



RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Routing Security Toolset

The challenges of origin
validation

RIPE NCC



- Members organisation founded in 1992
- Manages IP and ASN allocations in Europe, Middle East and former Soviet Union
 - Ensure unique holdership
 - Document holdership in RIPE Database (whois)
 - Facilitate operators to document use of their addresses



Inter-Domain Routing

- Border Gateway Protocol
 - IETF Standard, RFC1105, 1989
 - BGPv2, 1990
 - BGPv3, 1991
 - BGPv4, 1994
 - Many other extensions...
- Problem remains
 - Any network (ASN) can announce any IP prefix
 - No built-in security in BGP protocol

Accidents Happen



Accidents Happen



- Fat Fingers
 - 2 and 3 are really close on our keyboards..
- Policy violations (leaks)
 - Oops, we didn't mean this to go the public internet
 - Infamous incident Pakistan Telecom blackholed YouTube, for the world..

Or worse..

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



<https://pixabay.com/en/burglar-crime-criminal-theft-thief-157142/>



Incidents are common

- 2017 Routing Security Review by Internet Society
 - 14k incidents
 - 10% of all ASNs affected
 - 3k ASN victim of at least one incident
 - 1.5k ASN caused at least one incident

<https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/>

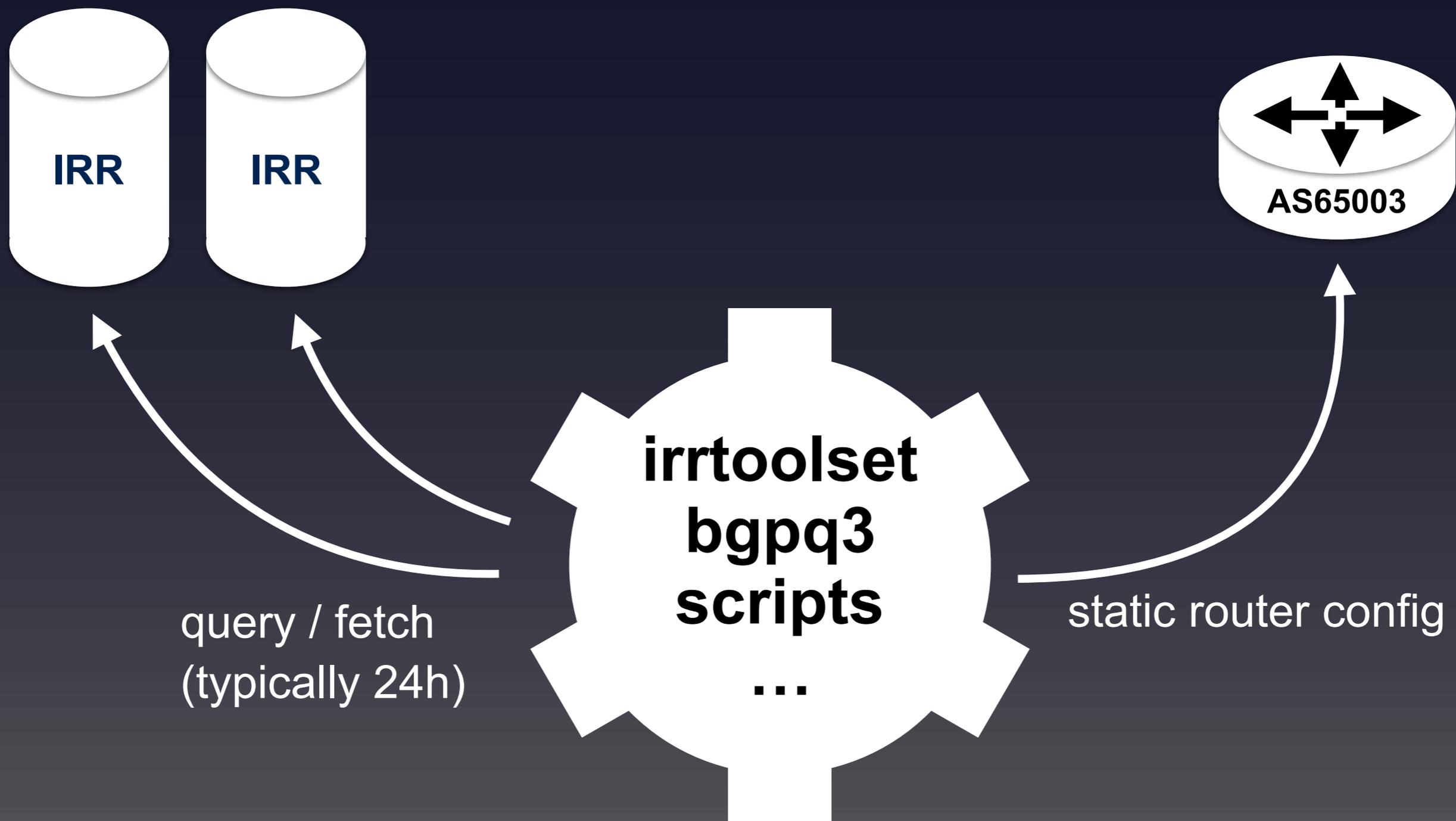


Internet Routing Registry



- Many exist, most widely used
 - RIPE Database
 - RADB
- Verification of holdership over resources
 - RIPE Database for RIPE region resources only
 - RIPE Database allows anyone to create out-of-region (deprecated)
 - RADB allows paying customers to create any object
 - Lot of other IRR don't formally verify holdership

Automate using IRR

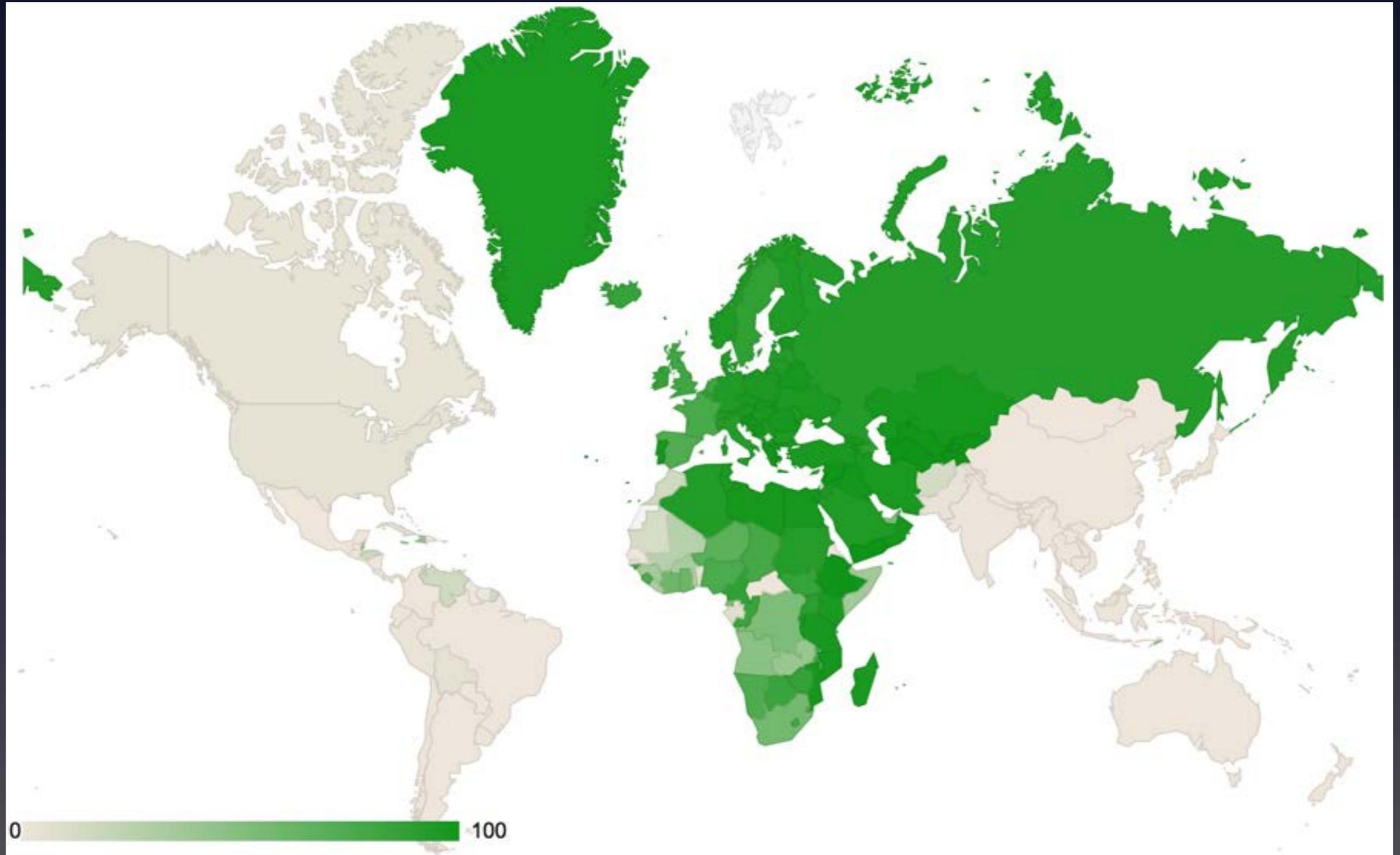


Filtering Value Proposition



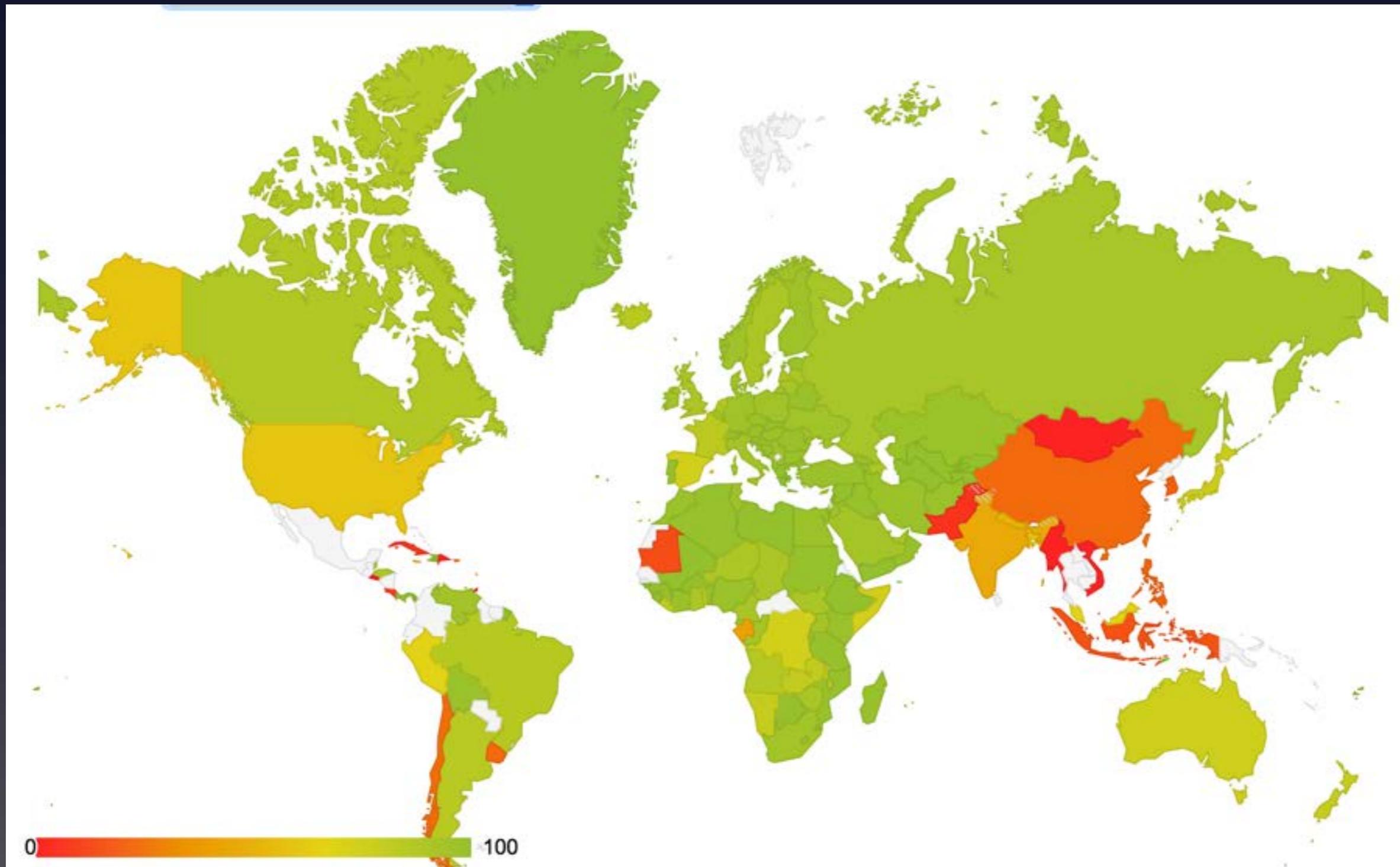
- Most commonly done by providers
- Internet Exchange points have started offering filtering as a service
- Transit providers usually do not filter
- Stub networks may filter because they want to block poisonous traffic

Coverage - RIPE IRR



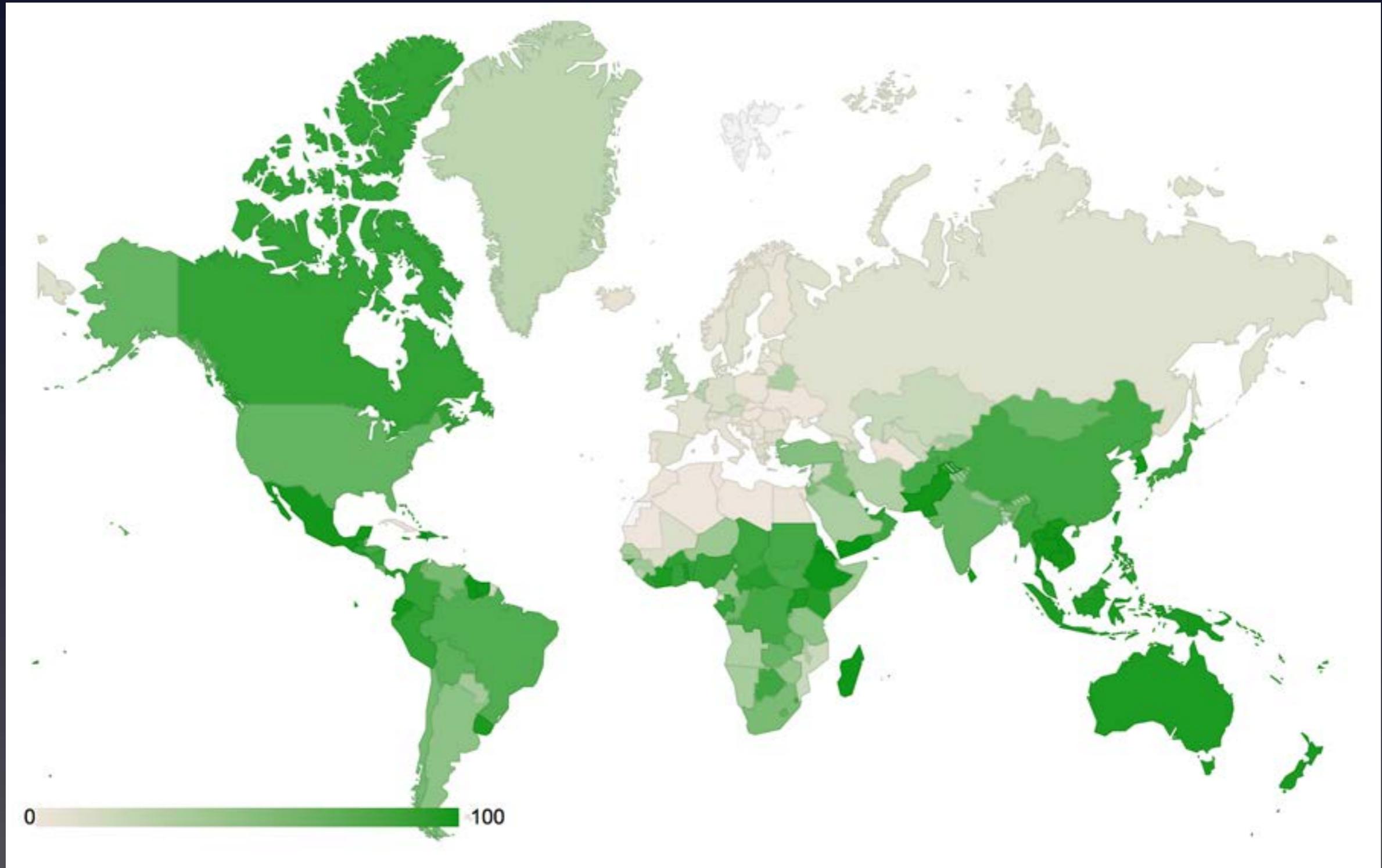
Fraction of IPv4 announcements valid according to ROUTE objects

Accuracy - RIPE IRR



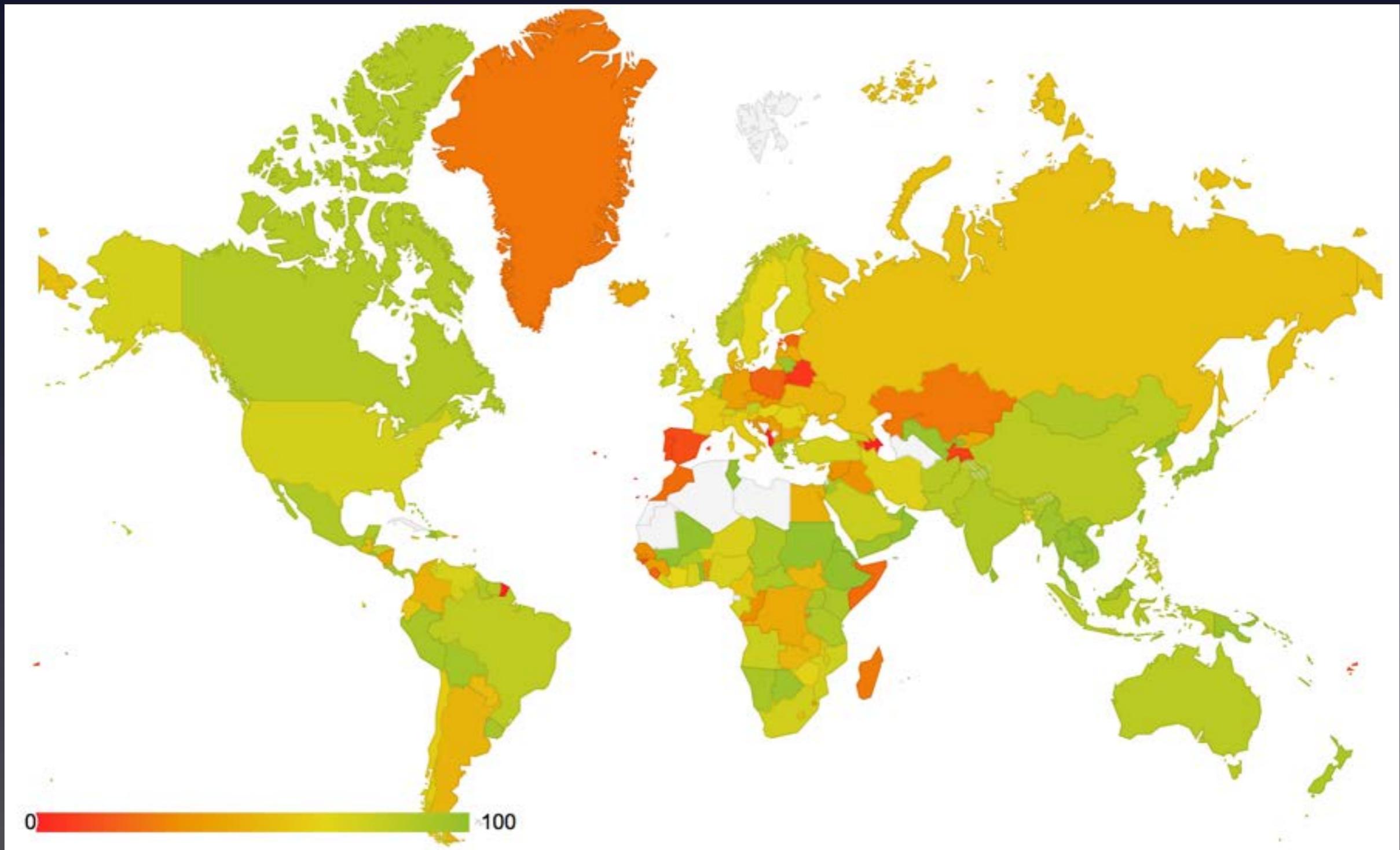
Accuracy - Valid announcements / covered announcements

Coverage - RADB IRR



Fraction of IPv4 announcements valid according to ROUTE objects

Accuracy - RADB IRR



Accuracy - Valid announcements / covered announcements



WE ARE
BETTER
THAN THIS!

Photo by Jerry Kiesewetter on Unsplash

Resource Public Key Infrastructure



- Resource Public Key Infrastructure
 - 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

Give me a button! — When I authorise



- We show members announcements
 - Member chooses to authorise, or not
 - No need to worry about the crypto
 - It's 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

How to set up ROAs



RPKI Dashboard 11 CERTIFIED RESOURCES ALERTS ARE SENT TO 1 ADDRESS

63 BGP Announcements 59 Valid 0 Invalid 0 Unknown **87 ROAs** 87 OK 0 Causing problems

BGP Announcements **Route Origin Authorisations (ROAs)** History

Create ROAs for selected BGP Announcements Valid Invalid Unknown

<input type="checkbox"/>	Origin AS	Prefix	Current Status	
<input type="checkbox"/>	AS3333	193.0.0.0/21	VALID	
<input type="checkbox"/>	AS3333	193.0.10.0/23	VALID	
<input type="checkbox"/>	AS3333	193.0.12.0/23	VALID	
<input type="checkbox"/>	AS3333	193.0.18.0/23	VALID	
<input type="checkbox"/>	AS3333	193.0.20.0/23	VALID	
<input type="checkbox"/>	AS3333	193.0.22.0/23	VALID	
<input type="checkbox"/>	AS3333	2001:67c:2e8::/48	VALID	
<input type="checkbox"/>	AS12654	2001:7fb:fd02::/48	VALID	
<input type="checkbox"/>	AS12654	2001:7fb:fd03::/48	INVALID ASN	
<input type="checkbox"/>	AS12654	2001:7fb:fe03::/48	VALID	

Show of 63 items Page 1 of 7

How to set up ROAs



RPKI Dashboard 11 CERTIFIED RESOURCES ALERTS ARE SENT TO 1 ADDRESS

63 BGP Announcements 59 Valid 0 Invalid 0 Unknown **87** ROAs 87 OK 0 Causing problems

BGP Announcements **Route Origin Authorisations (ROAs)** History

Fix announcement ×

Affected Announcement

AS number: AS12654, Prefix: 2001:7fb:fd03::/48, Max Length: 48 Create ROA

ROAs currently invalidating this announcement

AS number: AS196615, Prefix: 2001:7fb:fd03::/48, Max Length: 48 INVALID ASN

Manual fix

AS Number	Prefix	Max length	Add ROA
<input type="checkbox"/> AS12654	2001:7fb:fd02::/48	VALID	✕
<input type="checkbox"/> AS12654	2001:7fb:fd03::/48	INVALID ASN MUTED	🔔 ✎
<input type="checkbox"/> AS12654	2001:7fb:fe03::/48	VALID	✕

Show of 63 items Page 1 of 7 ⏪ ⏩

How to set up ROAs



RPKI Dashboard 11 CERTIFIED RESOURCES ALERTS ARE SENT TO 1 ADDRESS

63 BGP Announcements 59 Valid 0 Invalid 0 Unknown **87 ROAs** 87 OK 0 Causing problems

BGP Announcements **Route Origin Authorisations (ROAs)** History

Create ROAs for selected BGP Announcements Valid Invalid Unknown

<input type="checkbox"/>	Origin AS	Prefix	Current Status	Future Status
<input type="checkbox"/>	AS3333	193.0.0.0/21	VALID	
<input type="checkbox"/>	AS3333	193.0.10.0/23	VALID	
<input type="checkbox"/>	AS3333	193.0.12.0/23	VALID	
<input type="checkbox"/>	AS3333	193.0.18.0/23	VALID	
<input type="checkbox"/>	AS3333	193.0.20.0/23	VALID	
<input type="checkbox"/>	AS3333	193.0.22.0/23	VALID	
<input type="checkbox"/>	AS3333	2001:67c:2a9::/48	VALID	
<input type="checkbox"/>	AS12654			
<input type="checkbox"/>	AS12654			
<input type="checkbox"/>	AS12654			

Show 10 of

Publish Continue making changes Discard changes

Review and publish changes 1

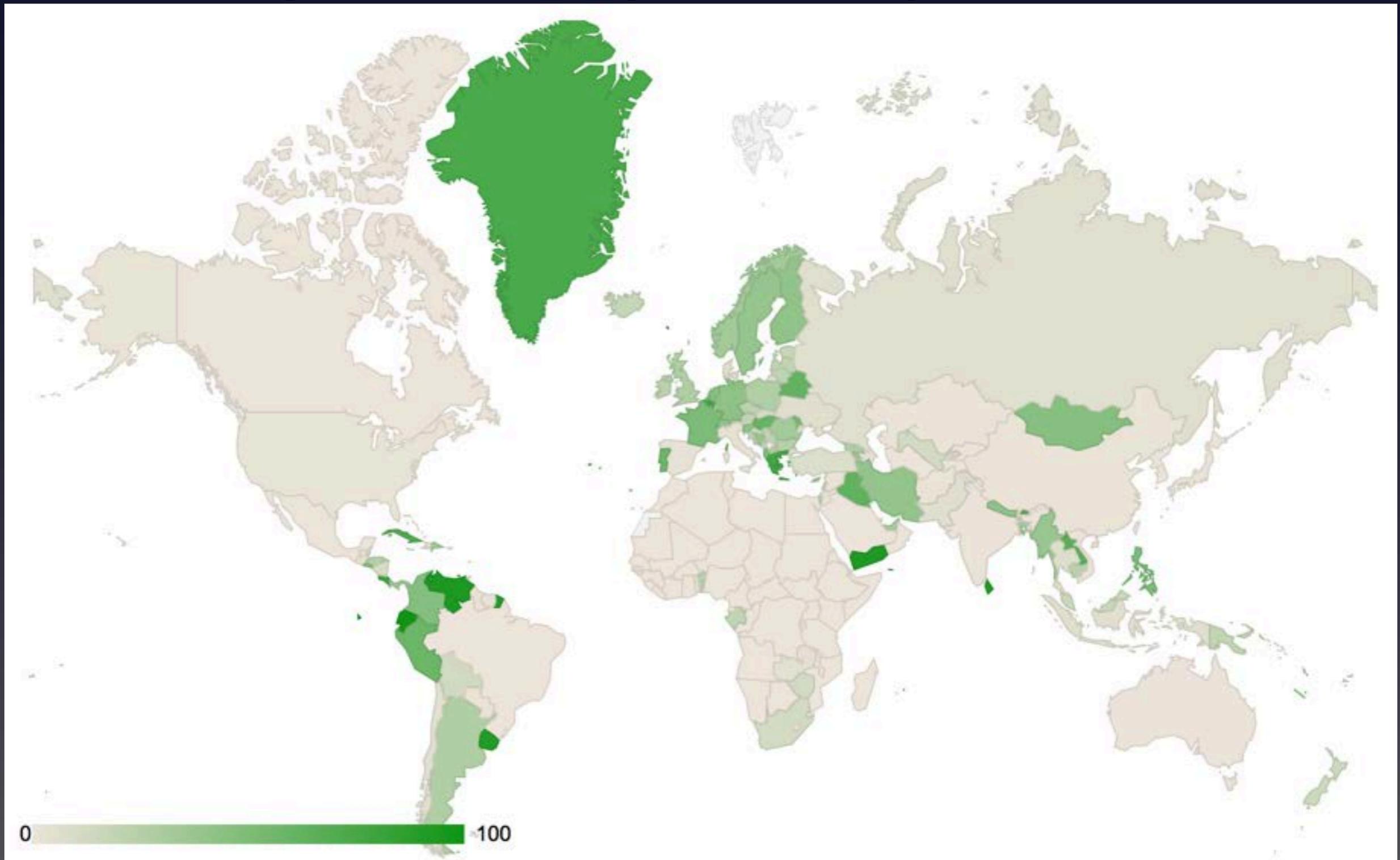
Staged ROAs

AS12654 2001:7fb:fd03::/48 → 48

Affected announcements

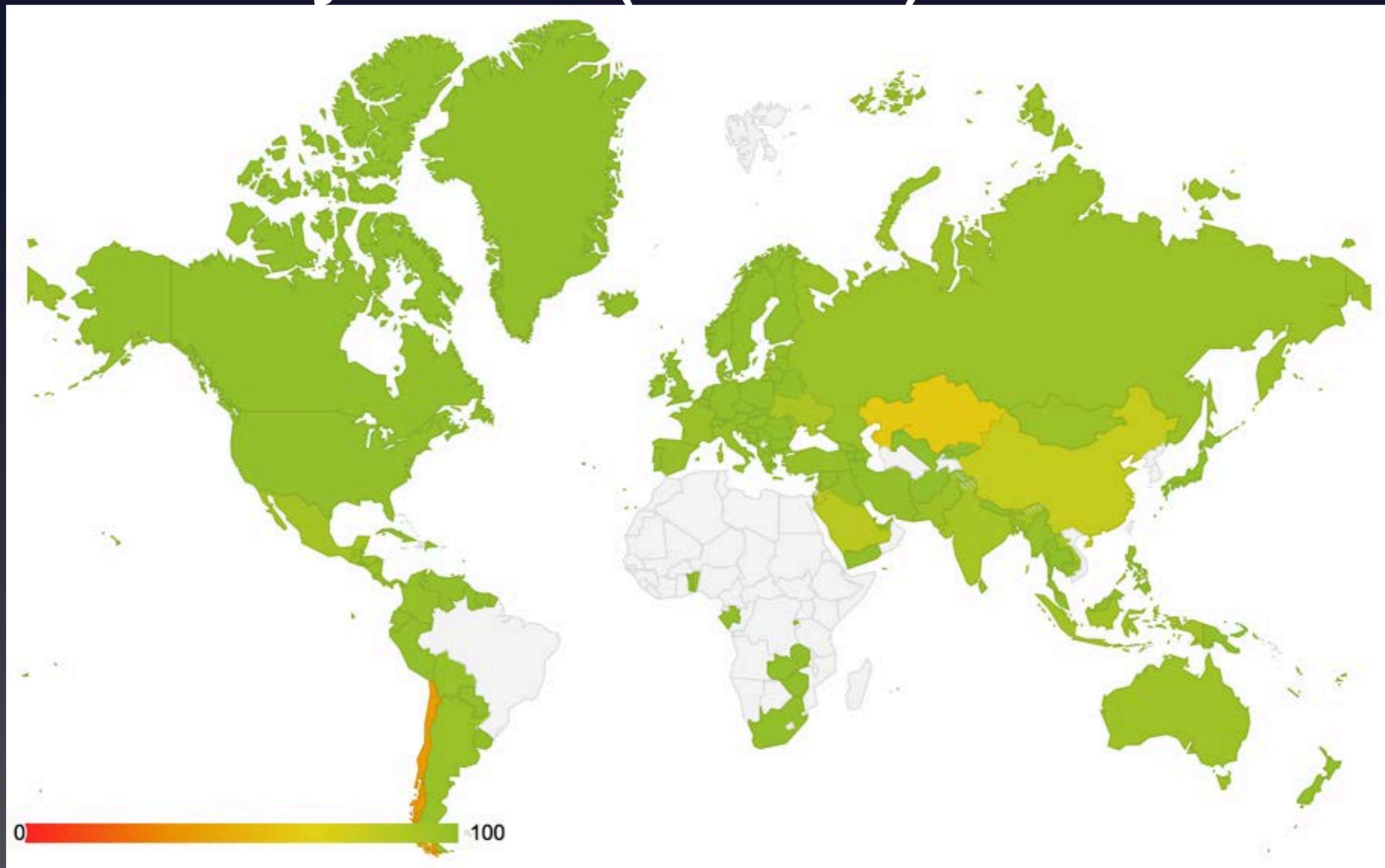
AS12654 2001:7fb:fd03::/48 INVALID ASN → VALID

Coverage - RPKI (all RIRs)



Fraction of IPv4 announced addresses valid according to ROAs

Accuracy - RPKI (all RIRs)



IPv4 addresses in valid announcements / covered announcements

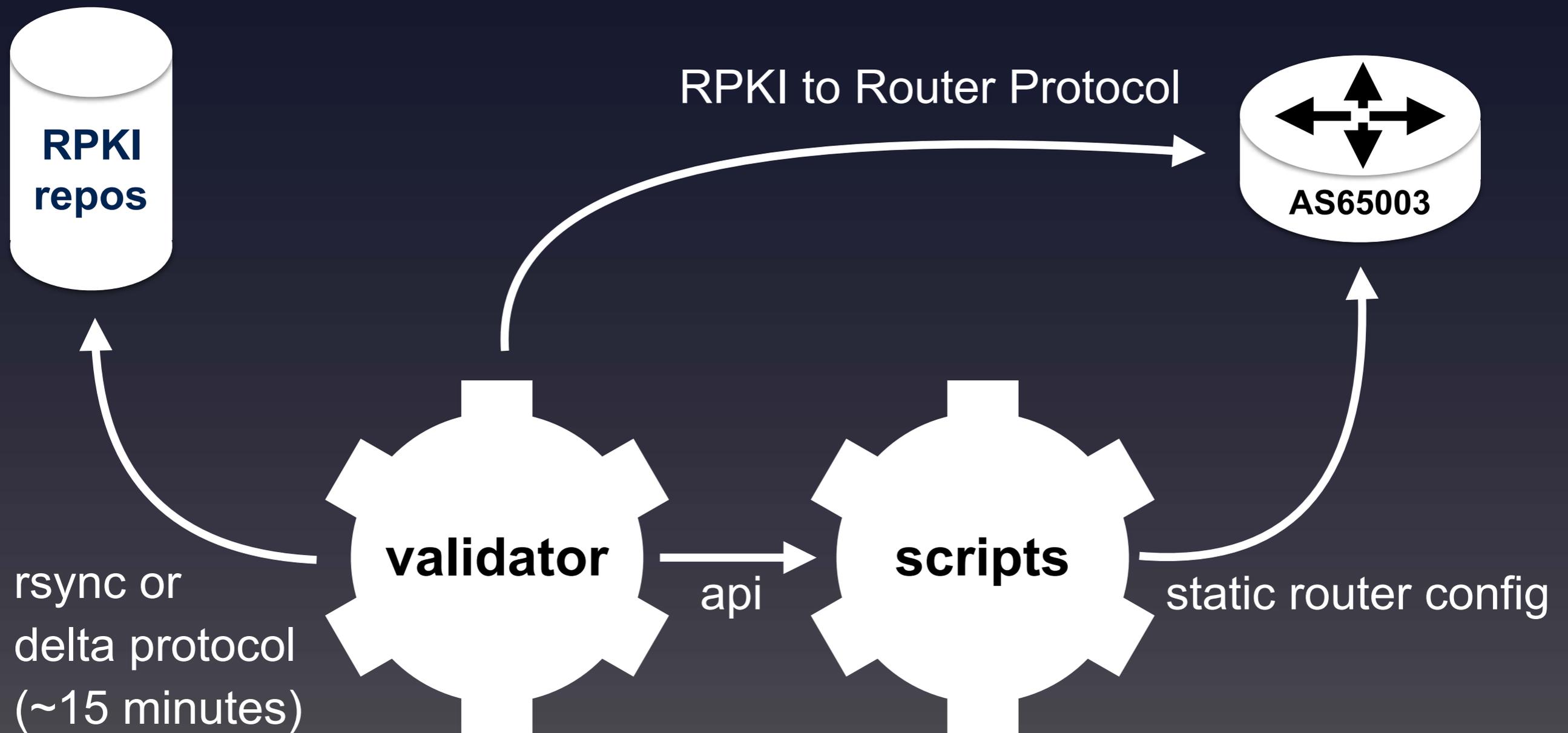
RPKI in some European countries



Country	% Prefixes	% Addresses	Accuracy
NL	25%	44%	99,9%
BE	27%	78%	100,0%
DE	17%	42%	100,0%
FR	26%	50%	96,9%
GB	14%	26%	99,9%
IE	20%	21%	99,9%
FI	20%	40%	100,0%
SE	12%	38%	100,0%
GR	46%	75%	100,0%
CZ	13%	23%	99,9%
SK	13%	10%	100,0%

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

Give me a button! — When I validate



Search through validated ROAs



RPKI Validator [Trust Anchors](#) [ROAs](#) [Ignore Filters](#) [Whitelist](#) [BGP Preview](#) [Announcement Preview](#)

Validated ROAs

Show entries Search:

ASN	Prefix	Max Length	Trust Anchors	URI of ROA
AS13335	1.0.0.0/24	24	APNIC RPKI Root	🔗
AS13335	1.1.1.0/24	24	APNIC RPKI Root	🔗
AS4788	1.9.0.0/16	24	APNIC RPKI Root	🔗
AS65037	1.9.12.0/24	24	APNIC RPKI Root	🔗
AS24514	1.9.21.0/24	24	APNIC RPKI Root	🔗
AS65120	1.9.23.0/24	24	APNIC RPKI Root	🔗
AS65077	1.9.31.0/24	24	APNIC RPKI Root	🔗
AS24514	1.9.65.0/24	24	APNIC RPKI Root	🔗
AS4760	1.36.0.0/16	16	APNIC RPKI Root	🔗
AS4760	1.36.0.0/19	19	APNIC RPKI Root	🔗

« « 1 2 3 4 5 » » Showing 1 to 10 of 52137 entries

Export

Here you are able to export the complete ROA data set for use in an existing BGP decision making workflow. The output will be in CSV or JSON format and consist of all validated ROAs, minus your ignore filter entries, plus your whitelist additions.

[Get CSV](#) [Get JSON](#)

Manage local exceptions



RPKI Validator [Trust Anchors](#) [ROAs](#) [Ignore Filters](#) **Whitelist** [BGP Preview](#) [Announcement Preview](#)

Whitelist

By adding a whitelist entry you can manually authorise an ASN to originate a prefix in addition to the validated ROAs from the repository. Please note that whitelist entries may **invalidate** announcements for this prefix from other ASNs, just like ROAs. This may be intentional (you are whitelisting ASN A, ASN B is hijacking), or not (ASN B should also be authorised, or you made a mistake). When you create a whitelist entry here, make sure to check the table below for a report on prefixes validated / invalidated by this entry and verify that no unintentional side effects occurred.

Add entry

Prefix: Origin: Maximum prefix length:

Comment:

Current entries

Show entries Search:

Prefix	ASN	Maximum prefix length	Validates	Invalidates	Comment	
193.0.0.0/21	1		0 announcement(s)	1 announcement(s)	Want this to be valid here	<input type="button" value="⊘"/>

Showing 1 to 1 of 1 entries

SLURM

Download or upload SLURM file.

Analyse any announcement



RPKI Validator Trust Anchors ROAs Ignore Filters Whitelist BGP Preview Announcement Preview

Announcement Preview

ASN: AS3333 Prefix: 193.0.0.0/21 Status: **INVALID ASN**

Relevant Validated ROAs

ASN	Prefix	Max Length	Source	URI	Status
AS1	193.0.0.0/21		Whitelist		INVALID ASN
AS3333	193.0.0.0/21	21	RIPE NCC RPKI Root	🔗	FILTERED VALID

 RIPE NCC Copyright ©2009-2018 the Réseaux IP Européens Network Coordination Centre RIPE NCC. All rights reserved.



RPKI Validator references

- RIPE NCC RPKI Validator 2.24
<https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources>
- RIPE NCC RPKI Validator 3
<https://github.com/RIPE-NCC/rpki-validator-3/wiki>
 - Release Candidate out NOW
 - Please try it! Your feedback is much appreciated
- Rcynic
<https://github.com/dragonresearch/rpki.net/>
- RPSTIR
<https://github.com/bgpsecurity/rpstir>



Questions



awolski@ripe.net
@taihen