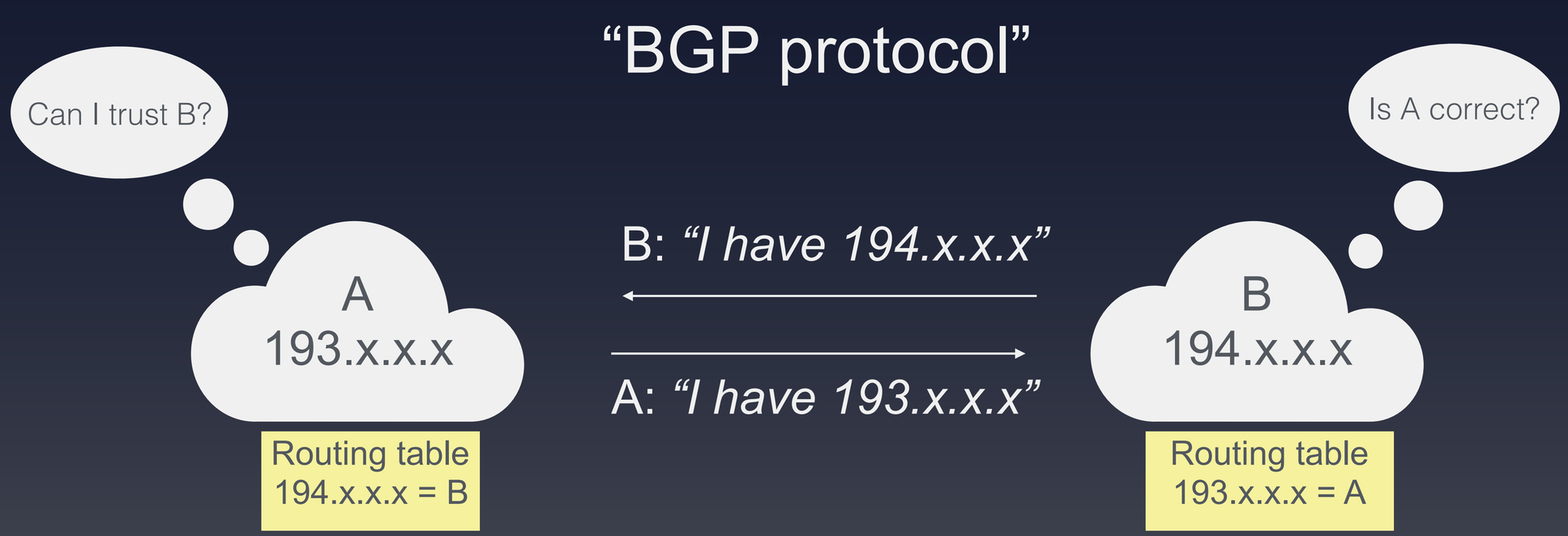
Routing on the Internet



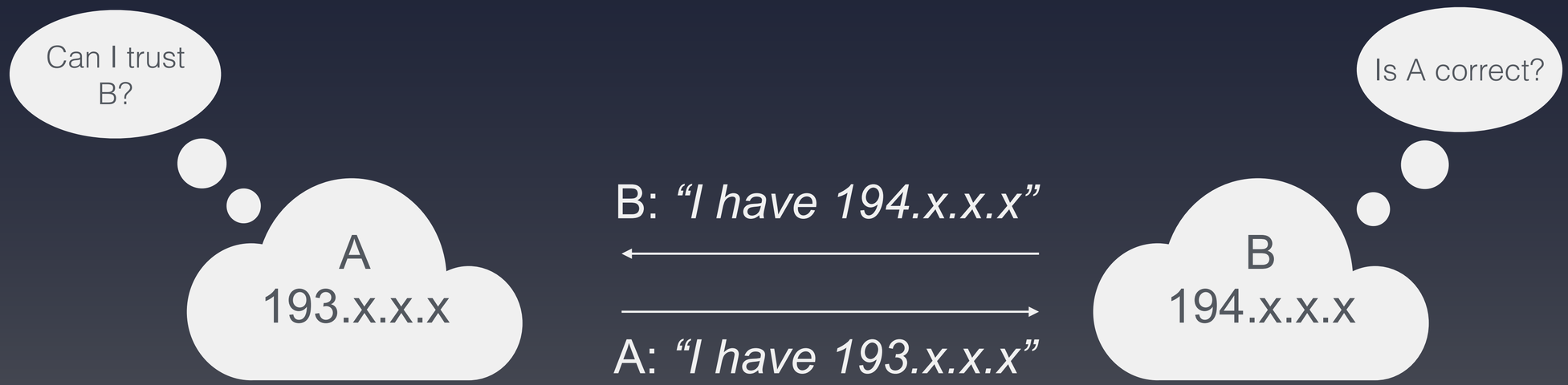
Routing on the Internet



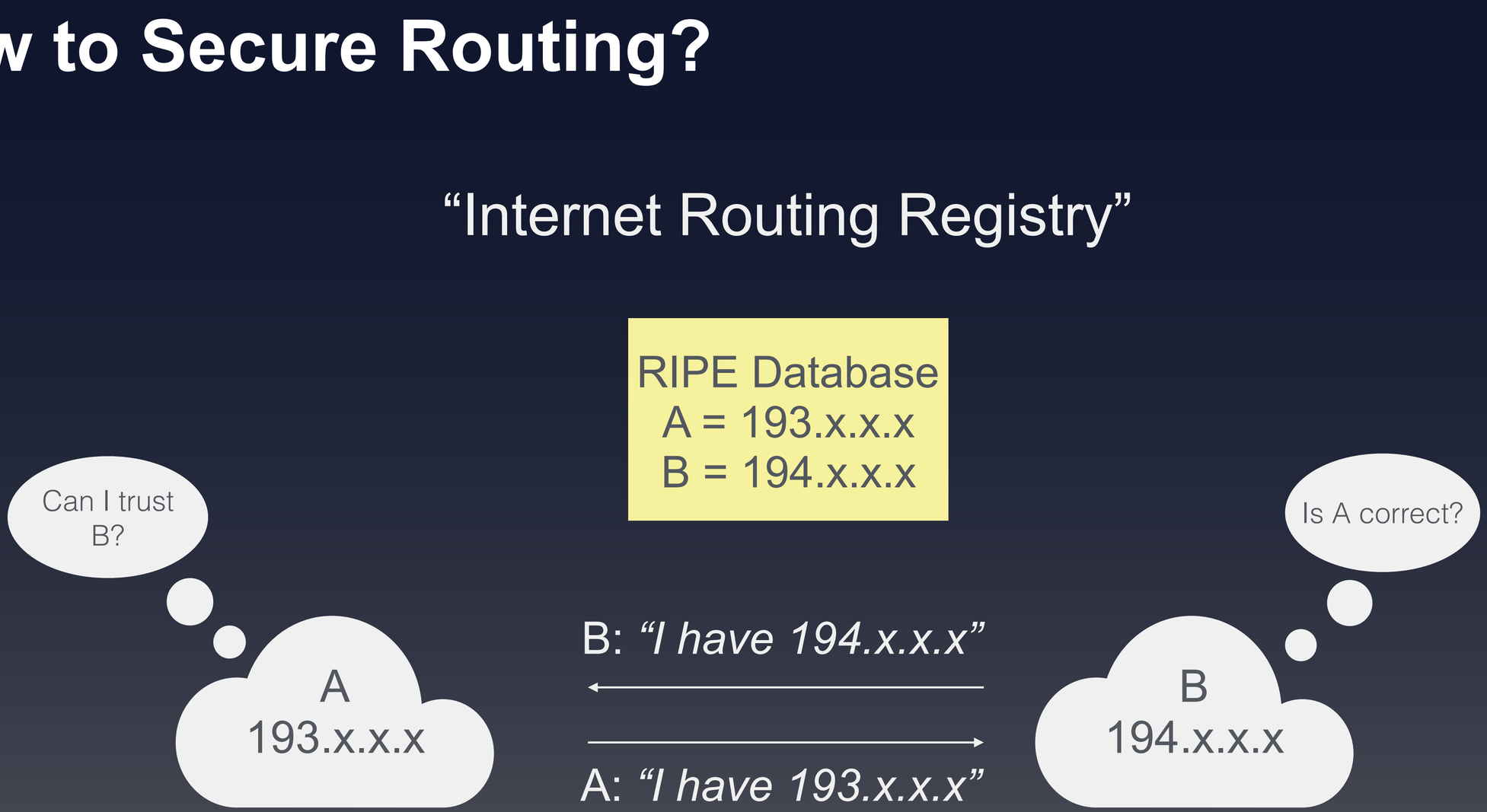
Routing on the Internet



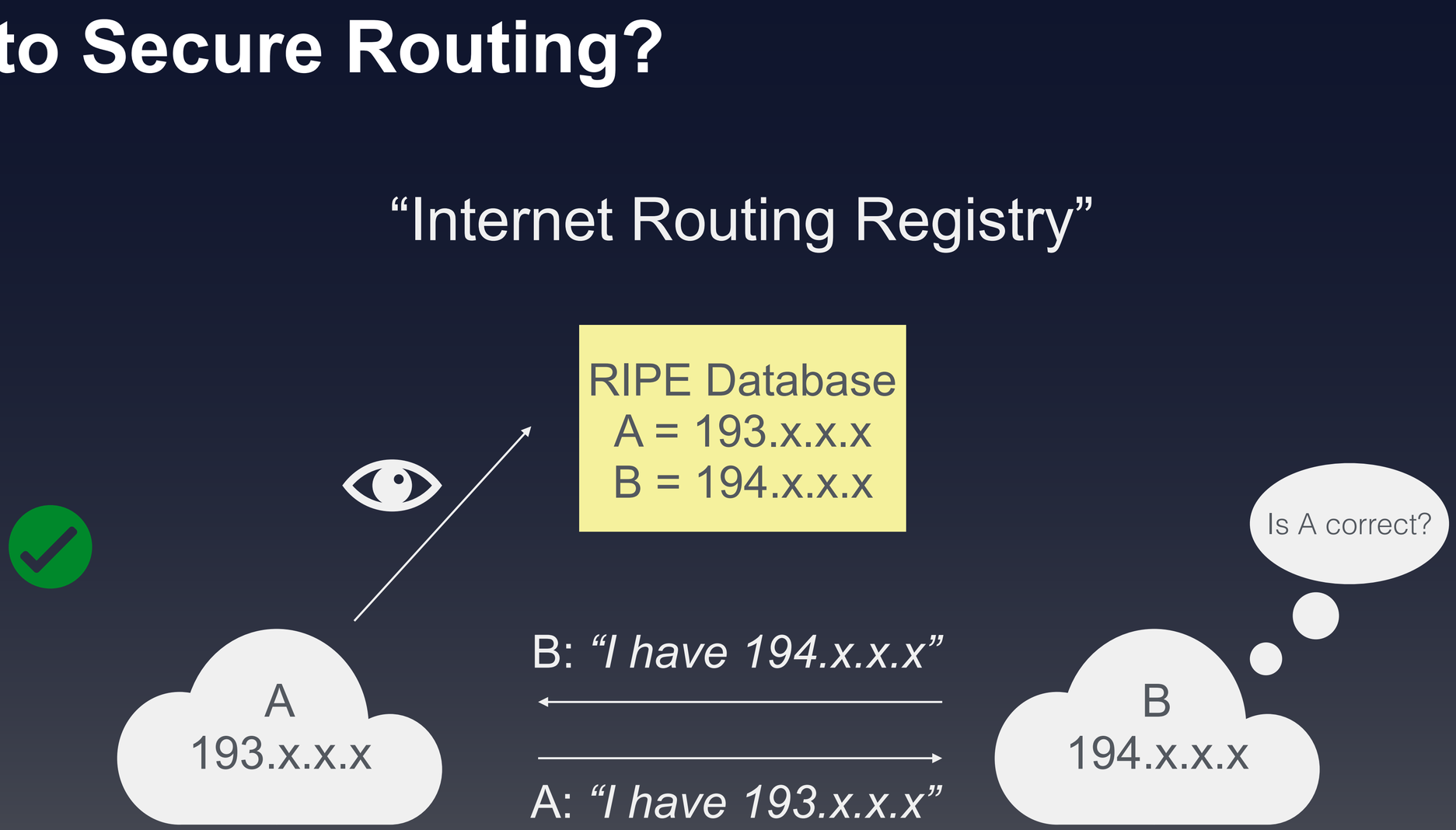
How to Secure Routing?



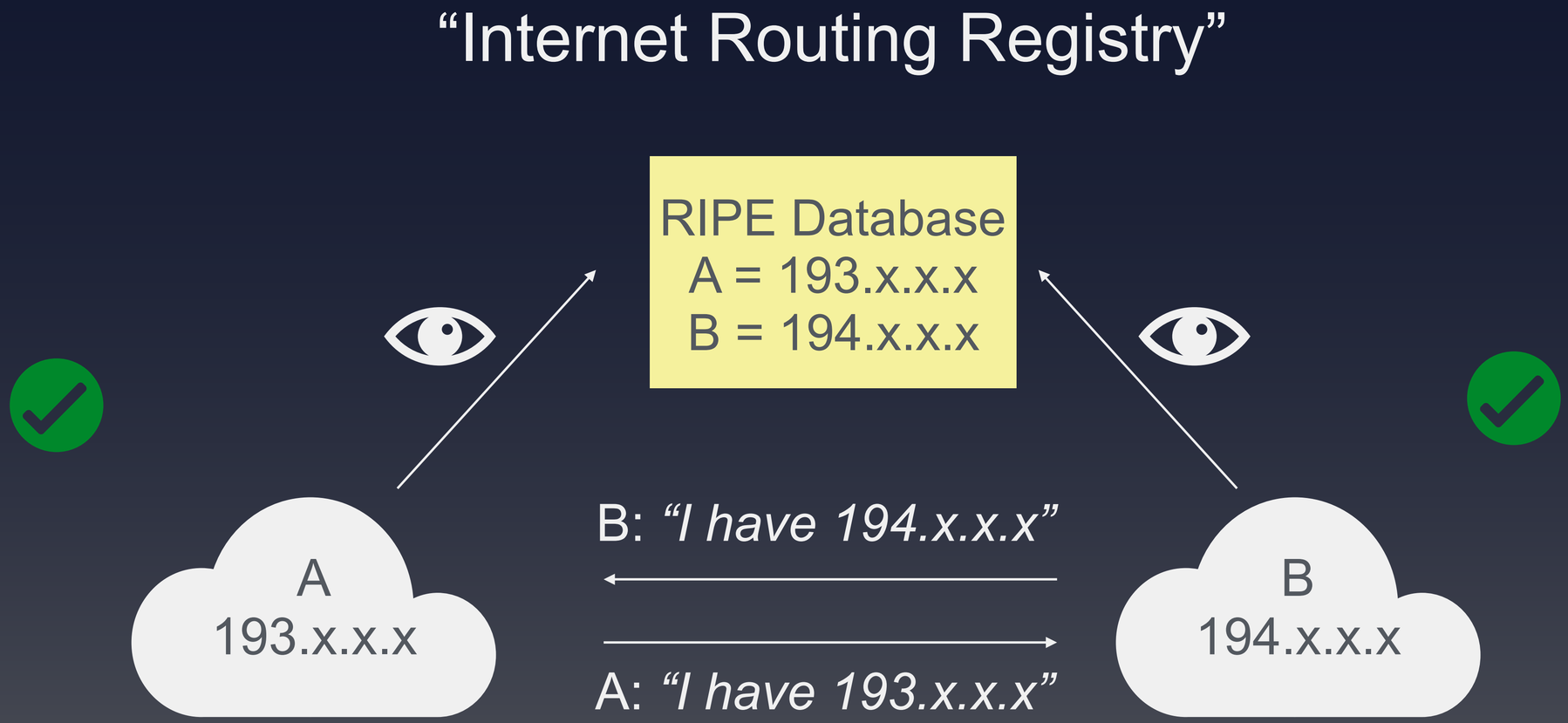
How to Secure Routing?



How to Secure Routing?



How to Secure Routing?



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

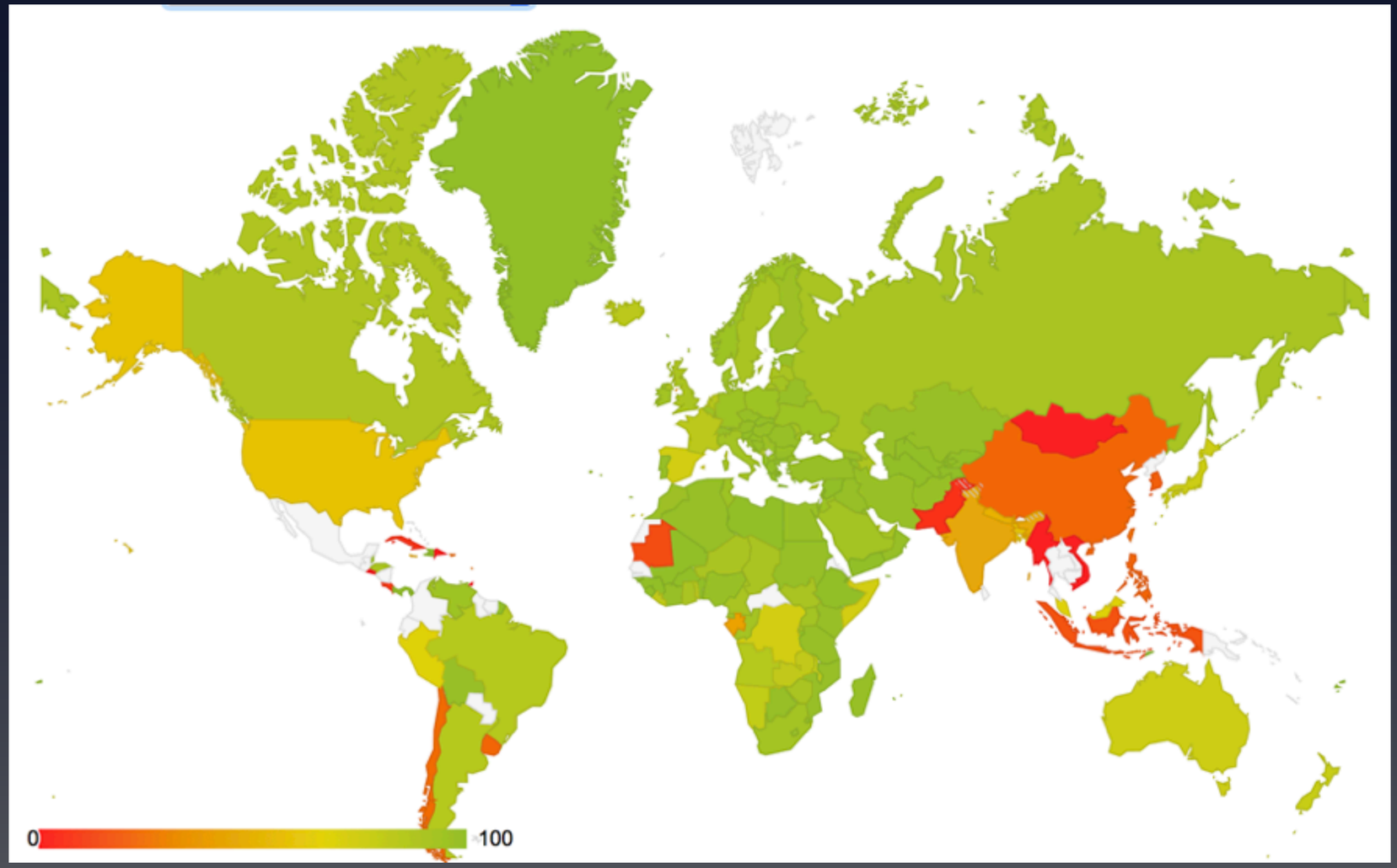
- **2018 Routing Security Review**
  - 12.6k incidents
  - 4.4% of all ASNs affected
  - 3k ASNs victims of at least one incident
  - 1.3k ASNs caused at least one incident

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

Internet Routing Registry

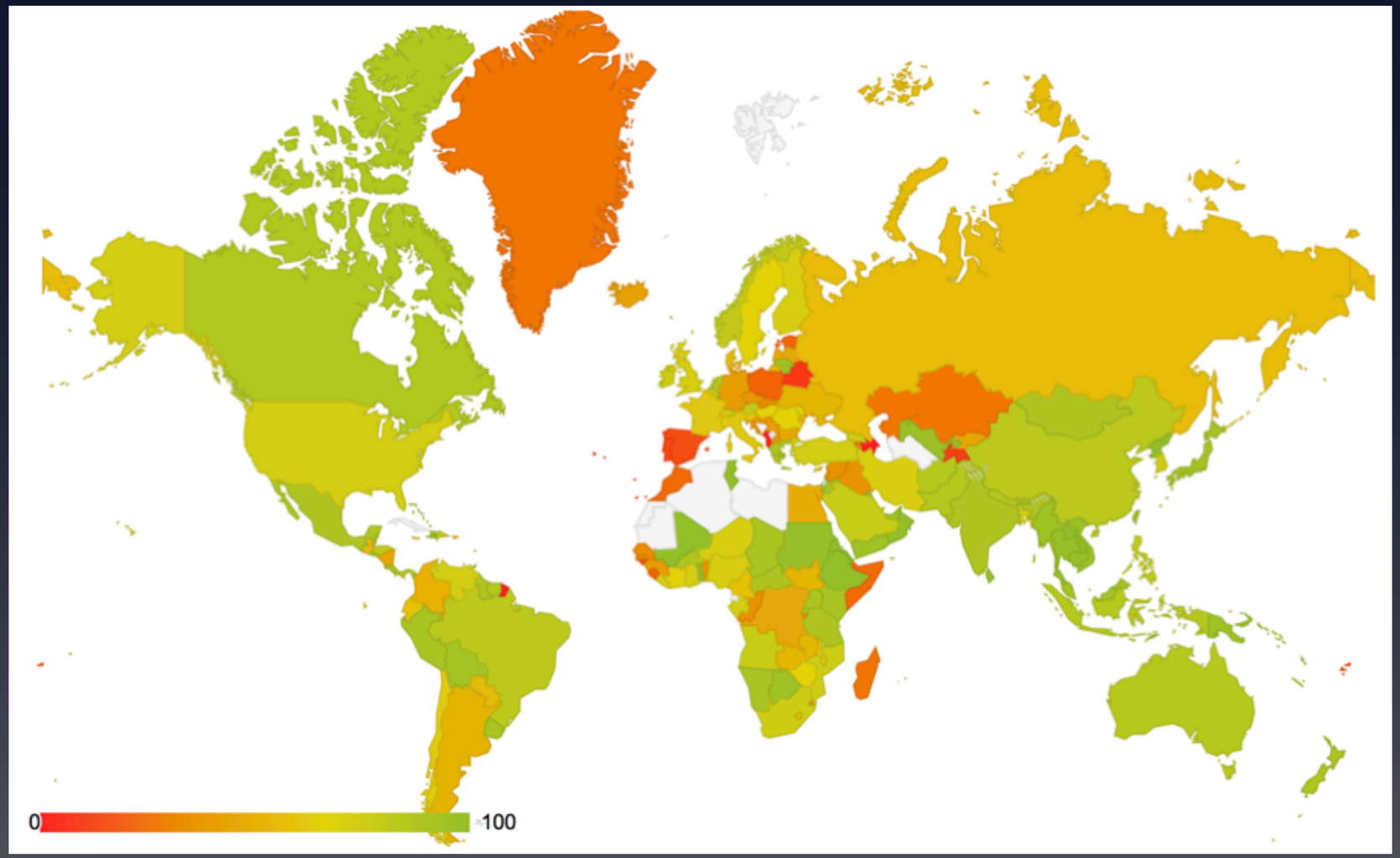
- Many exist, most widely used
  - RIPE Database
  - RADB
- Verification of holdership over resources
  - RIPE Database for RIPE region resources only
  - RADB allows paying customers to create any object
  - Lots of the other IRRs do not formally verify holdership

Accuracy - RIPE IRR



Accuracy - Valid announcements / covered announcements

Accuracy - RADB IRR



Accuracy - Valid announcements / covered announcements

Resource Public Key Infrastructure

- RPKI
  - Ties IP addresses and ASNs to public keys
  - Follows the hierarchy of the registry
- Authorised statements from resource holders
  - 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

Elements of RPKI

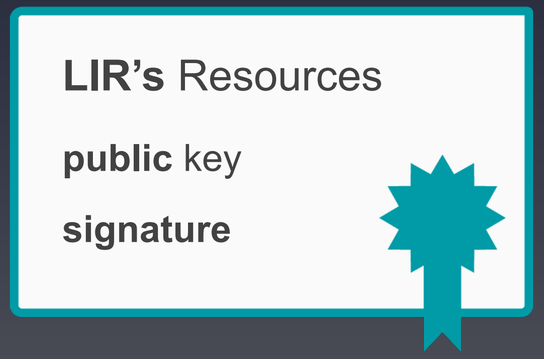
Signing

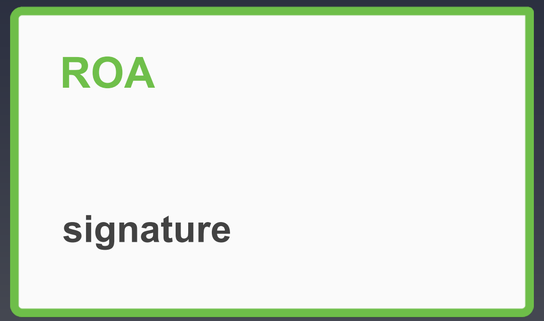
Create your ROAs

Validating

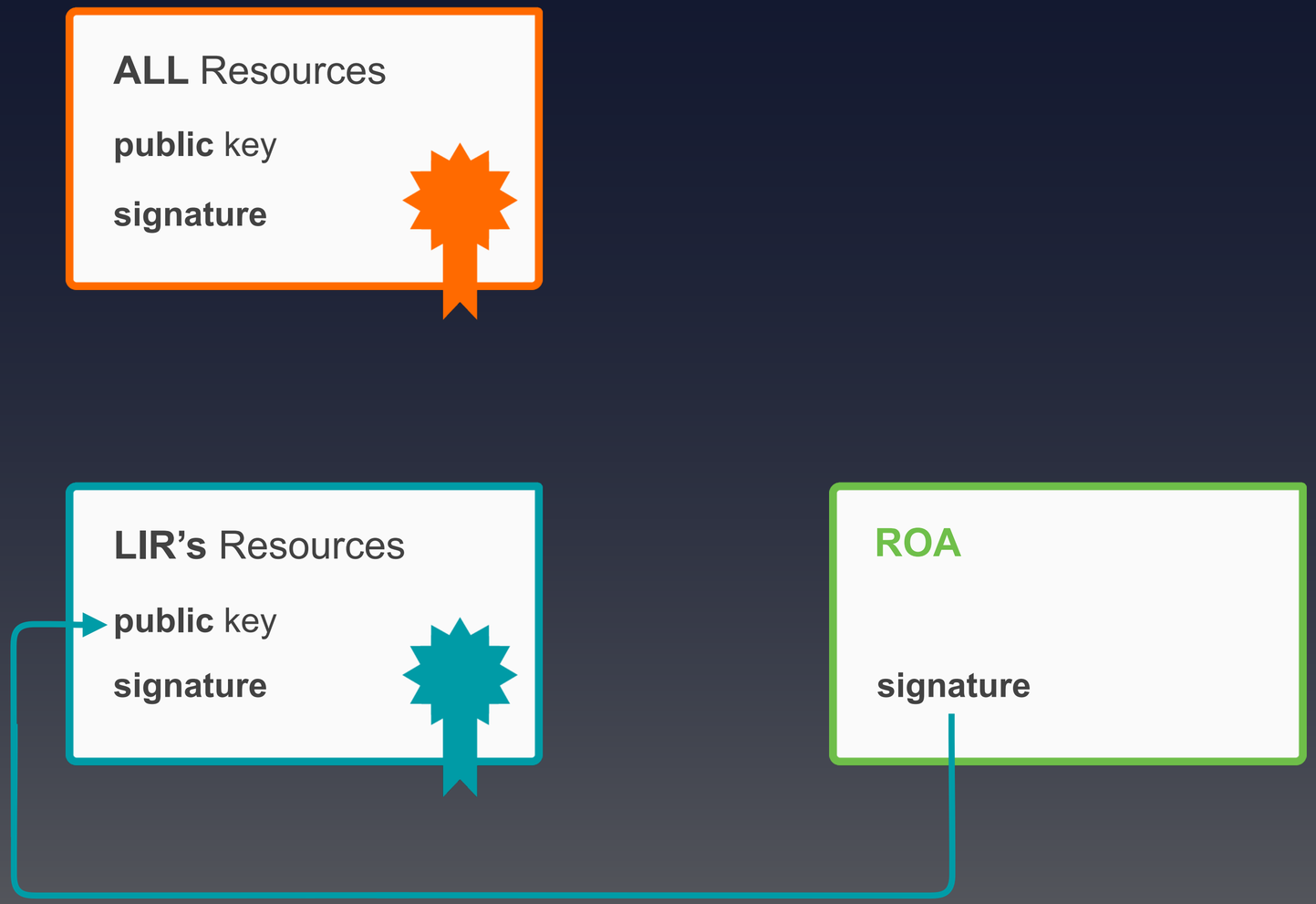
Verifying others

RPKI Chain of Trust

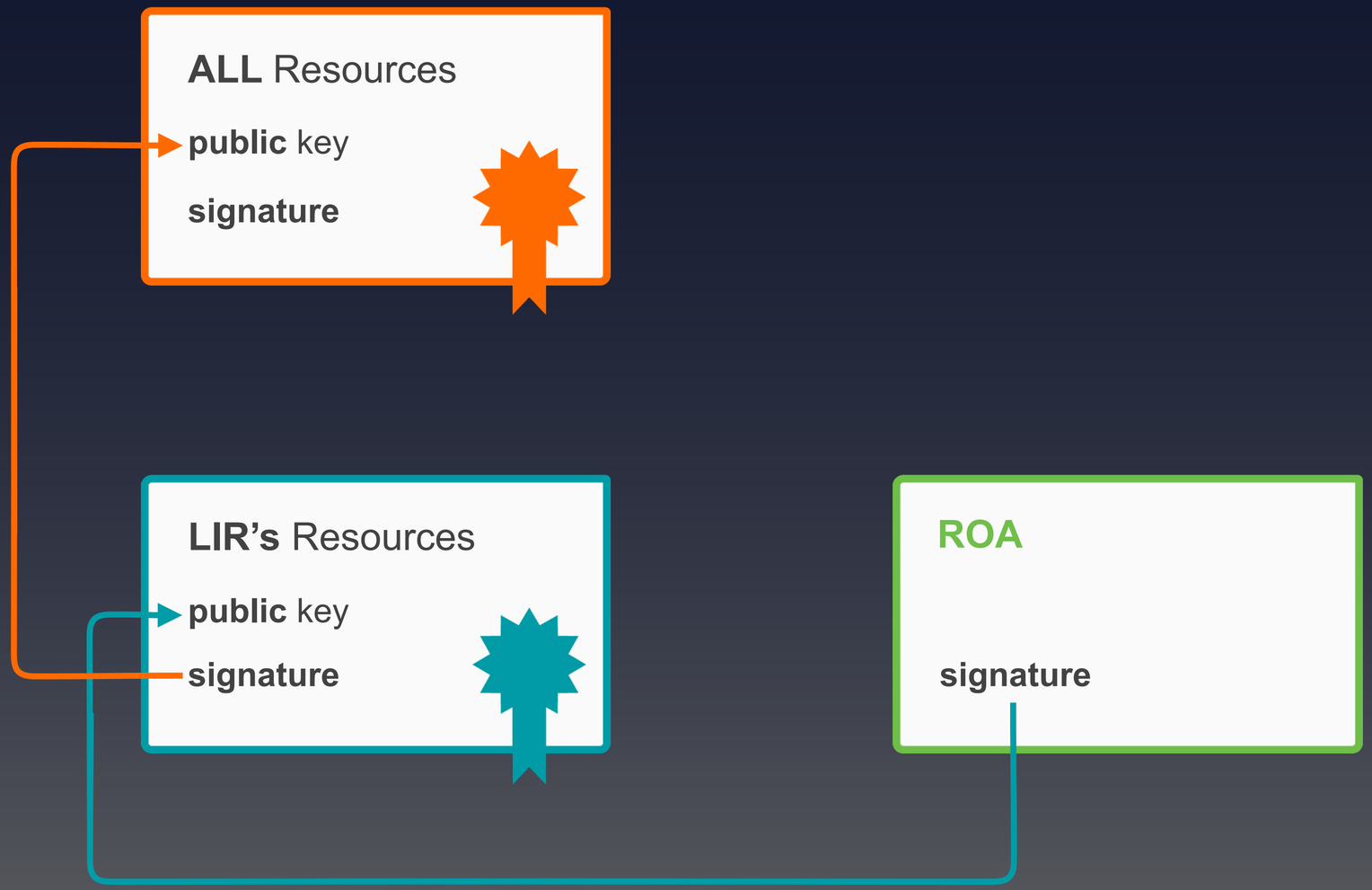




RPKI Chain of Trust



RPKI Chain of Trust



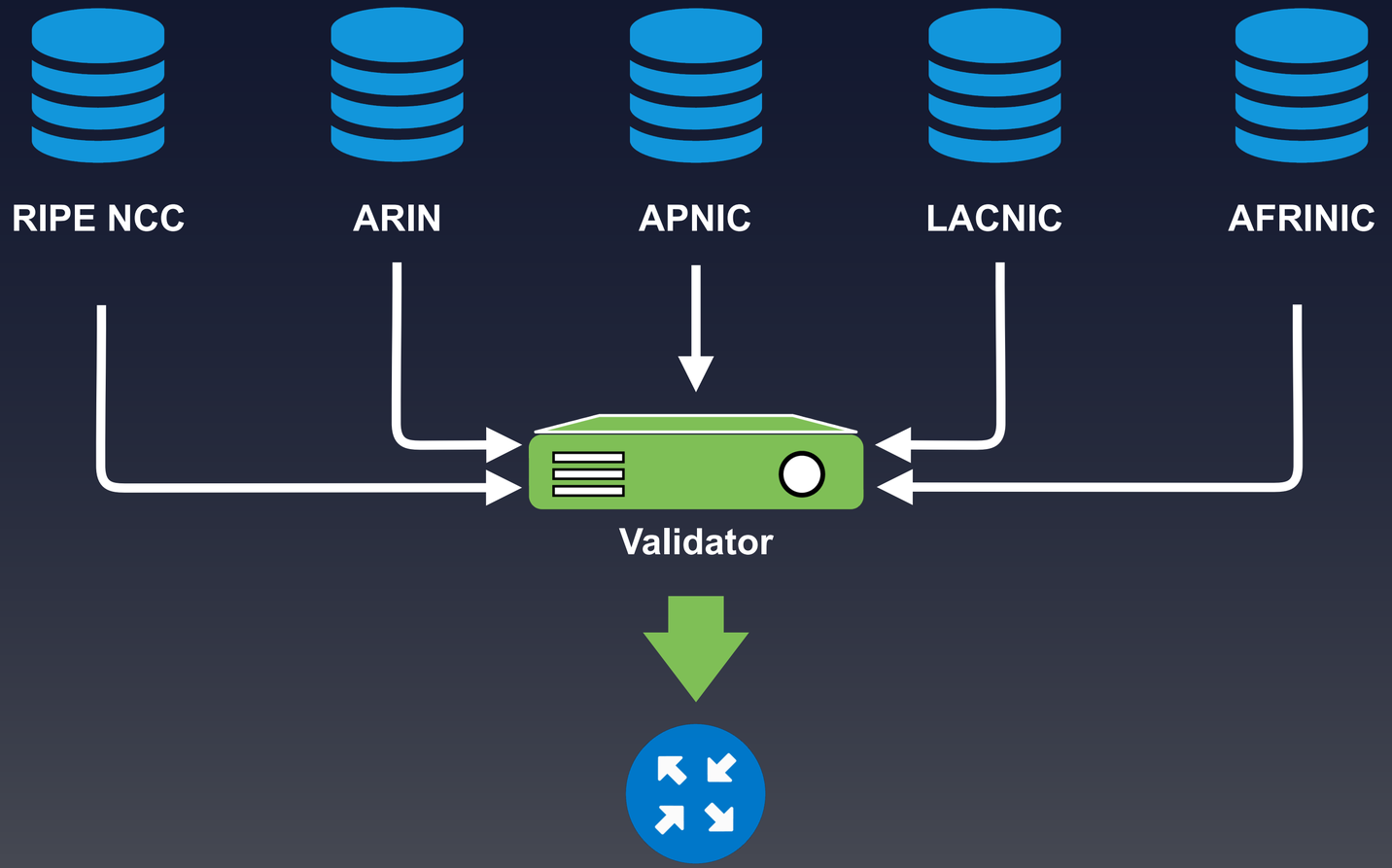
What's in a ROA

Prefix → The network for which you are creating the ROA

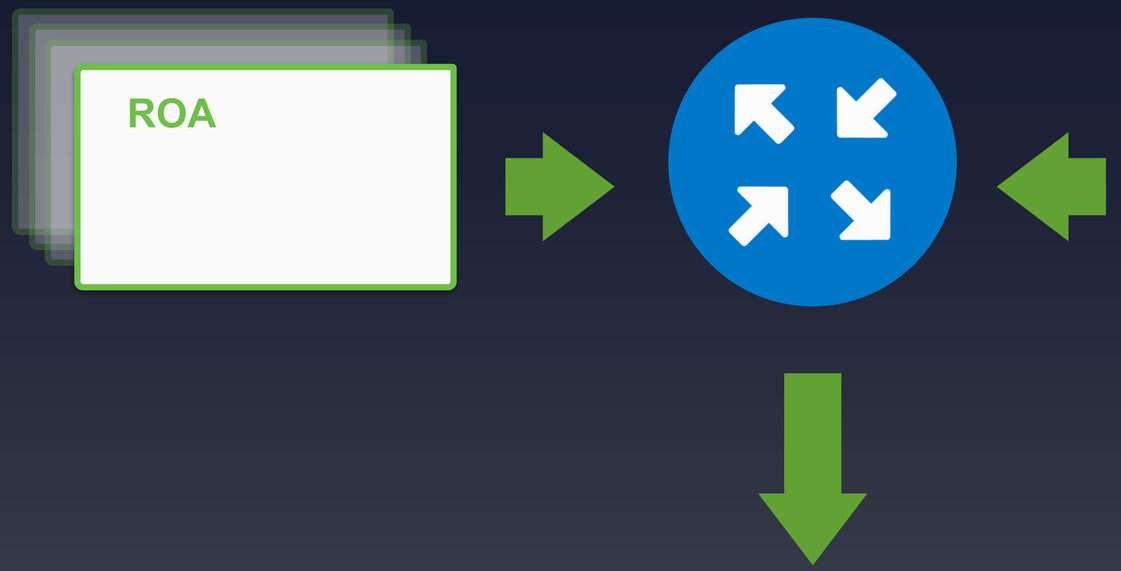
Origin ASN → The ASN supposed to be originating the BGP Announcement

Max Length → The Maximum prefix length accepted for this ROA

Route Origin Validation



Route Origin Validation

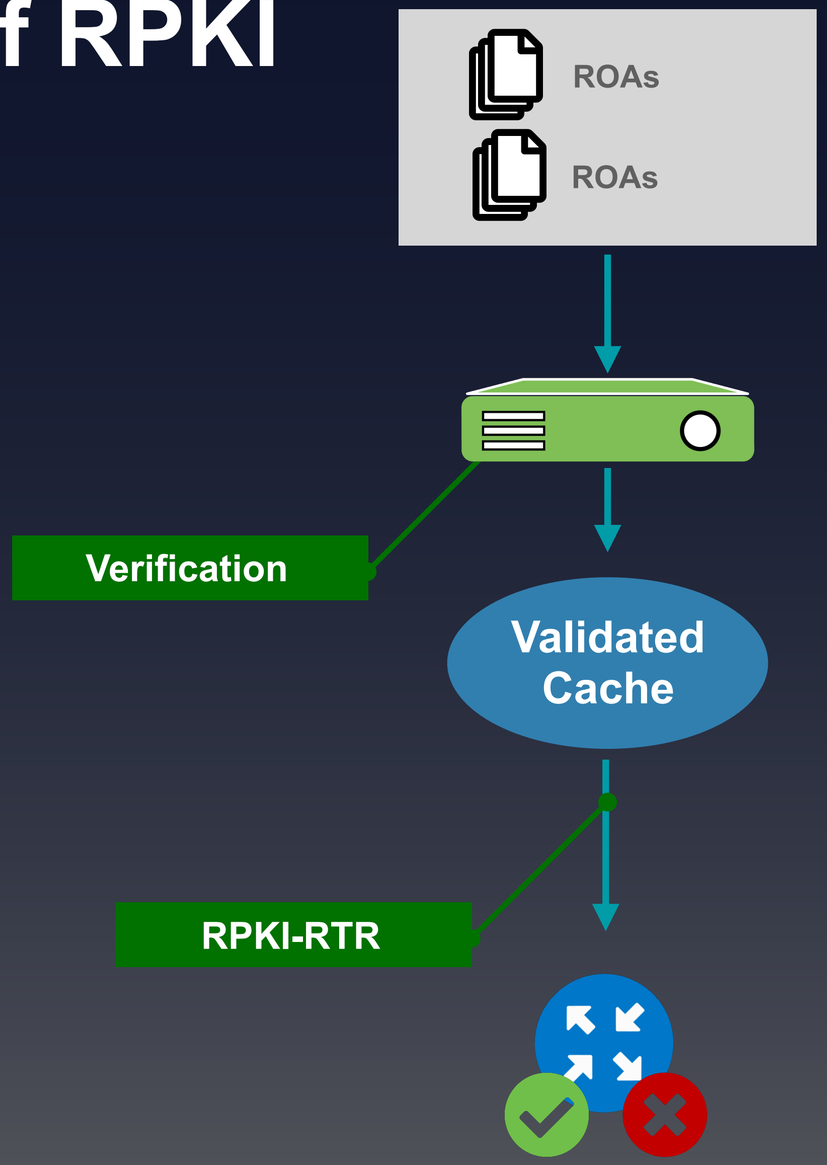


BGP Announcements

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

Elements of RPKI

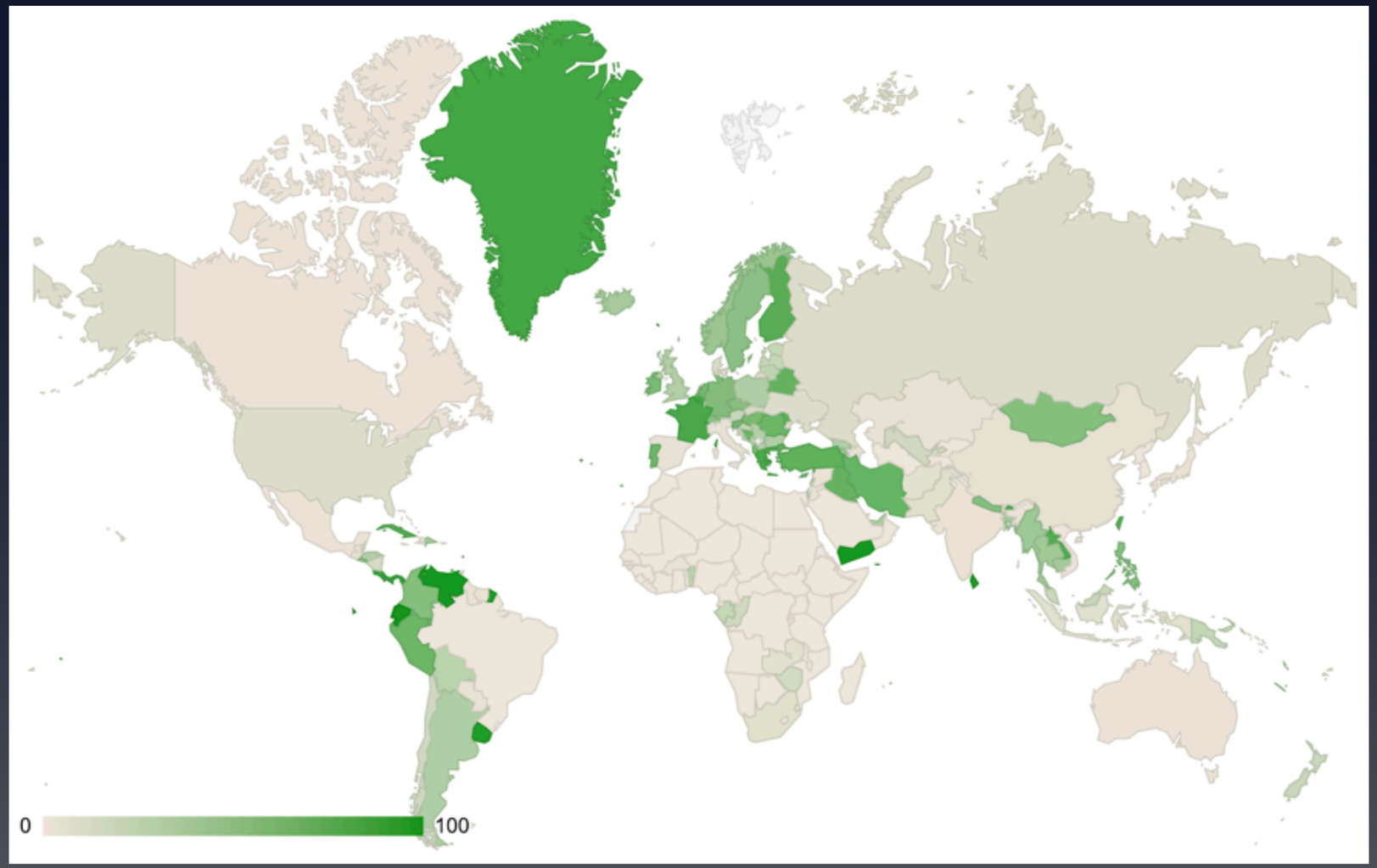


RIR REPOSITORIES

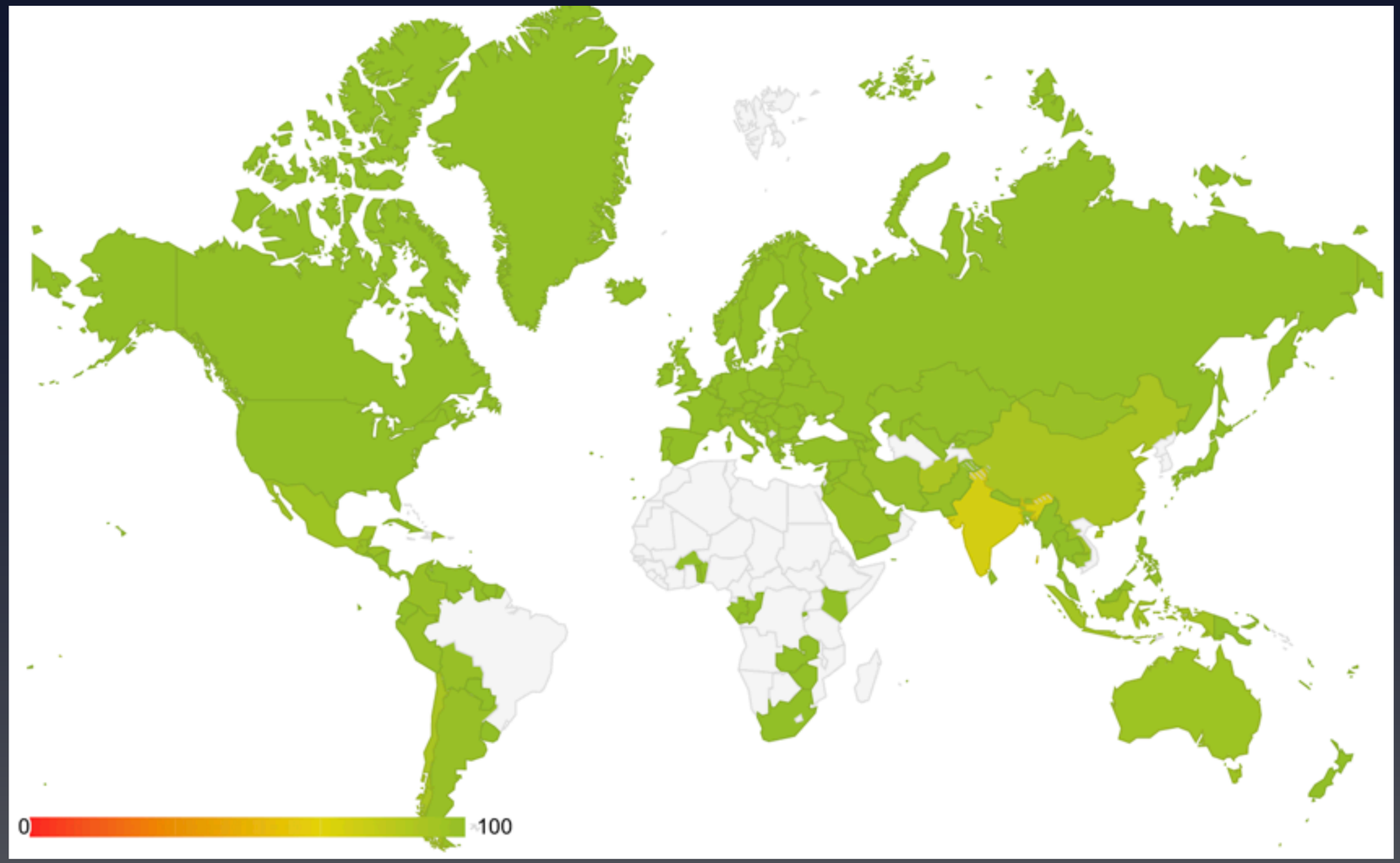
VALIDATOR SOFTWARE

ROUTERS

Coverage - RPKI (all RIRs)



Accuracy - RPKI (all RIRs)



IPv4 addresses in valid announcements / covered announcements

Recommendations to Get Started

- Create your ROAs in the LIR Portal
- Pay attention to the Max Length attribute
- Download and run a Validator
- Check validation status manually, which routes are invalid?
- Set up monitoring, for example pmacct
- (https://github.com/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

Making the Difference

- Is routing security on your agenda?
- Initiate the conversation with providers and colleagues

Are you leading by example ?

Questions

rpki@ripe.net