RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Securing the Internet's Backbone - Exploring RPKI

ENISA Telecom & DI Security Forum 2024

RIPE NCC | Jad El Cham | May 2024

Agenda

Problem Statement

- Is Internet Routing secure?

Routing Incidents

- Causes and Impact

Routing Security with RPKI

- What is RPKI and how does it works?

RPKI Adoption

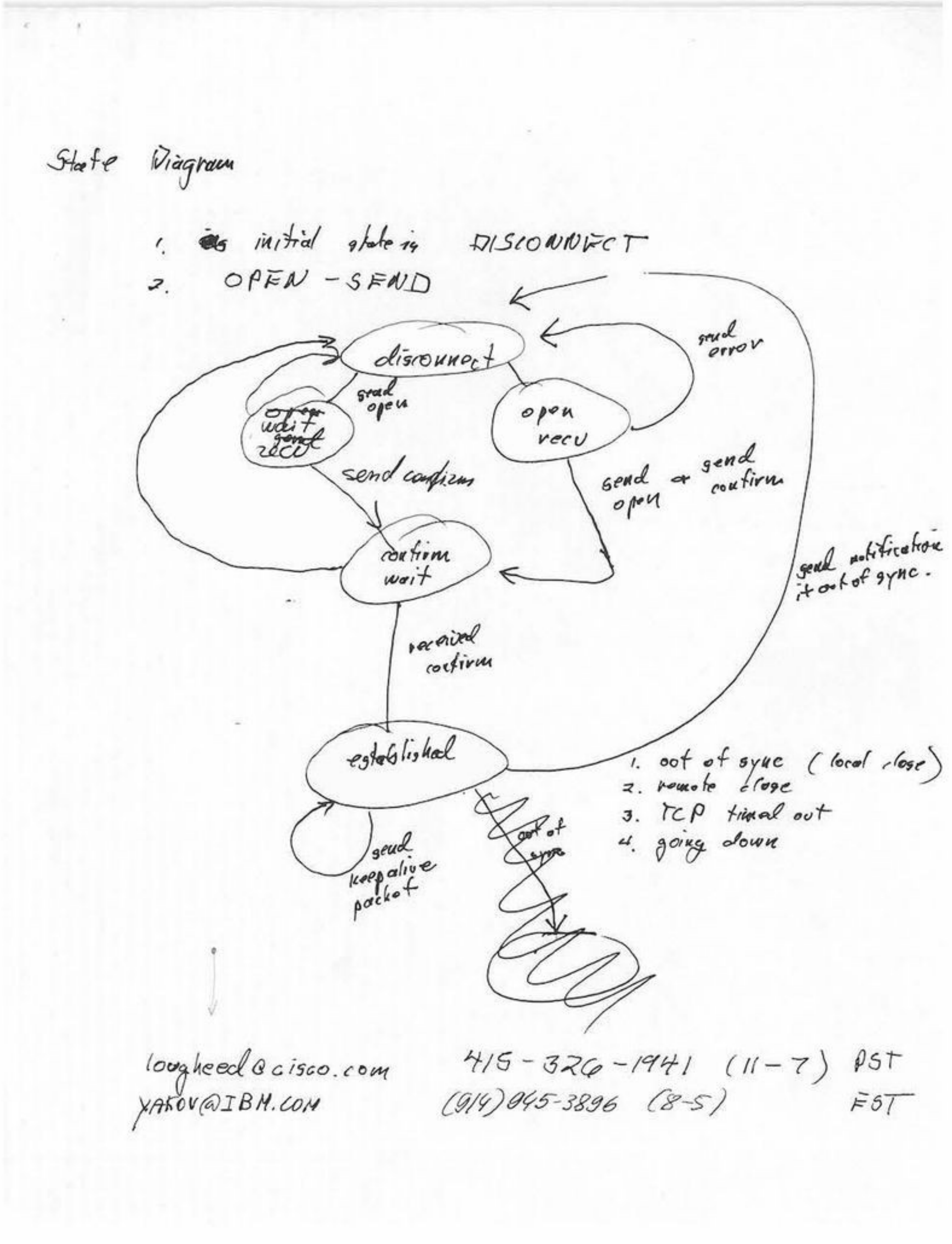
- Are networks using RPKI today?

Problem Statement

Is Internet Routing secure?

35 Years ago, at an IETF meeting’s cafeteria

BGP: The Two-Napkin protocol

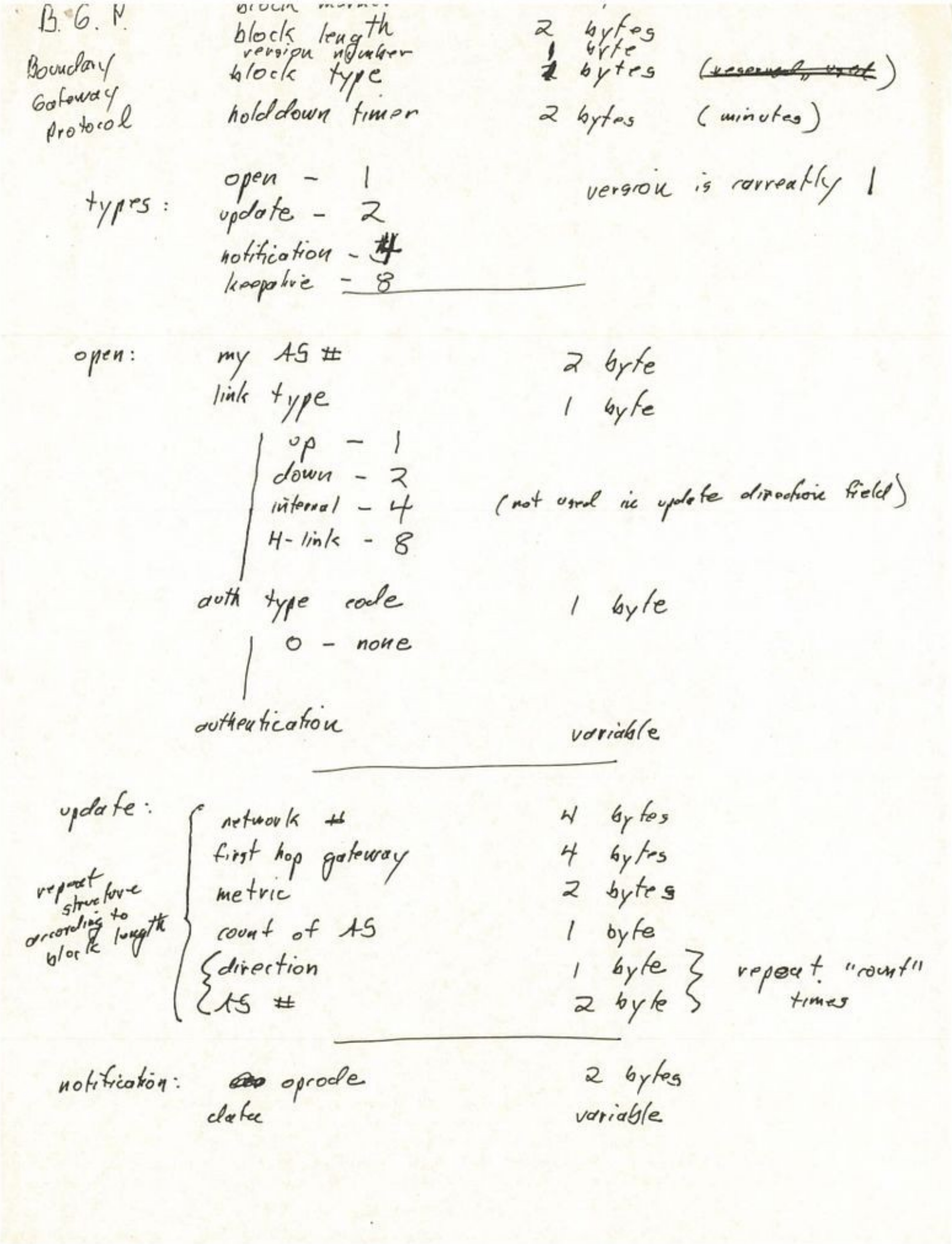


State Diagram

1. ~~is~~ initial state is DISCONNECT
2. OPEN - SEND

1. out of sync (local close)
2. remote close
3. TCP timed out
4. going down

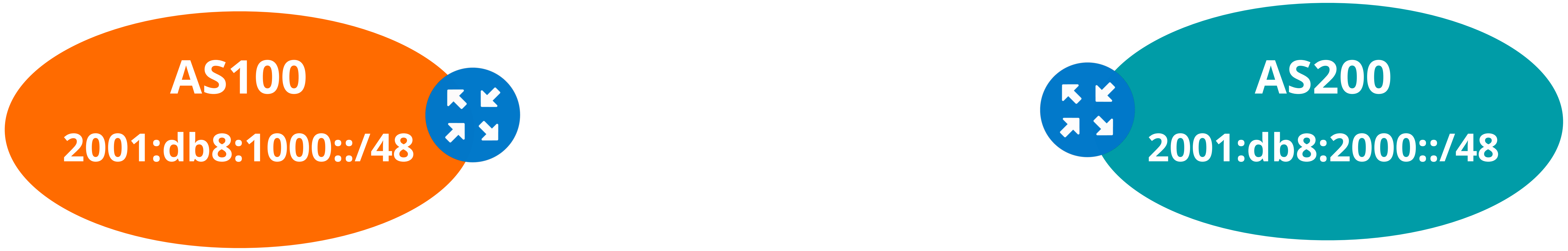
loughead@cisco.com 415-326-1941 (11-7) PST
YAKOV@IBM.COM (914)945-3896 (8-5) EST



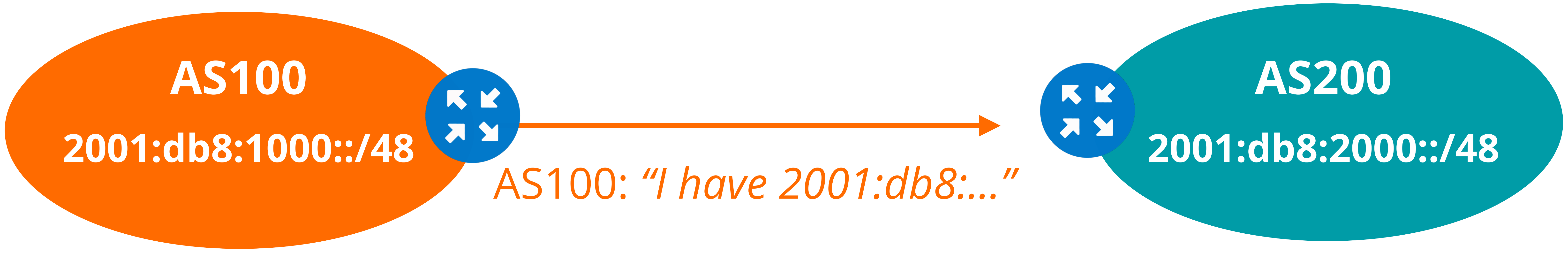
B.G.P.	block marker		
Boundary Gateway protocol	block length	2 bytes	
	version number	1 byte	
	block type	~~2~~ bytes	(~~reserved, unit~~)
	holddown timer	2 bytes	(minutes)
types:	open - 1		version is currently 1
	update - 2		
	notification - 4		
	keepalive - 8		
open:	my AS #	2 byte	
	link type	1 byte	
	up - 1		
	down - 2		
	internal - 4		(not used in update direction field)
	H-link - 8		
	auth type code	1 byte	
	0 - none		
	authentication	variable	
update:	network #	4 bytes	
repeat structure according to block length	first hop gateway	4 bytes	
	metric	2 bytes	
	count of AS	1 byte	
	direction	1 byte	repeat "count" times
	AS #	2 byte	
notification:	~~co~~ opcode	2 bytes	
	data	variable	

BGP, the Protocol of the Internet!

How does it work?



How does it work?



AS100

2001:db8:1000::/48

AS100: *“I have 2001:db8:...”*

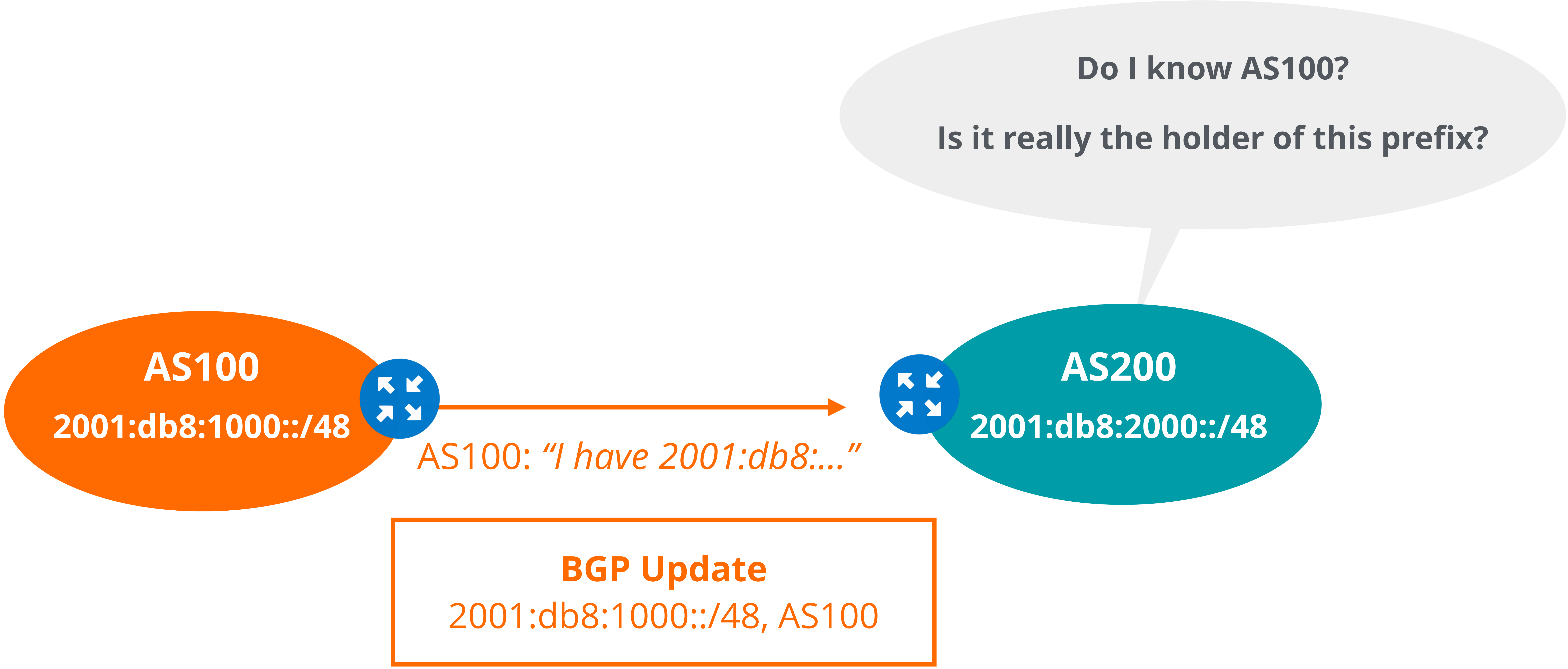
AS200

2001:db8:2000::/48

BGP Update

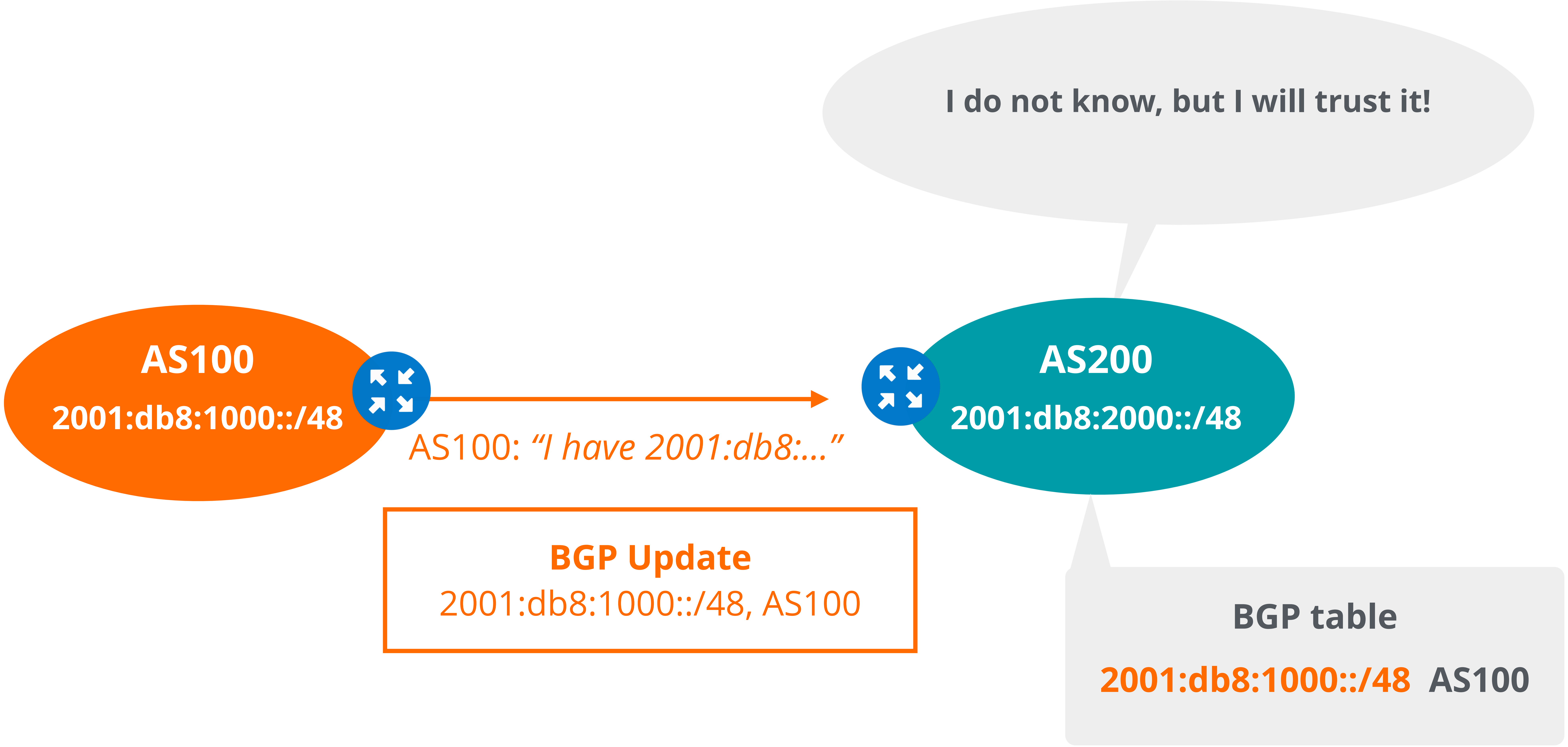
2001:db8:1000::/48, AS100

How does it work?


Do I know AS100?
Is it really the holder of this prefix?
AS100
2001:db8:1000::/48
AS100: *"I have 2001:db8:..."*
AS200
2001:db8:2000::/48

BGP Update
2001:db8:1000::/48, AS100

How does it work?



I do not know, but I will trust it!

AS100

2001:db8:1000::/48

AS100: *"I have 2001:db8:..."*

AS200

2001:db8:2000::/48

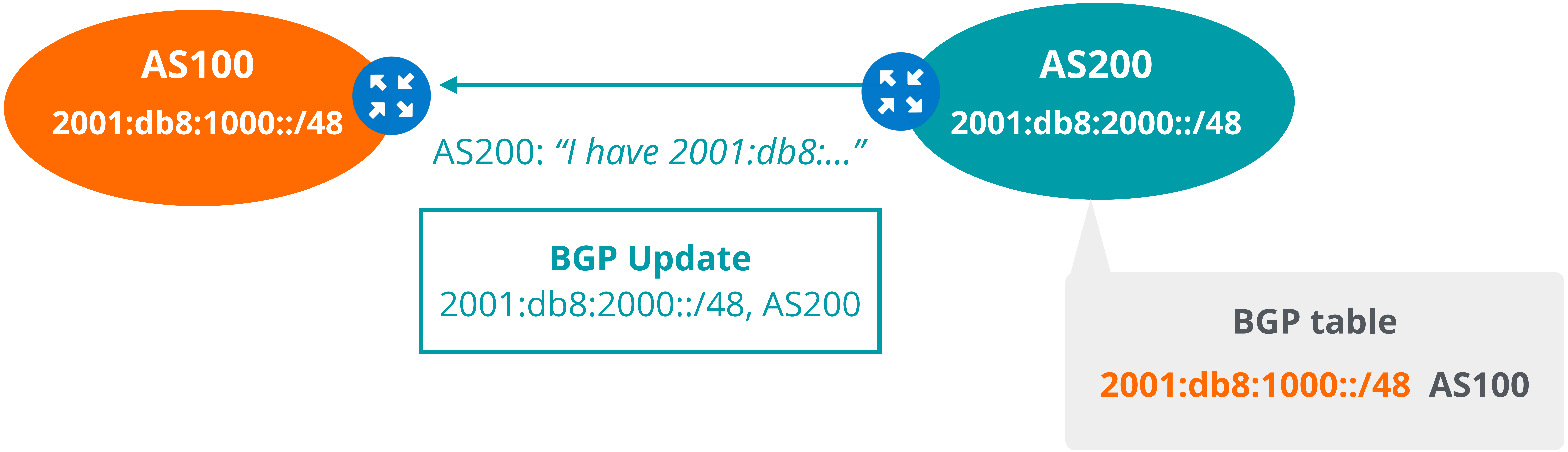
BGP Update

2001:db8:1000::/48, AS100

BGP table

2001:db8:1000::/48 AS100

How does it work?

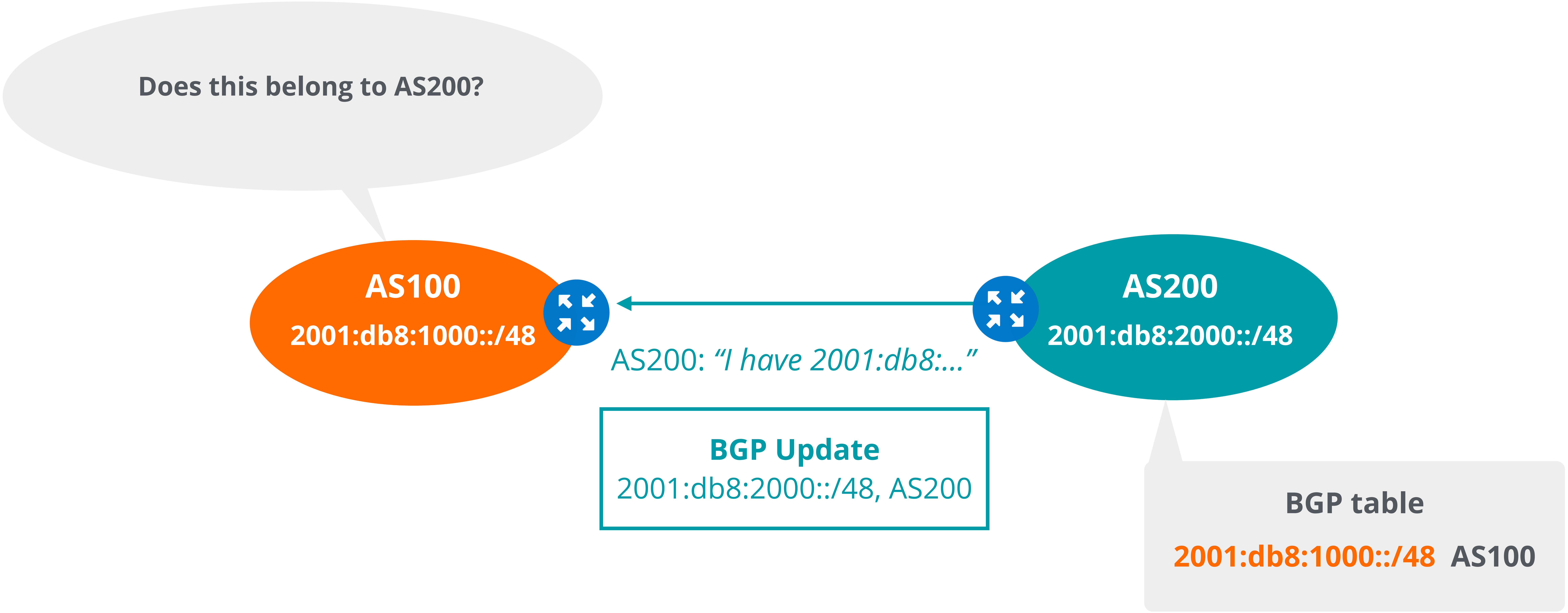


BGP Update
2001:db8:2000::/48, AS200

BGP table

2001:db8:1000::/48 **AS100**

How does it work?



Does this belong to AS200?

AS100

2001:db8:1000::/48

AS200: *"I have 2001:db8:..."*

AS200

2001:db8:2000::/48

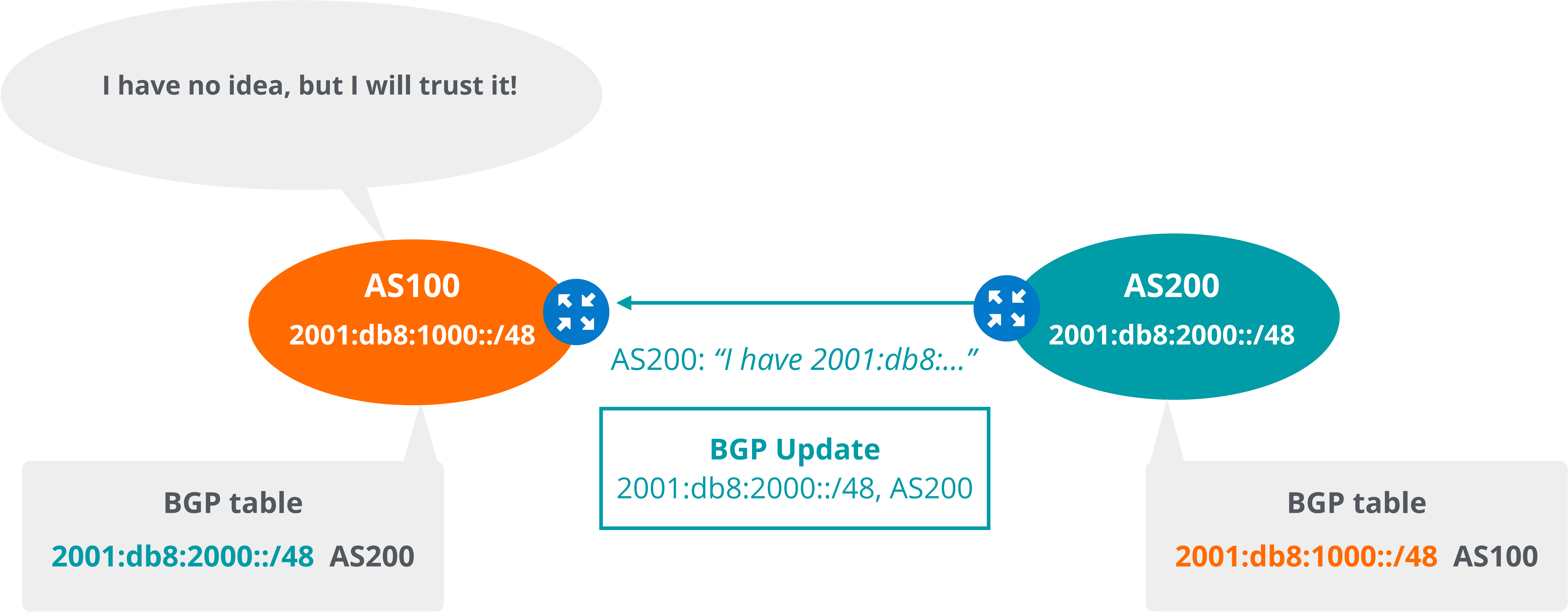
BGP Update

2001:db8:2000::/48, AS200

BGP table

2001:db8:1000::/48 AS100

How does it work?



I have no idea, but I will trust it!

AS100

2001:db8:1000::/48

AS200: *“I have 2001:db8:...”*

AS200

2001:db8:2000::/48

BGP Update

2001:db8:2000::/48, AS200

BGP table

2001:db8:2000::/48 AS200

BGP table

2001:db8:1000::/48 AS100

BGP assumes that everybody is telling the truth!

But what if someone lies?

or makes a mistake?

Routing Incidents

Causes and Impacts

It happens…

- Because there is no built-in security in BGP!
  - Any organisation can announce any IP prefix
  - Anyone can prepend any ASN to the BGP path
  - BGP announcements are accepted without validation

- Incorrect routing information can be propagated all over the Internet

Malicious BGP incidents

- An attacker may use BGP hijack for different purposes, such as…
  - censorship
  - stealing cryptocurrency
  - traffic interception and eavesdropping
  - blackholing the entire network
  - stealing credentials
  - sending spam…

Not all BGP incidents are intentional!

Sometimes they are just human errors…

- Typo errors
  - Also known as “fat fingers”
  - May cause mis-origination

- Configuration errors

A few notable incidents from recent years

2008

Pakistan Telecom hijacked YouTube

2013

Ukranian Telco (Vega) hijacked BT prefixes

2014

STE hijacked many prefixes including US DoD, YouTube, Level 3, Akamai…

2016

AWS Route Leak

2017

Google, Apple, FB, Microsoft, Riot Games prefixes were hijacked

2018

Amazon Route 53 Hijack myetherwallet.com cryptocurrency hijack

Google Prefix Leak

2019

Taiwan Network Information Center Public DNS in Taiwan was hijacked

2020

Telstra hijacked 500 prefixes

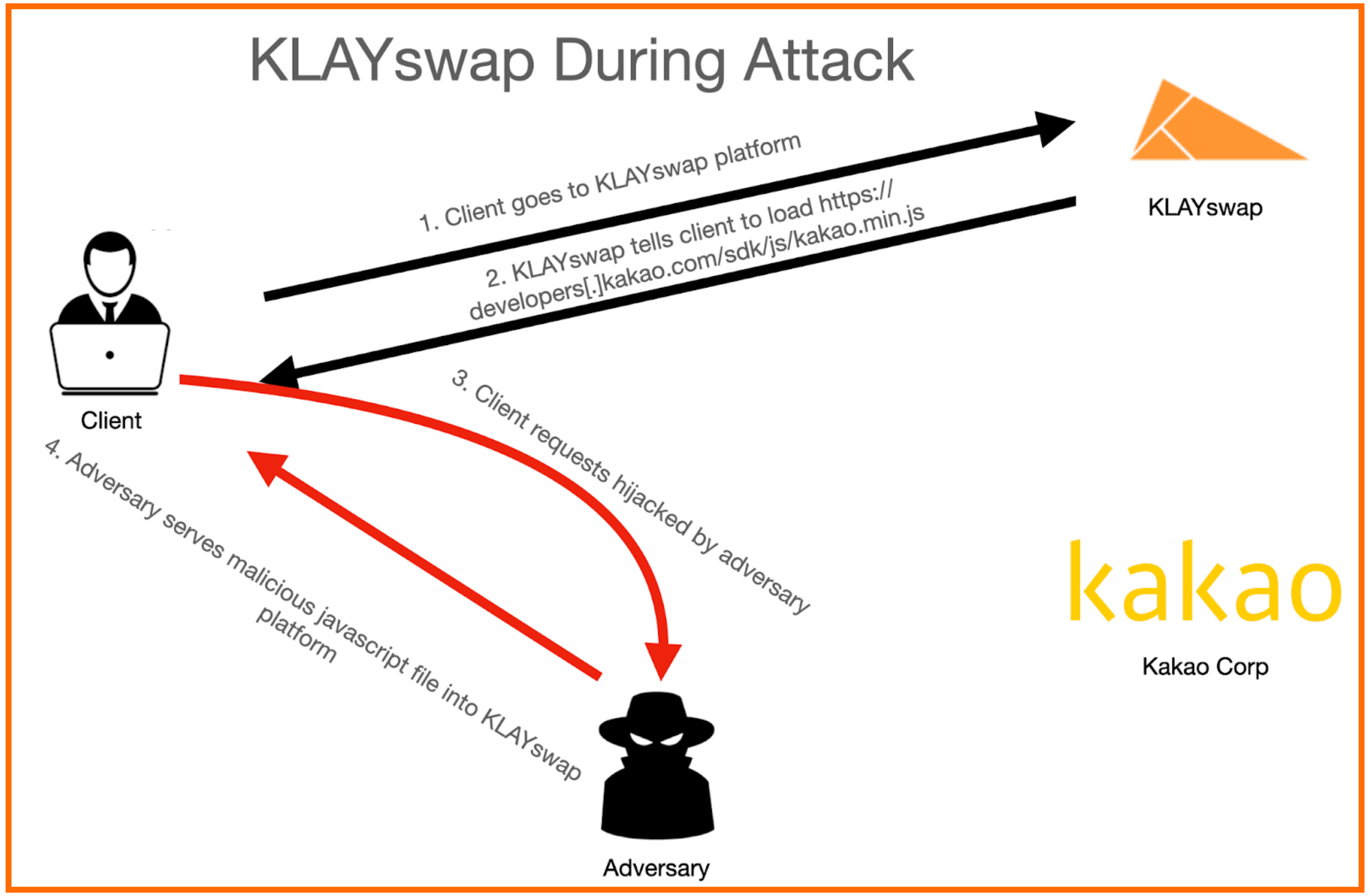
>8k BGP prefixes hijacked, affected companies such as Amazon, Akamai, Alibaba

2021

AS55410 (Vodafone Idea) hijacked almost 40k prefixes, belonging to 4k+ ASNs in 164 countries.

Feb 2022: Attackers steal $2M in cryptocurrency

- What happened?
  - Cryptocurrency exchange platform was targeted by a cross-layer attack
  - Attackers announced 2 IP Prefixes belonging to Kakao. 2 Attacks in 1



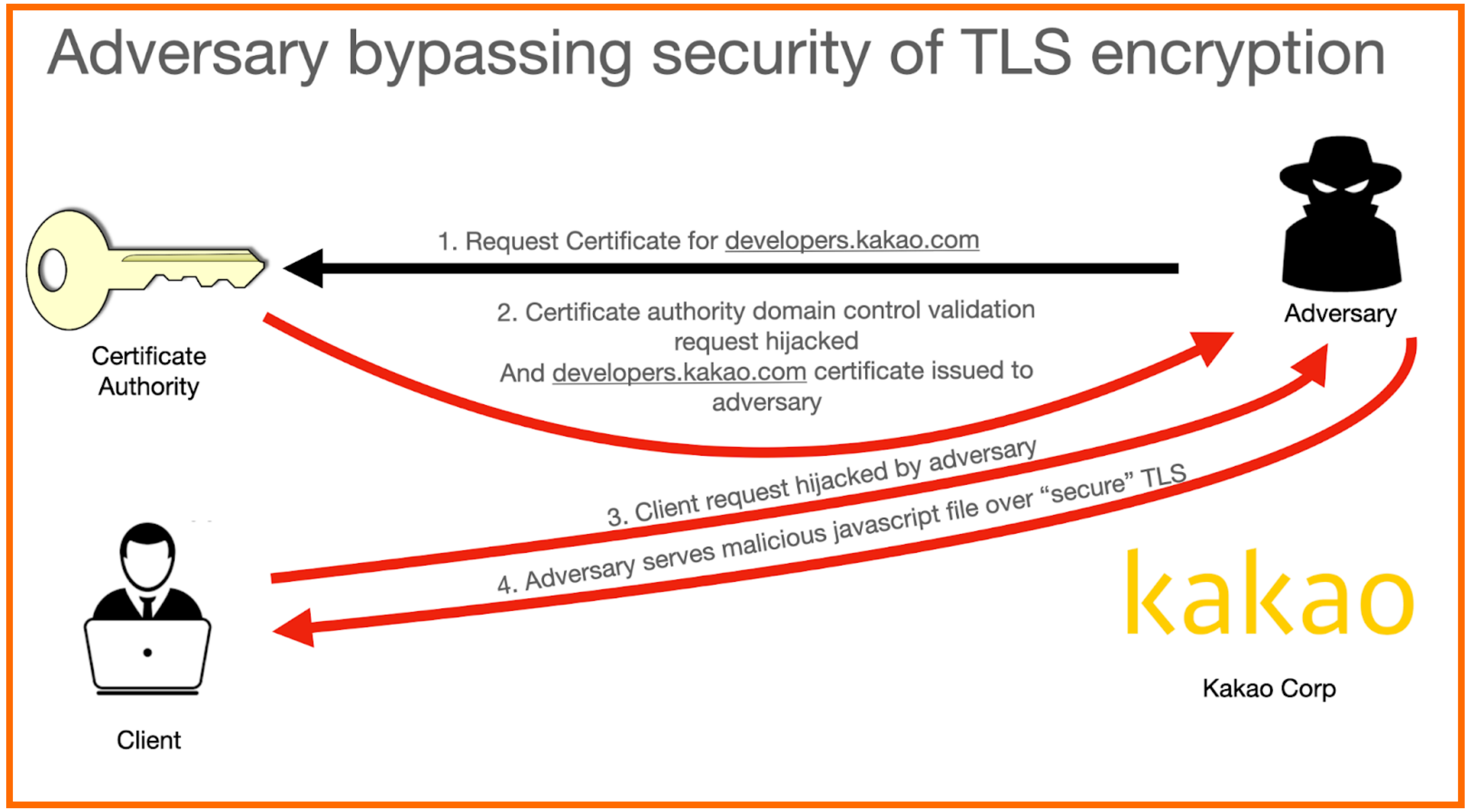
KLAYswap During Attack

1. Client goes to KLAYswap platform

2. KLAYswap tells client to load https://developers[.]kakao.com/sdk/js/kakao.min.js

3. Client requests hijacked by adversary

4. Adversary serves malicious javascript file into KLAYswap platform



Adversary bypassing security of TLS encryption

1. Request Certificate for developers.kakao.com

2. Certificate authority domain control validation request hijacked And developers.kakao.com certificate issued to adversary

3. Client request hijacked by adversary

4. Adversary serves malicious javascript file over "secure" TLS

Source: Freedom to tinker

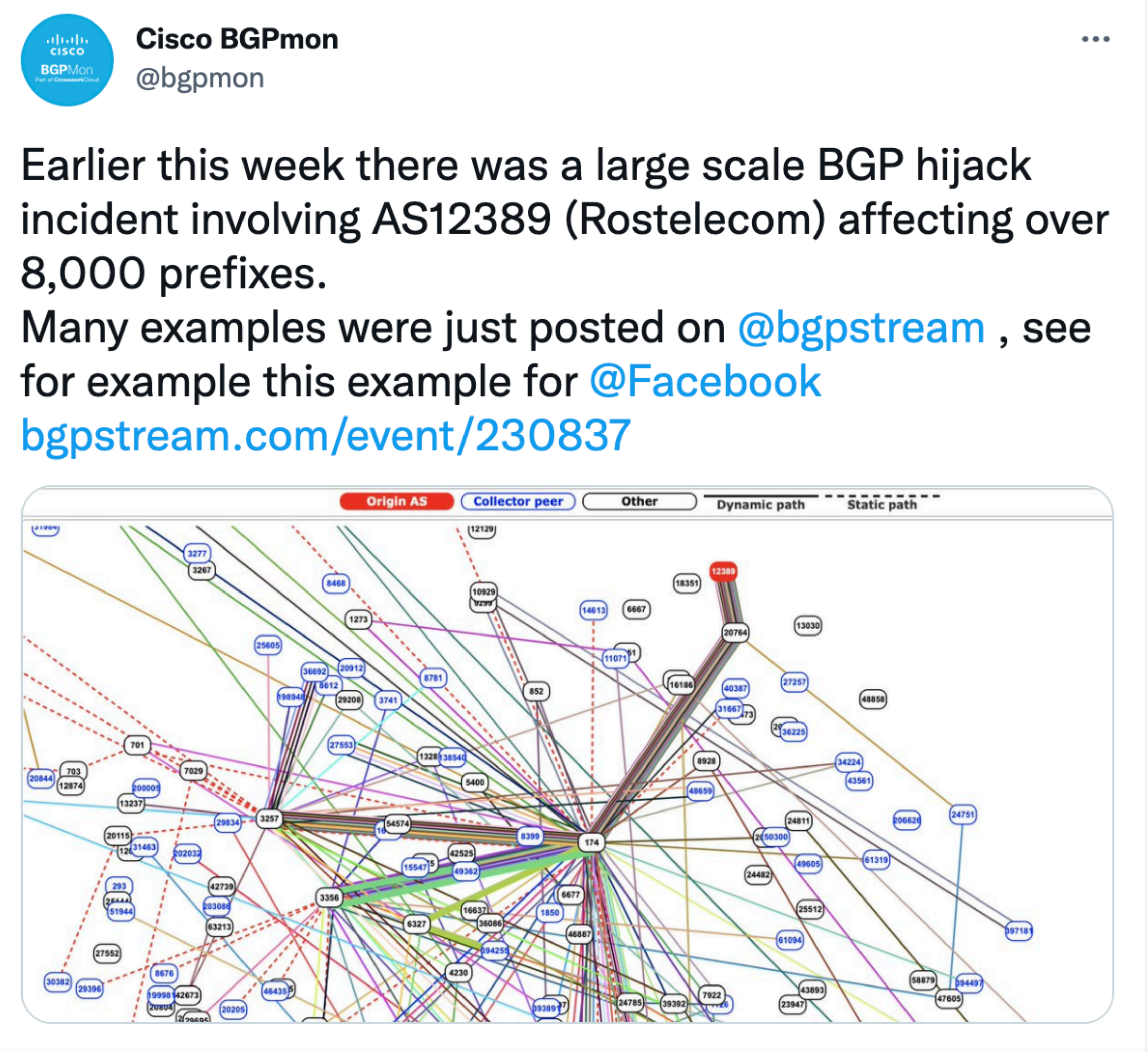
April 2021: BGP hijack by Vodafone Idea, AS55410

- What happened?
  - 34,000+ prefixes hijacked!
  - Impacted major network operators, cloud and CDN providers
  - ISP links got saturated: 13 times more traffic than usual

- Why did it happen?
  - Caused by wrong advertisement
  - Lack of good filtering by upstream providers

April 2020: Akamai, Amazon and Alibaba

- What happened?
  - 8k+ routes hijacked by Rostelecom (AS12389)
  - 200+ CDNs and cloud providers impacted
  - Not known how much data leaked



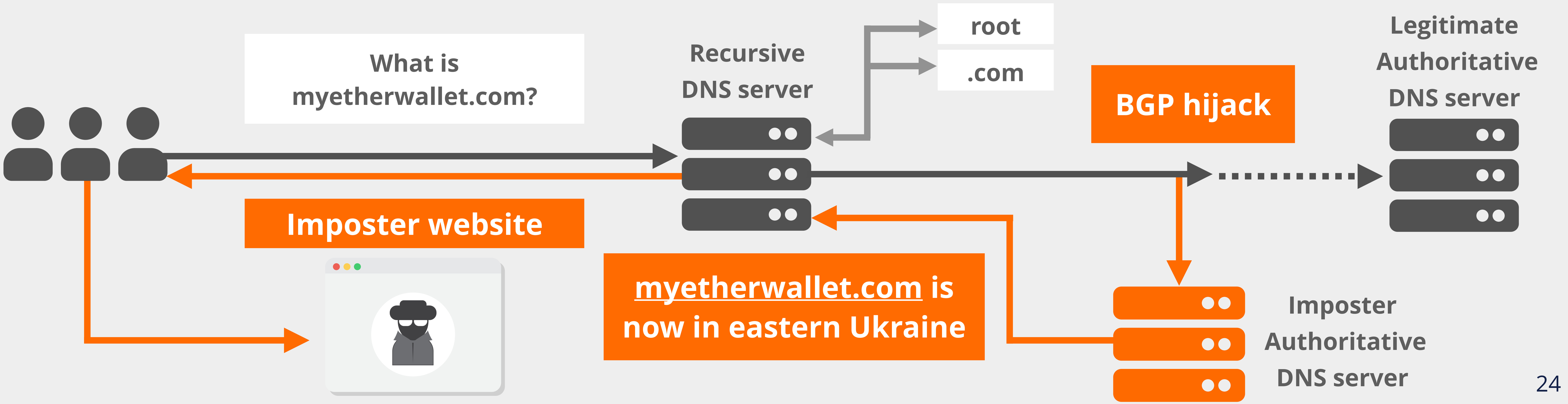
Cisco BGPmon
@bgpmon

Earlier this week there was a large scale BGP hijack incident involving AS12389 (Rostelecom) affecting over 8,000 prefixes.
Many examples were just posted on @bgpstream , see for example this example for @Facebook bgpstream.com/event/230837

- Why did it happen?
  - Unidentified cause?
  - Lack of good filtering by upstream providers/peers

April 2018: Amazon - MyEtherWallet

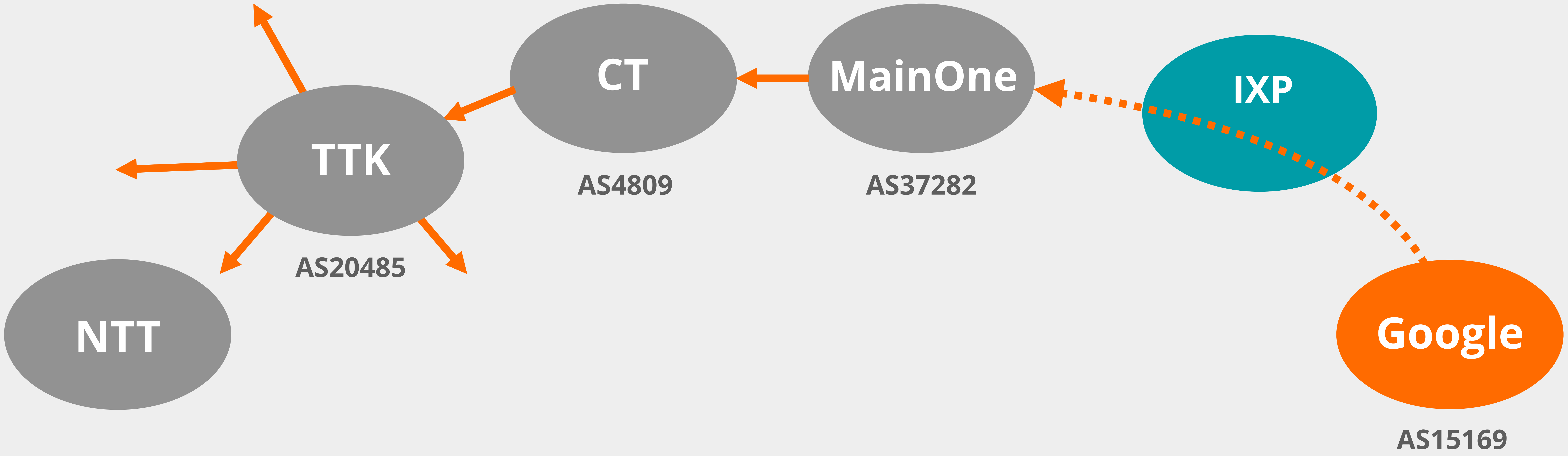
- BGP hijack of Amazon DNS
- How did it happen?
- Why?
  - Attack to steal cryptocurrency



What is myetherwallet.com?
Recursive DNS server
root
.com
BGP hijack
Legitimate Authoritative DNS server
Imposter website
myetherwallet.com is now in eastern Ukraine
Imposter Authoritative DNS server

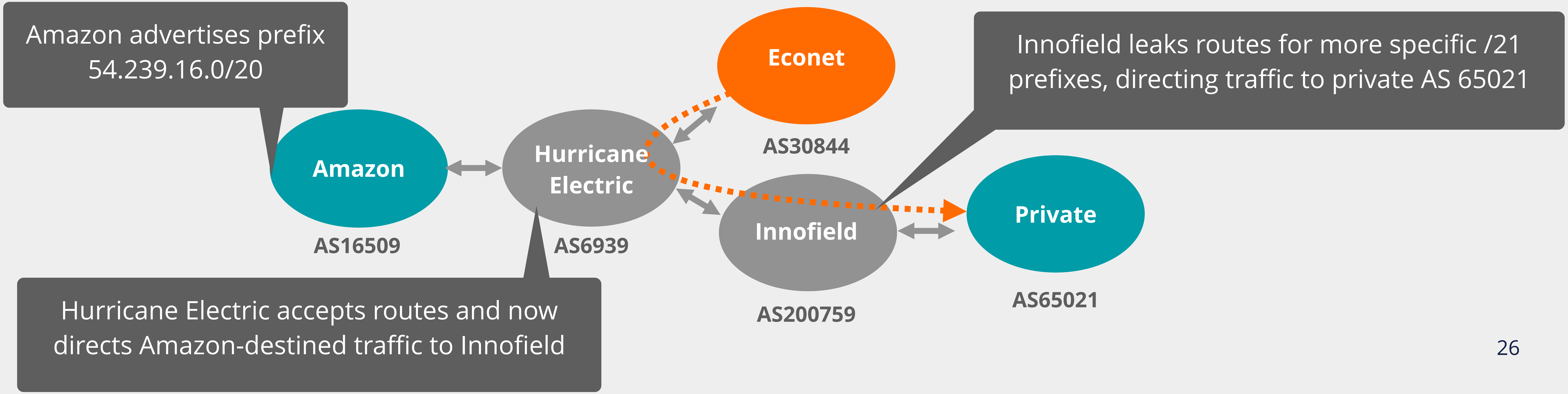
November 2018: Google prefix leak

- MainOne leaked Google routes to CT
- CT propagated them to several transit ISPs
- Google services (G Suite and Google Search) affected by the leak
- Due to misconfigured filters



April 2016: AWS route leak

- Private AS originated Amazon’s prefixes, but more specific
- Innofield leaked these routes to its upstream
- No big impact because most ISPs didn’t accept the bogus route
- Caused by misconfigured route optimiser



Amazon advertises prefix 54.239.16.0/20

Innofield leaks routes for more specific /21 prefixes, directing traffic to private AS 65021

Hurricane Electric accepts routes and now directs Amazon-destined traffic to Innofield

Routing Security with RPKI

What is RPKI and how does it work?

But first… Let’s book some flight tickets

Can you trust this website?

emirates.com/ae/english/

ⓘ **Important:** Baggage progress following the Dubai storm disruption

Departure airport: Dubai (DXB)

Arrival airport: Helsinki (HEL)

Departing: 14 May 24 - Returning: 16 May 24

Passengers: 1 Passenger

Class: Economy Class

Show more
BOOK
MANAGE
EXPERIENCE
WHERE WE FLY
LOYALTY
HELP
AE
Jad
Emirates
FLY BETTER
Enjoy summer offers with
MY EMIRATES PASS
in Dubai and the UAE
Learn more
Feedback
Search flights
Manage booking / Check in
What's on your flight
Flight status
Flight
Flight + hotel
Classic rewards
Advanced search: multi-city, promo codes, partner airlines
Search flights

The connection seems secure

emirates.com/ae/english/

emirates.com

mportant: Baggage progress following the Dubai storm disruption

njoy summer offers with MY EMIRATES PASS in Dubai and the UAE

Departure airport: Dubai (DXB)

Arrival airport: Helsinki (HEL)

Departing: 14 May 24 - Returning: 16 May 24

Passengers: 1 Passenger

Class: Economy Class

Connection is secure
Cookies and site data
Ads privacy
Site settings
About this page
Learn about its source and topic
Show more
BOOK
MANAGE
EXPERIENCE
WHERE WE FLY
LOYALTY
HELP
AE
Jad
FLY BETTER
Learn more
Search flights
Manage booking / Check in
What's on your flight
Flight status
Flight
Flight + hotel
Classic rewards
Advanced search: multi-city, promo codes, partner airlines
Search flights
Feedback

Is the certificate valid?

emirates.com/ae/english/

Security
emirates.com

Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate is valid
Issued to: Emirates [AE]

mportant: Baggage progress following the Dubai storm disruption

Show more
BOOK
MANAGE
EXPERIENCE
WHERE WE FLY
LOYALTY
HELP
AE
Jad
nirates
FLY BETTER

njoy summer offers with
MY EMIRATES PASS
in Dubai and the UAE

Learn more
Search flights
Manage booking / Check in
What's on your flight
Flight status
Feedback

☑ Flight | Flight + hotel

□ Classic rewards

Advanced search: multi-city, promo codes, partner airlines

Departure airport: Dubai (DXB)

Arrival airport: Helsinki (HEL)

Departing: 14 May 24 - Returning: 16 May 24

Passengers: 1 Passenger

Class: Economy Class

Can I trust this certificate?

emirates.com/ae/english/
Important: Baggage progress following th
Show more
BOOK
MANAGE
EX
AE
Jad
Emirates
Enjoy summer offe
MY EMIRA
in Du
FLY BETTER
Search flights
Flight status
Feedback
✓ Flight
Flight + hotel
□ Classic rewards
ulti-city, promo codes, partner airlines

Departure airport: Dubai (DXB)

Arrival airport: Helsinki (HEL)

Departing: 14 May 24 - Returning: 16 May 24

Passengers: 1 Passenger

Class: Economy Class

Search flights

Certificate Viewer: www.emirates.com

General
Details

Issued To

Common Name (CN)	www.emirates.com
Organisation (O)	Emirates
Organisational Unit (OU)	<Not part of certificate>

Issued By

Common Name (CN)	DigiCert SHA2 Extended Validation Server CA
Organisation (O)	DigiCert Inc
Organisational Unit (OU)	www.digicert.com

Validity Period

Issued On	Monday, 10 July 2023 at 04:00:00
Expires On	Thursday, 11 July 2024 at 03:59:59

SHA-256 Fingerprints

Certificate	acbd584b65c1add3b63b72e74ff9e0c69fd9f387b1abdf370a83ff2a5dfeb440
Public key	7b732673daeebe264ce0a0665131b0cb43af38cd7669a032fc1e057adf32270e

Oh yes, I trust the issuer!

emirates.com/ae/english/

Important: Baggage progress following th

Certificate Viewer: www.emirates.com

General | Details

Issued To

Common Name (CN)	www.emirates.com
Organisation (O)	Emirates
Organisational Unit (OU)	<Not part of certificate>

Issued By

Common Name (CN)	DigiCert SHA2 Extended Validation Server CA
Organisation (O)	DigiCert Inc
Organisational Unit (OU)	www.digicert.com

Validity Period

Issued On	Monday, 10 July 2023 at 04:00:00
Expires On	Thursday, 11 July 2024 at 03:59:59

SHA-256 Fingerprints

Certificate	acbd584b65c1add3b63b72e74ff9e0c69fd9f387b1abdf370a83ff2a5dfeb440
Public key	7b732673daeebe264ce0a0665131b0cb43af38cd7669a032fc1e057adf32270e

☑ Flight | Flight + hotel

□ Classic rewards

Departure airport: Dubai (DXB)

Arrival airport: Helsinki (HEL)

Departing: 14 May 24 - Returning: 16 May 24

Passengers: 1 Passenger

Class: Economy Class

What is RPKI?

- RPKI is ...
  - a **resource certification** (X.509 PKI certificates)
  - a security framework
- It is used to make Internet routing more secure and reliable

How does RPKI help with routing security?

- Verifies the association between resource holders and their Internet number resources.
  - Proves holdership through a public key and certificate infrastructure

- Used to validate the **origin of BGP announcements**
  - Is the originating ASN authorised to originate a particular prefix?

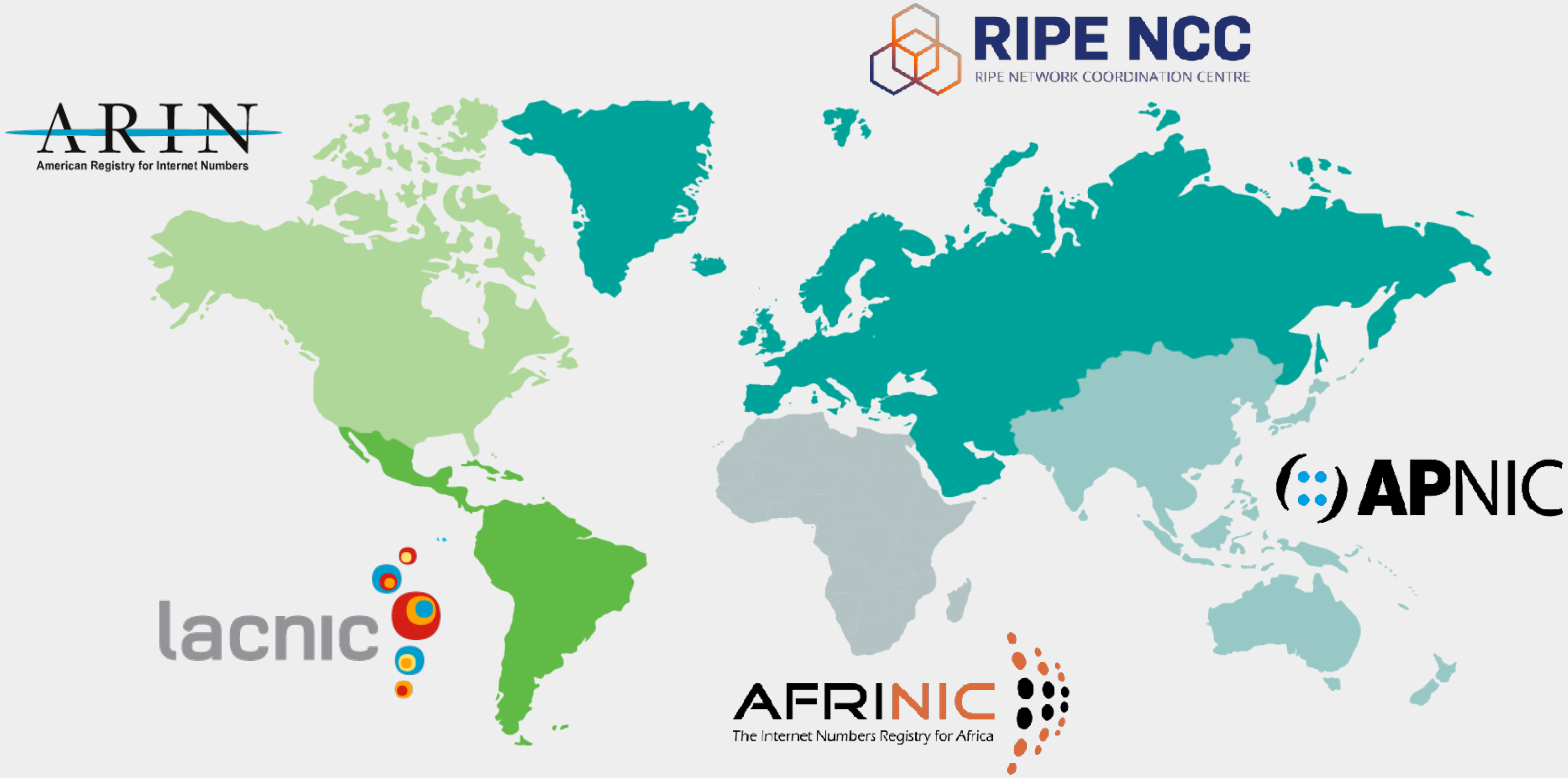
- Stepping stone to “**Path Validation**”

Implementing RPKI helps to prevent…

- BGP Origin Hijacks
  - Caused by malicious activities
- Mis-origination
  - Due to typos/fat fingers
- Route leaks
  - Caused by configuration mistakes

How is it different than the IRR system?

- RPKI is based on RIRs as Trust Anchors
  - RIRs have control over the accuracy of registered data


RIPE NCC
RIPE NETWORK COORDINATION CENTRE
ARIN
American Registry for Internet Numbers
APNIC
lacnic
AFRINIC
The Internet Numbers Registry for Africa

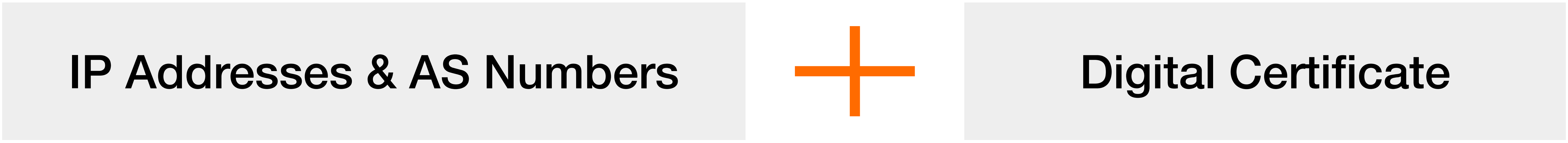
How is it different than the IRR system?

- RPKI is based on RIRs as Trust Anchors
  - RIRs have control over the accuracy of registered data

- Cryptography is used to verify the holdership
  - Provides data you can trust

How does it work?

- RPKI attaches a digital certificate to IP addresses and AS numbers

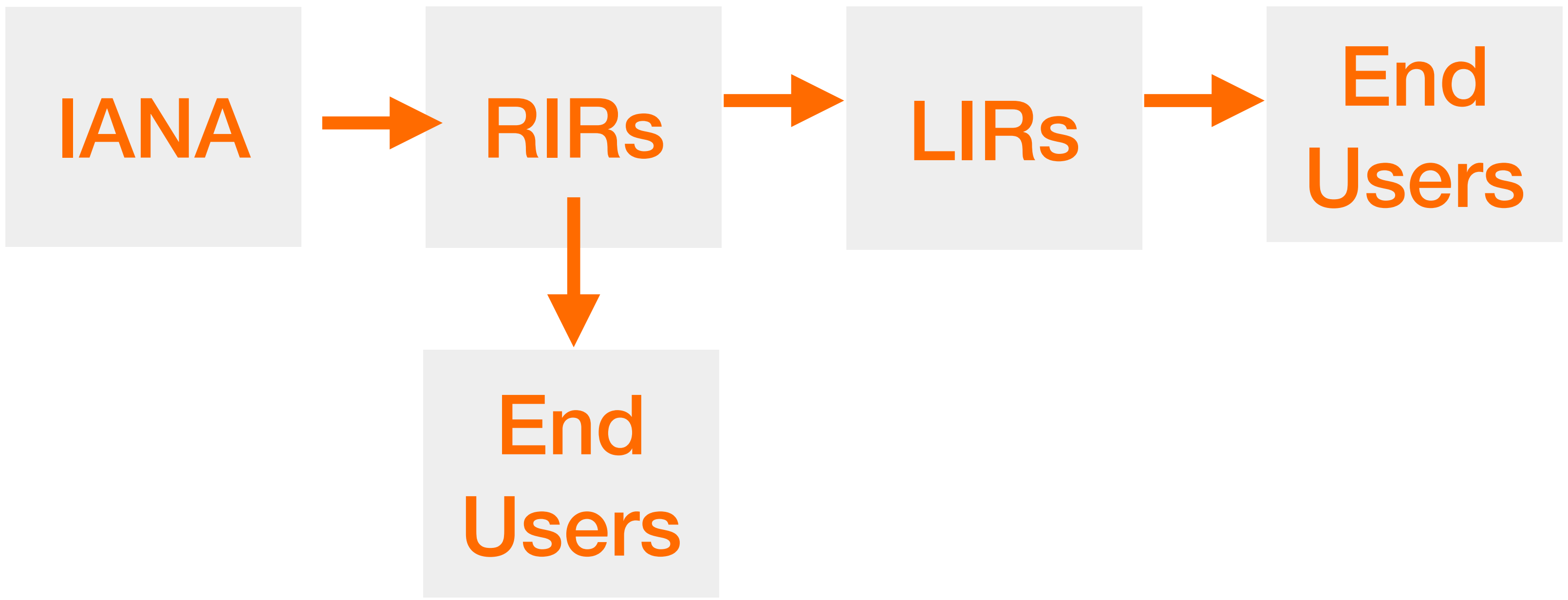


IP Addresses & AS Numbers + Digital Certificate

- Digital signatures authorise the use of resources
  - Private key to sign, public key to validate

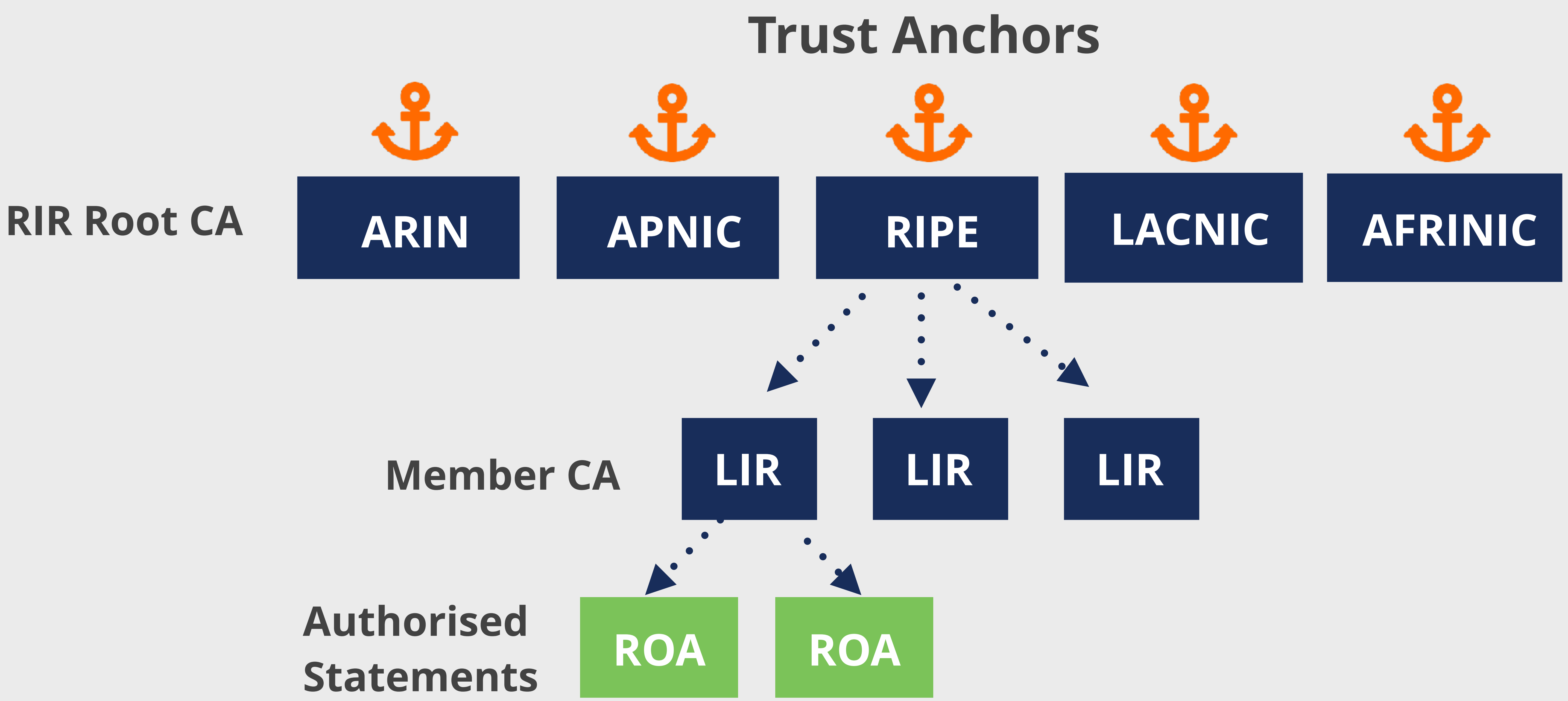
How to provide trust in RPKI?

- It relies on the 5 RIRs as Trust Anchors
- Certificate structure follows the RIR hierarchy
- RIRs issue certificates to resource holders



IANA → RIRs → LIRs → End Users

RIRs → End Users



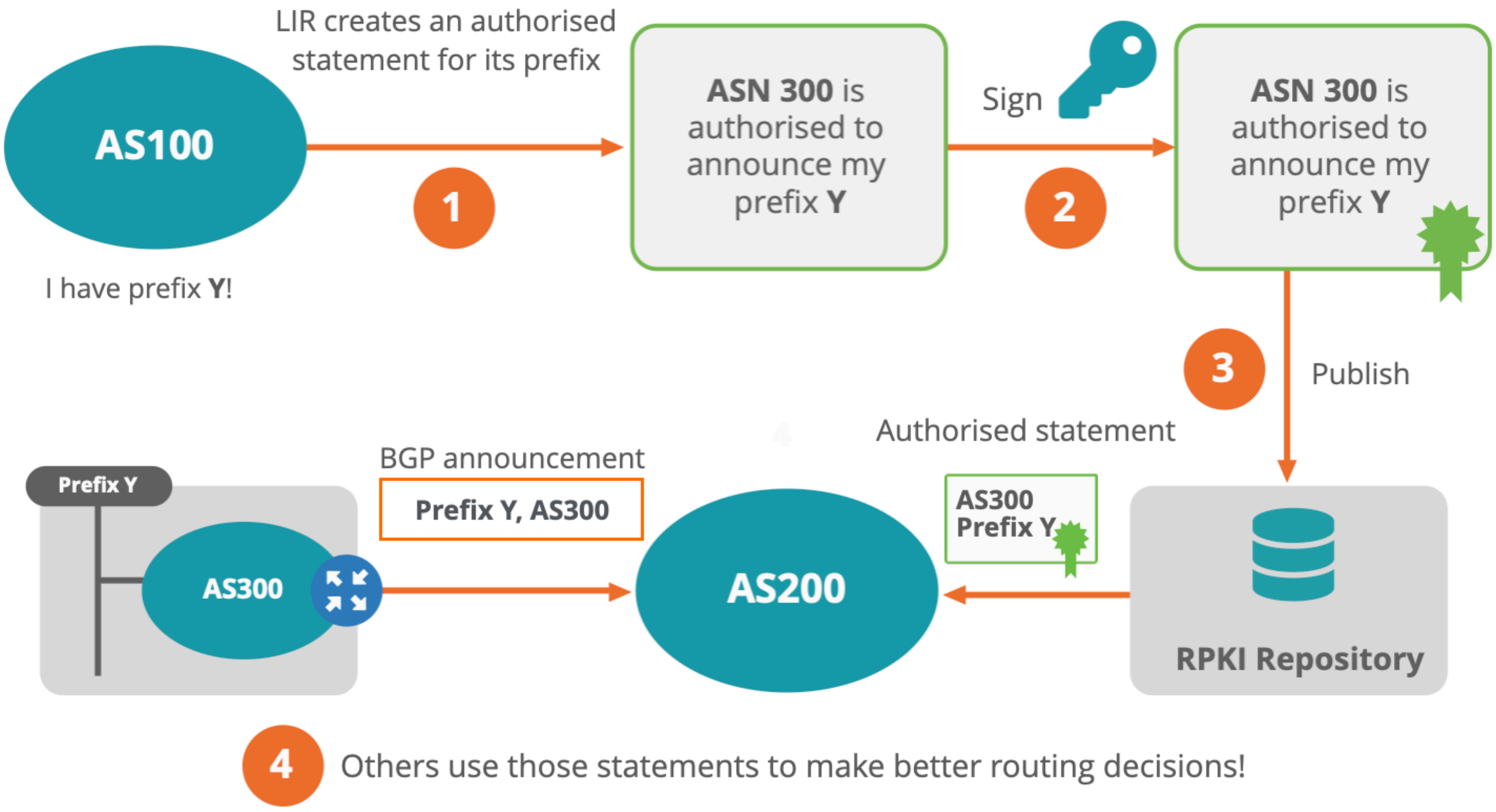
Trust Anchors

RIR Root CA: ARIN, APNIC, RIPE, LACNIC, AFRINIC

Member CA: LIR, LIR, LIR

Authorised Statements: ROA, ROA

How does it work?


LIR creates an authorised statement for its prefix
AS100
1
I have prefix **Y**!
ASN 300 is authorised to announce my prefix **Y**
Sign
2
ASN 300 is authorised to announce my prefix **Y**
3
Publish
Authorised statement
BGP announcement
Prefix Y
AS300
Prefix Y, AS300
AS200
AS300
Prefix Y
RPKI Repository
4

Others use those statements to make better routing decisions!

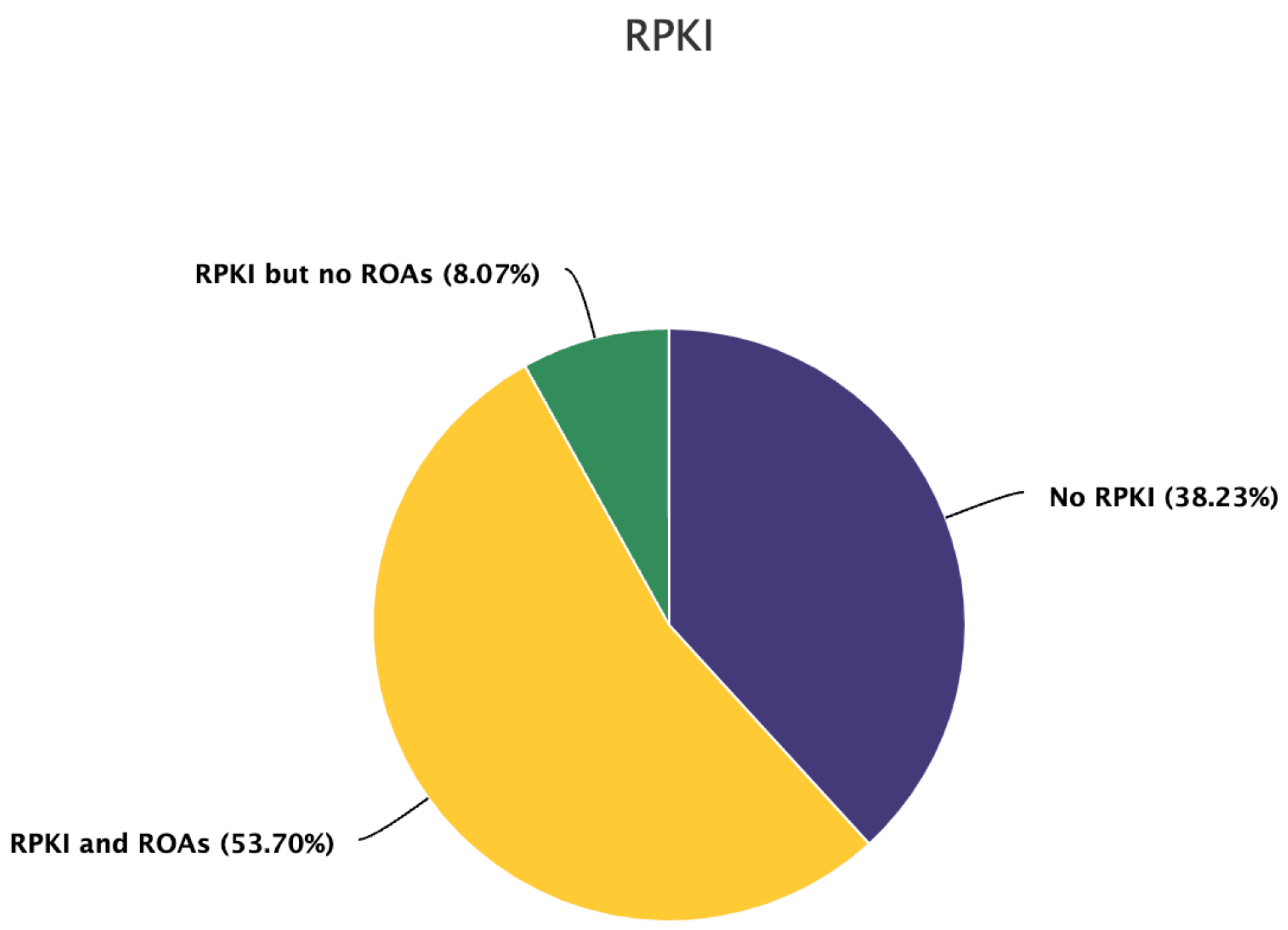
RPKI Adoption

Are networks using RPKI today?

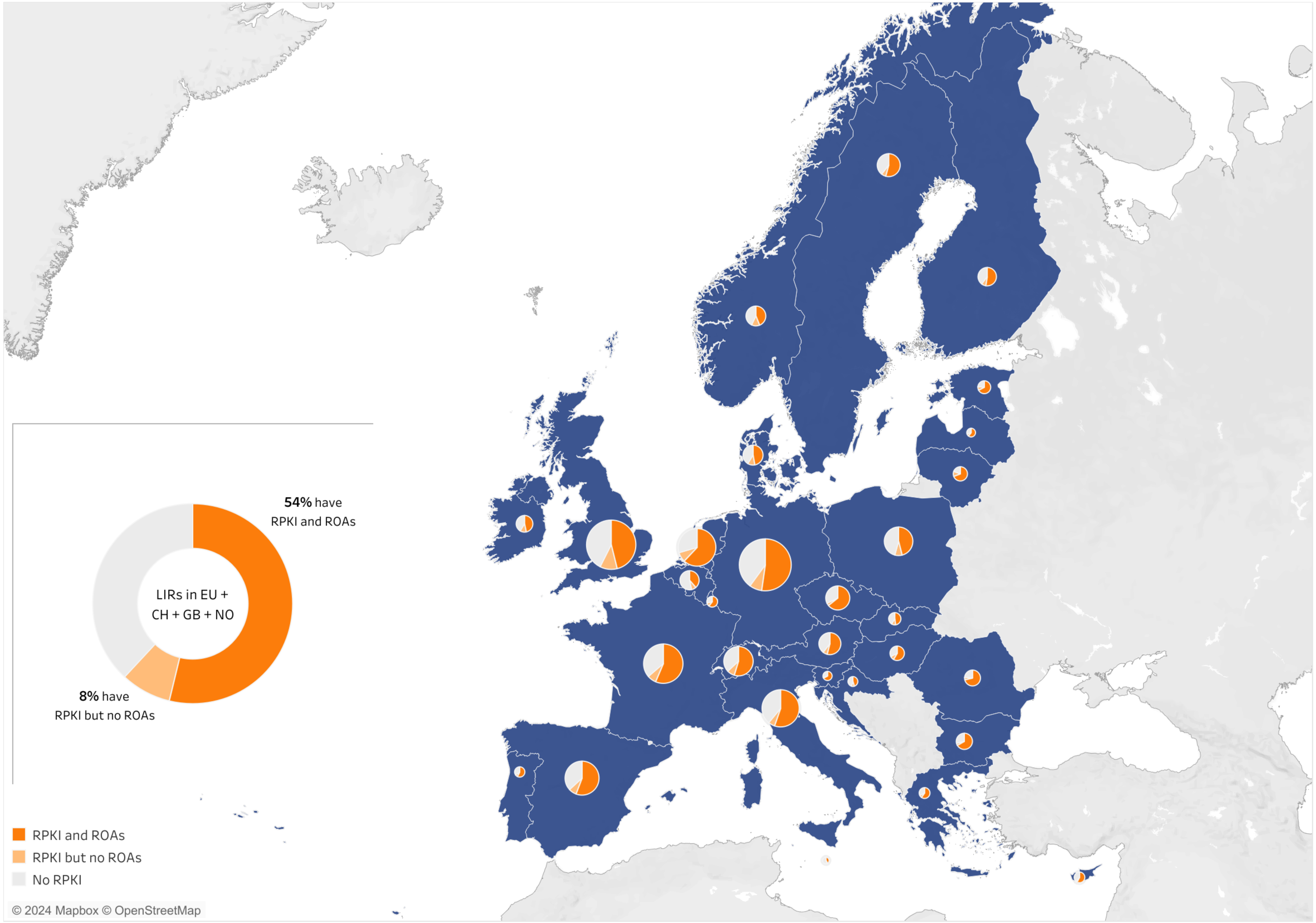
RPKI Adoption in RIPE NCC region

- Data based on 21 600 LIRs

- 3 Possible stages:
  - **No RPKI**: LIR did not start the RPKI journey
  - **RPKI but no ROAs**: LIR received its RPKI certificate but did not start creating ROAs for their IP space
  - **RPKI and ROAs**: LIR received its RPKI certificate and started creating ROAs for their IP space

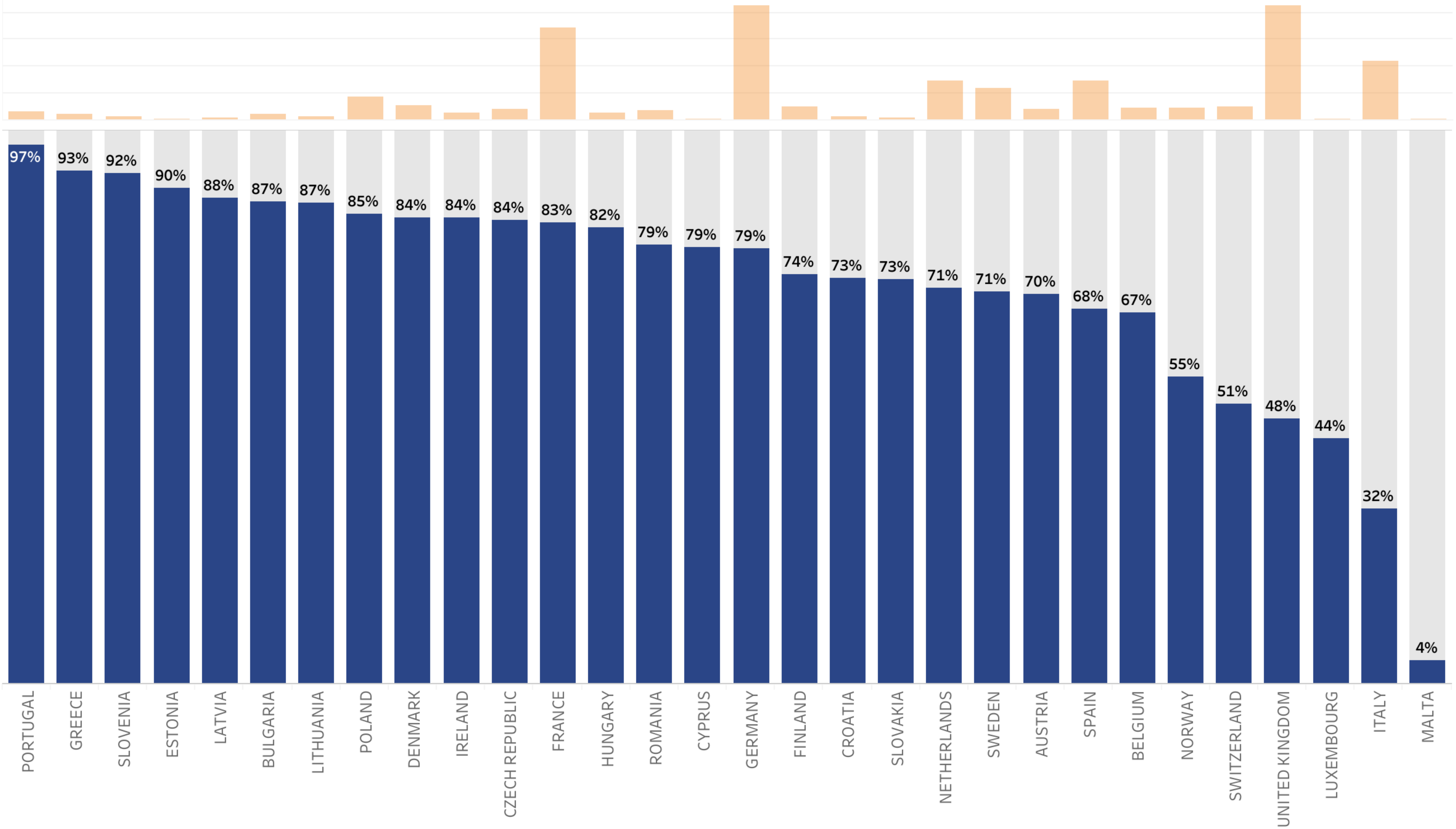


RPKI Adoption in Europe

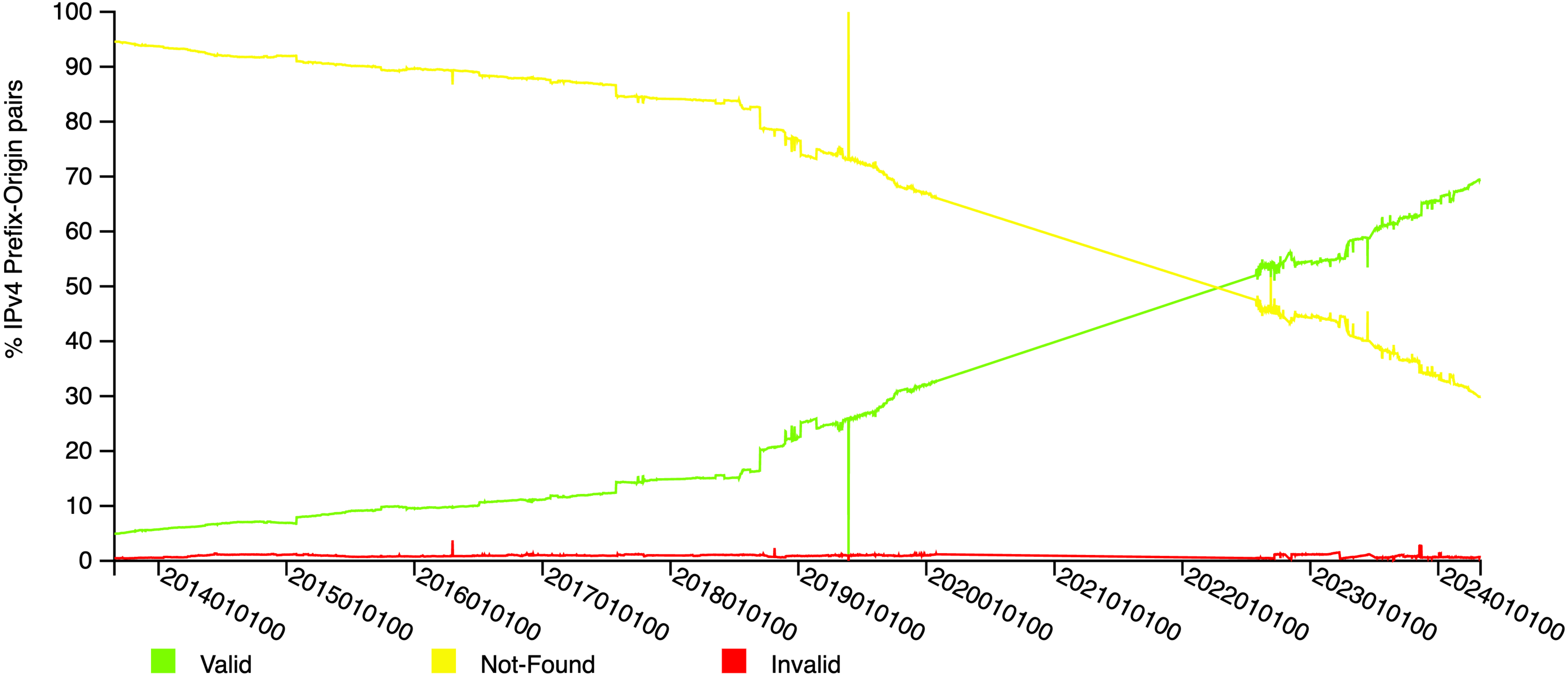

LIRs in EU + CH + GB + NO
54% have RPKI and ROAs
8% have RPKI but no ROAs
🟧 RPKI and ROAs
🟧 RPKI but no ROAs
⬜ No RPKI

© 2024 Mapbox © OpenStreetMap

RPKI Adoption in Europe

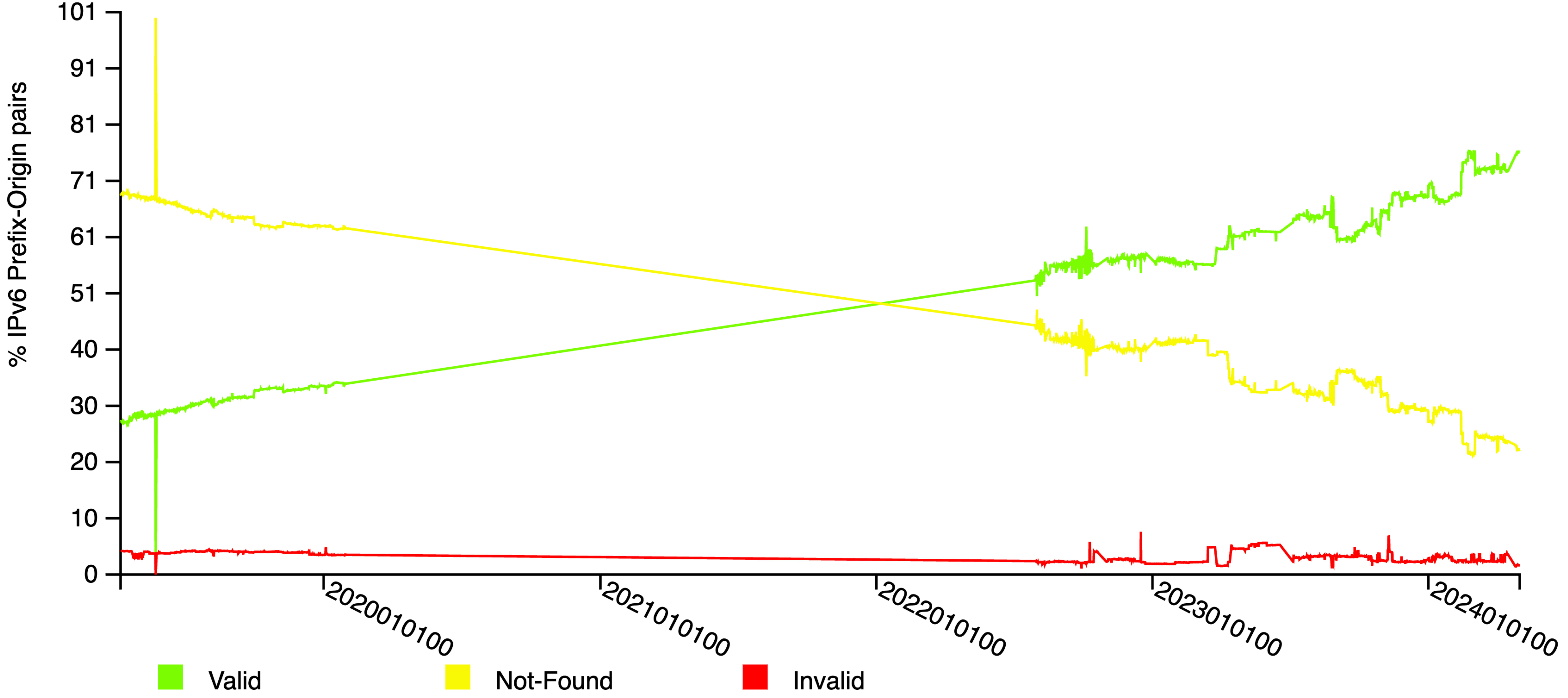


RPKI IPv4 space coverage - RIPE NCC region



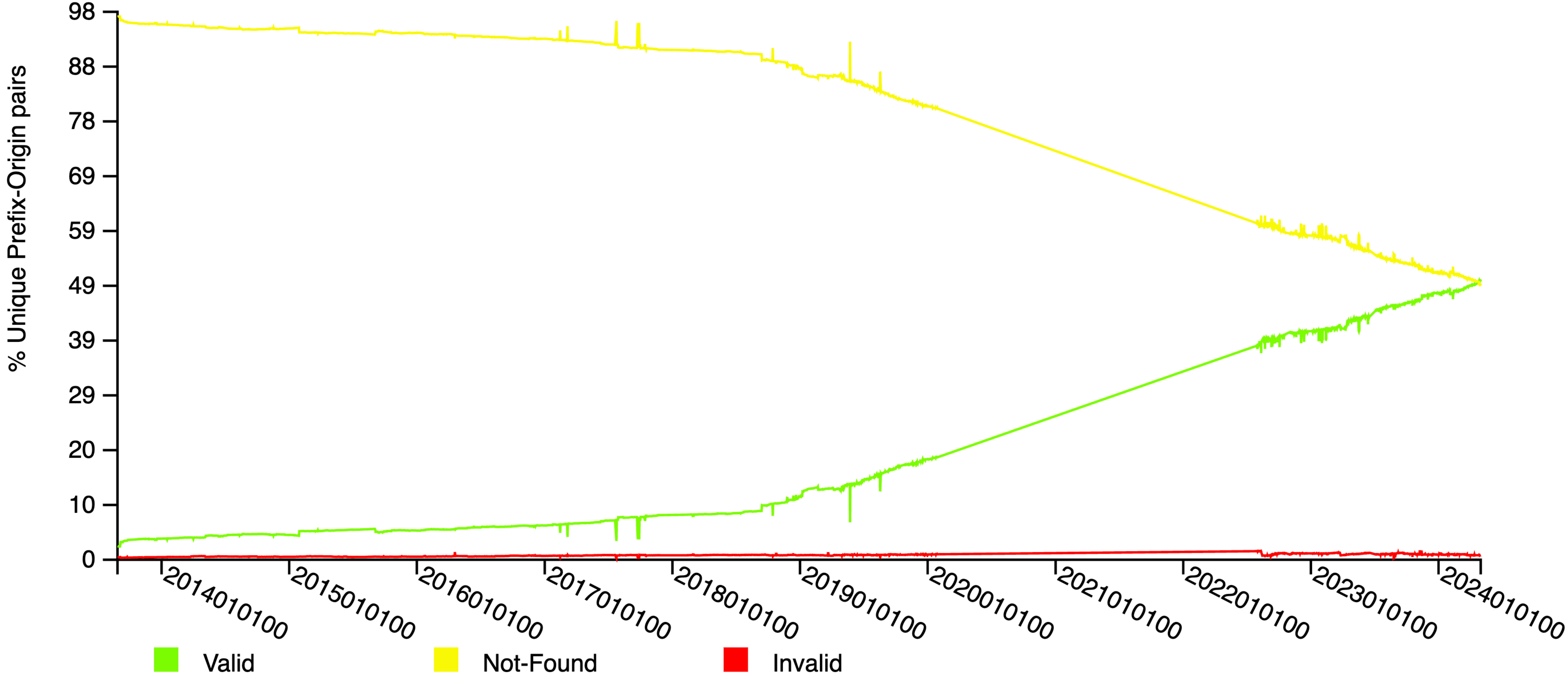
NIST RPKI Monitor: RPKI-ROV Analysis **Protocol:** IPv4 **RIR:** RIPE

RPKI IPv6 space coverage - RIPE NCC region



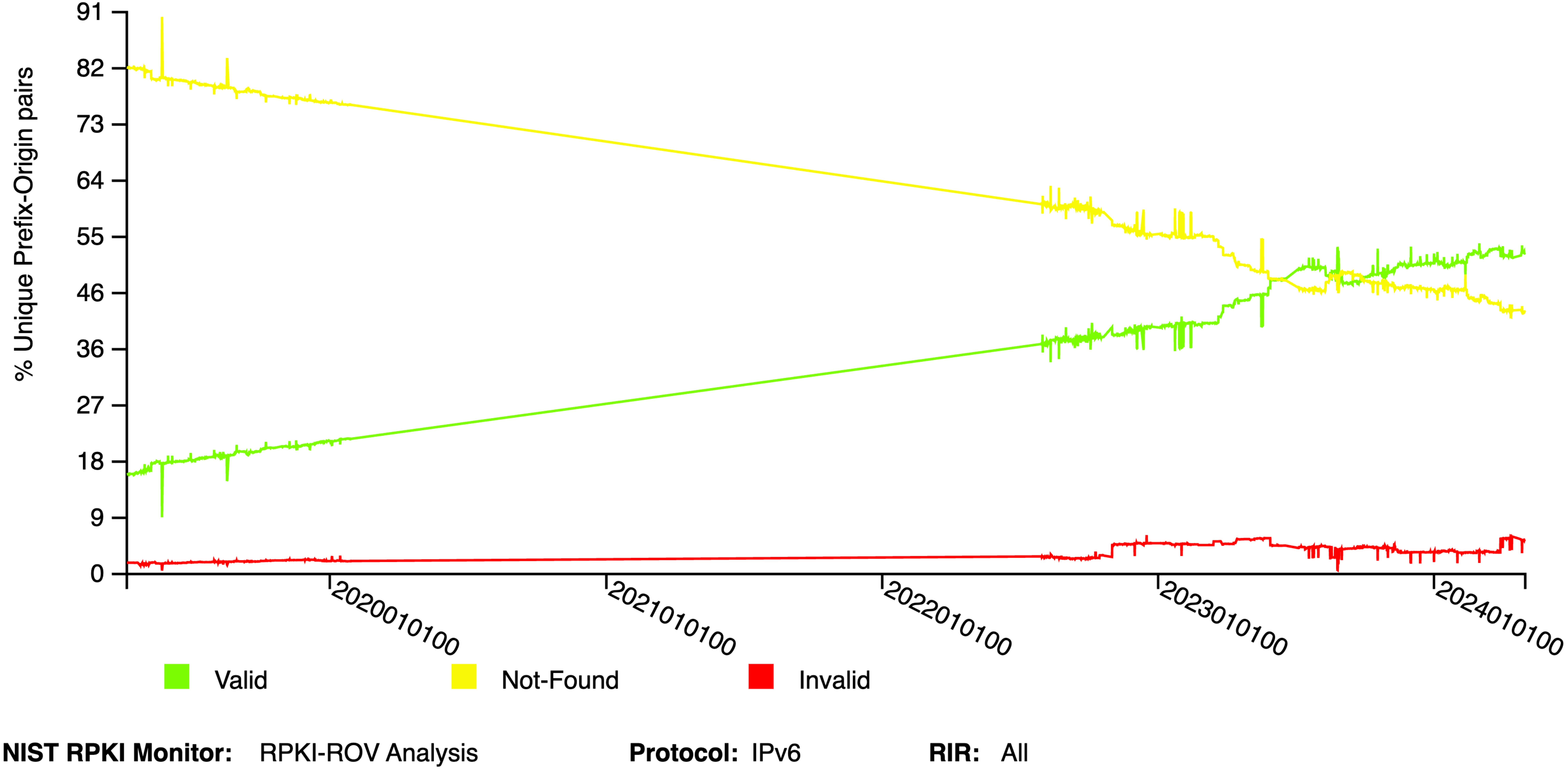
NIST RPKI Monitor: RPKI-ROV Analysis **Protocol:** IPv6 **RIR:** RIPE

RPKI IPv4 space coverage - Globally

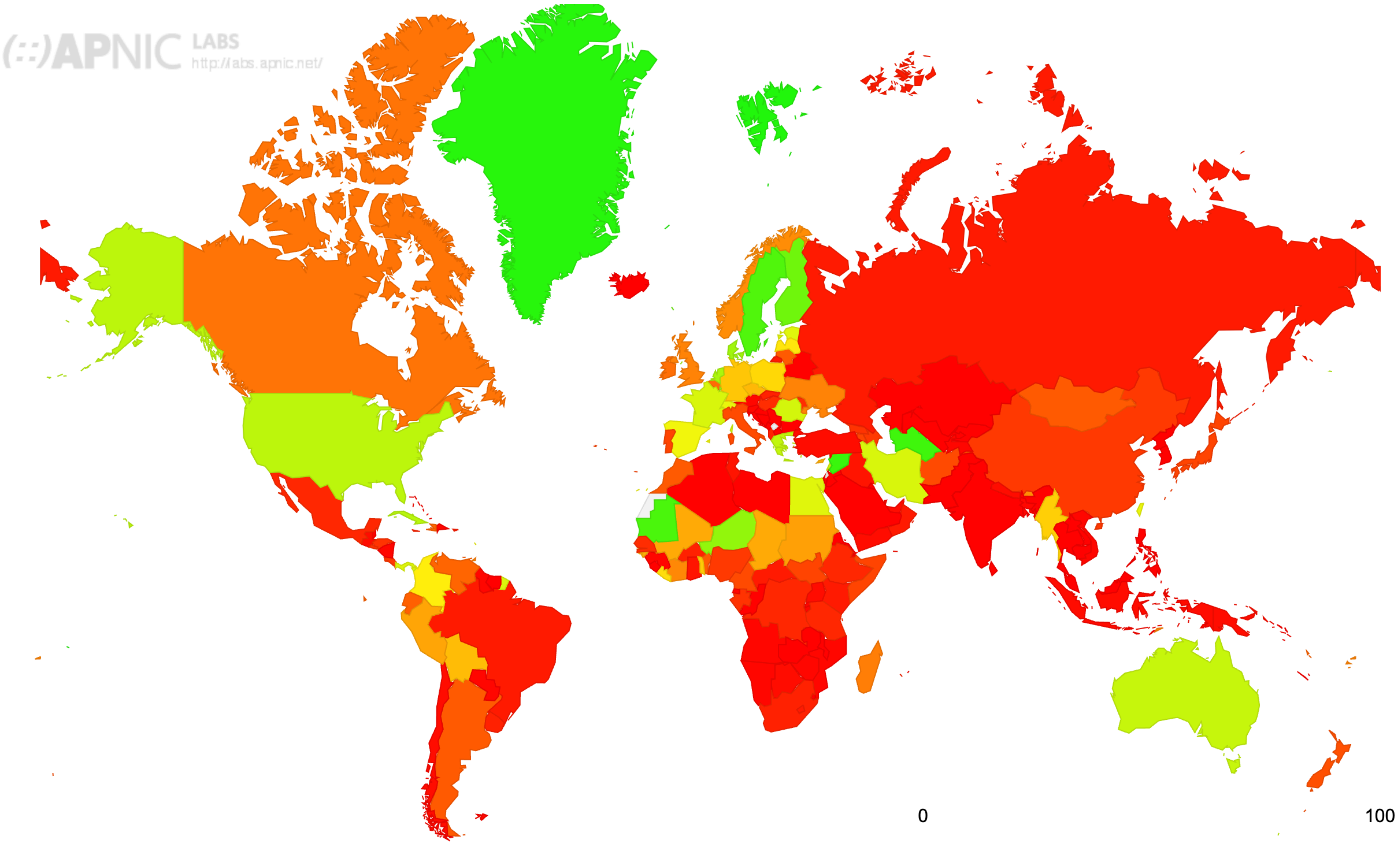


NIST RPKI Monitor: RPKI-ROV Analysis **Protocol:** IPv4 **RIR:** All

RPKI IPv6 space coverage - Globally

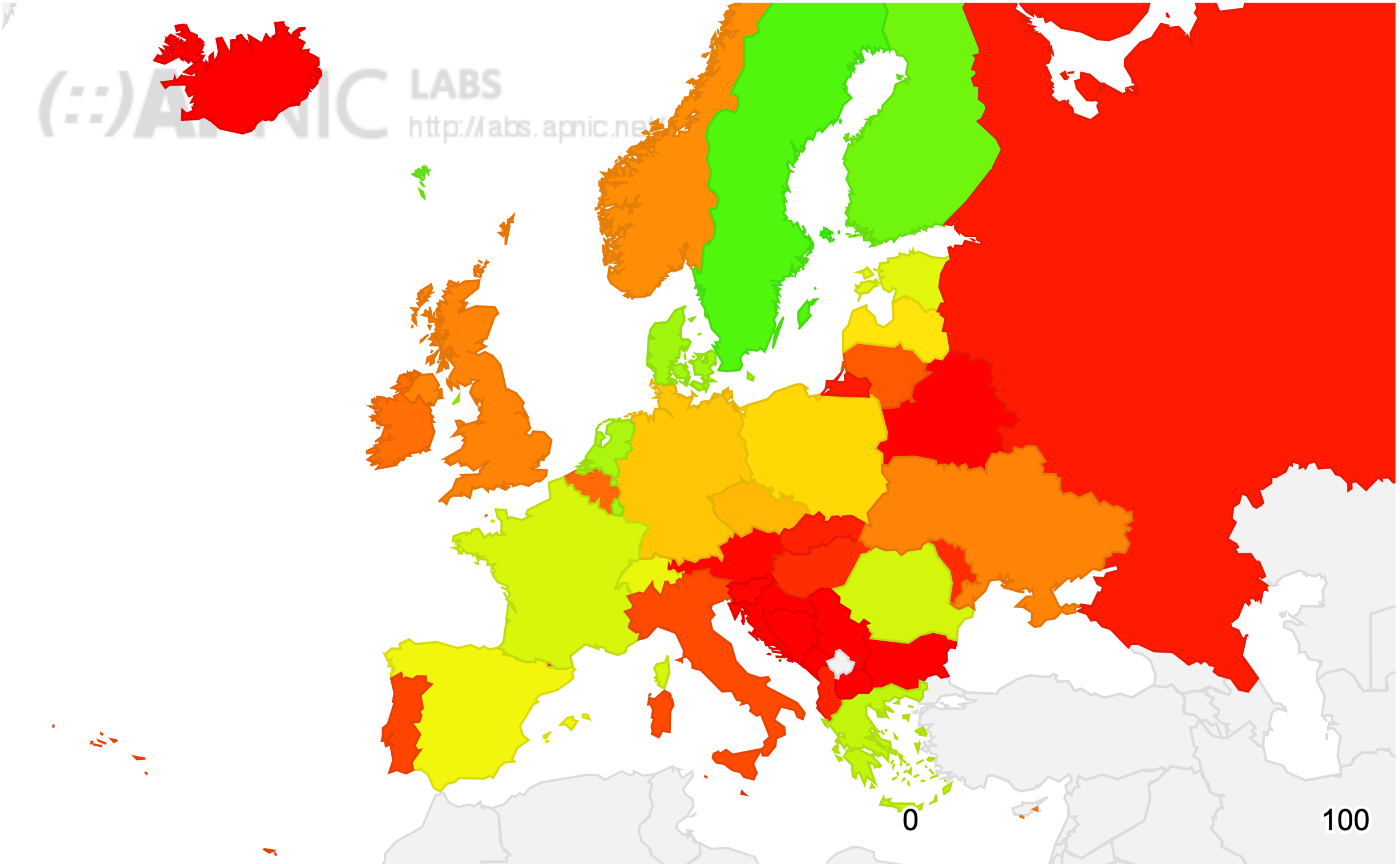


Are networks filtering based on RPKI data - Global?



Source: APNIC

Are networks filtering based on RPKI data - Europe?



Source: APNIC

A global RPKI ecosystem enhances routing security!

- RPKI is a powerful mechanism
  - Prevents BGP hijacks, mis-originations and route leaks
  - Currently used for validating the origin AS
  - Stepping stone to Full BGP path validation

- RPKI is opt-in
  - It will only work if every network agrees to abide by it

Let’s deploy RPKI today!

Give support for secure Internet routing
and
help to mitigate routing incidents globally!

Questions ?