

The Role of RIRs in RPKI Adoption

Cecilia Testart
Georgia Tech

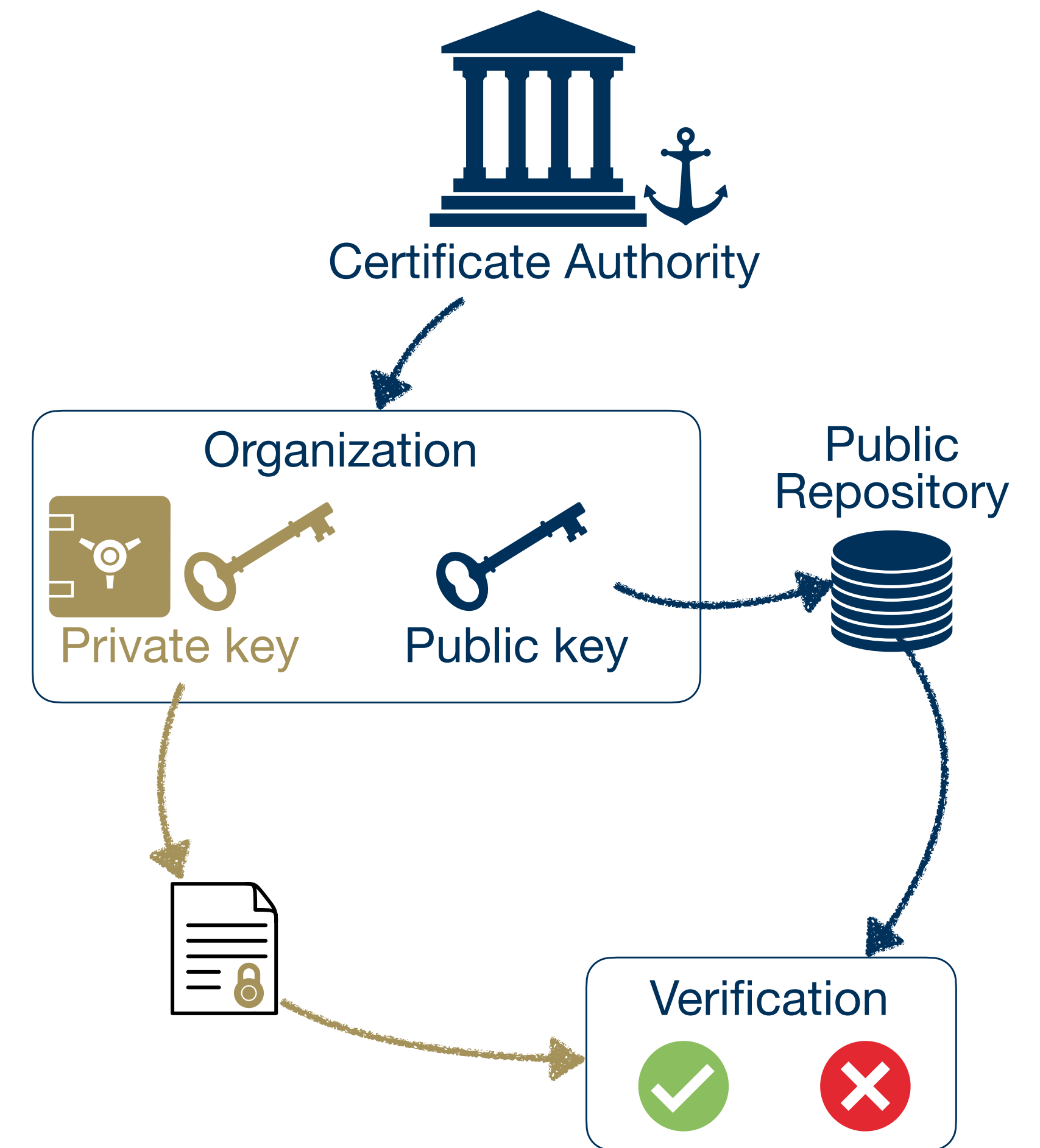
&

Josephine Wolff
Tufts University

TPRC'53
September 19, 2025

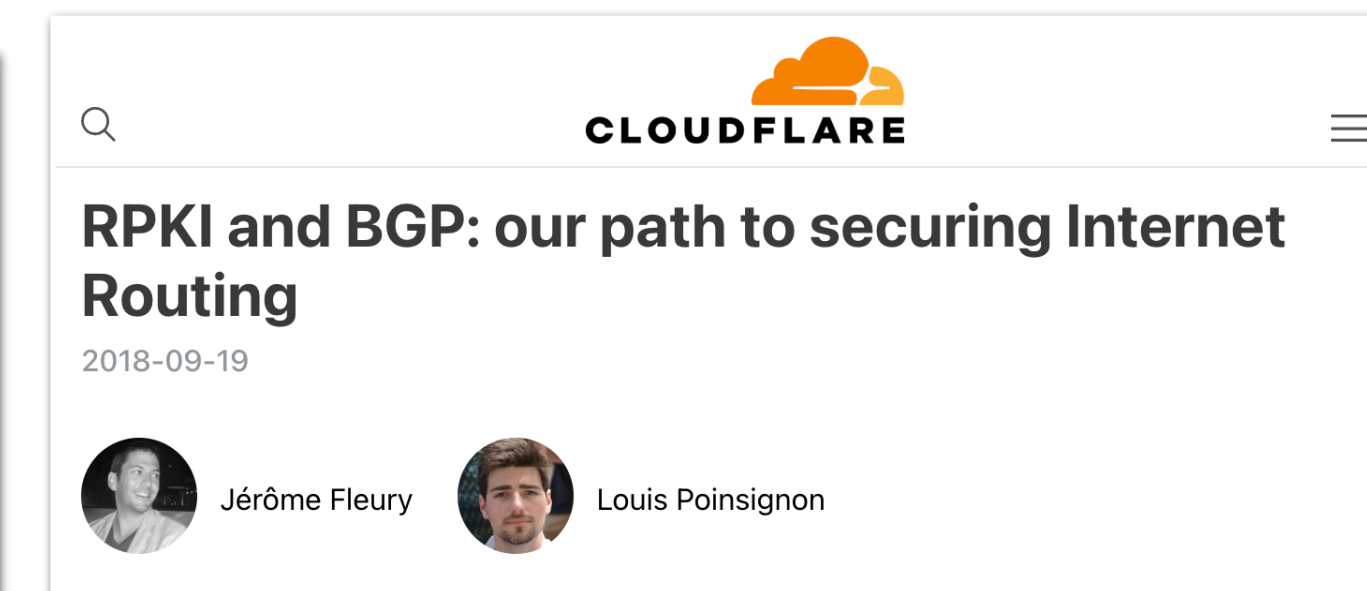
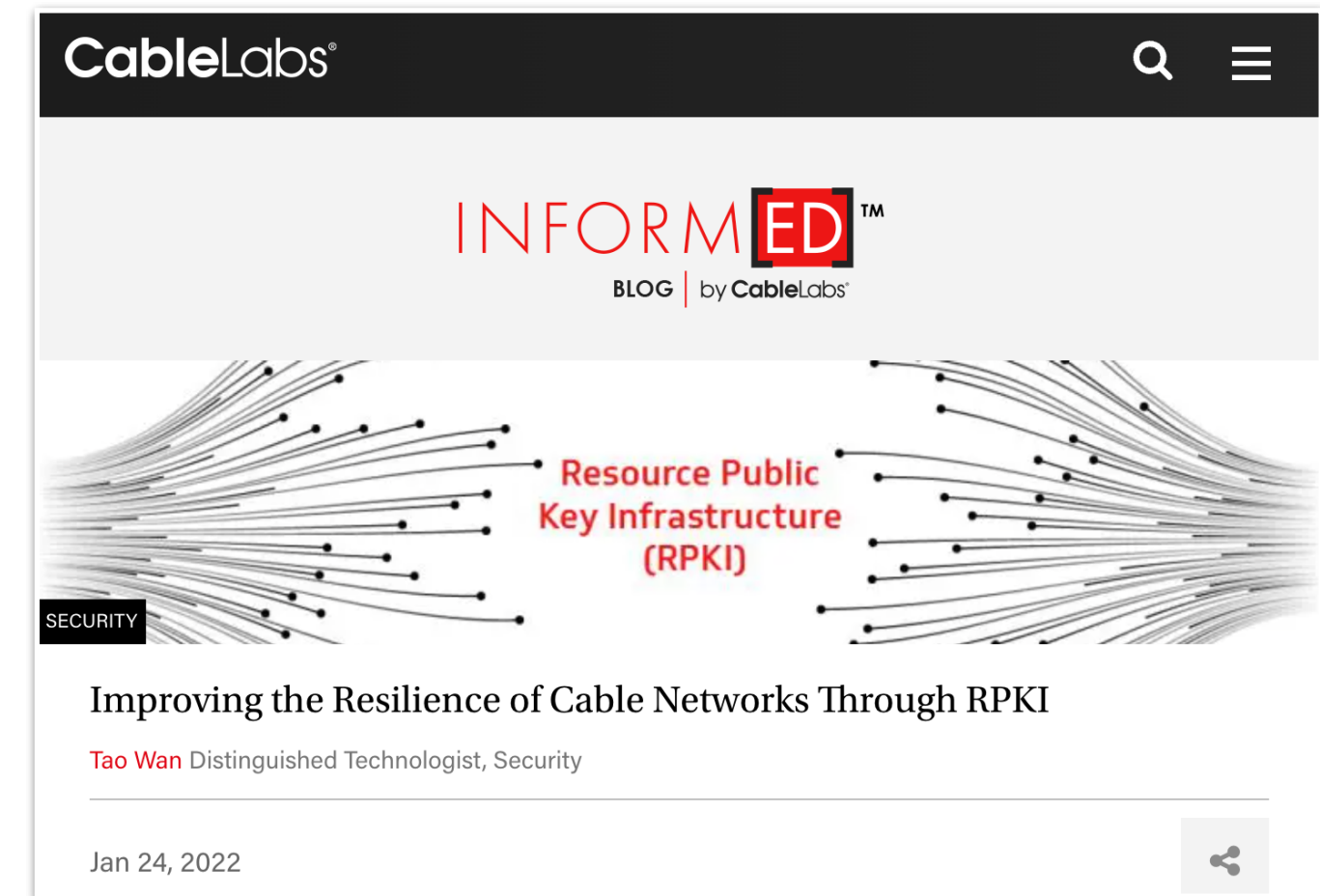
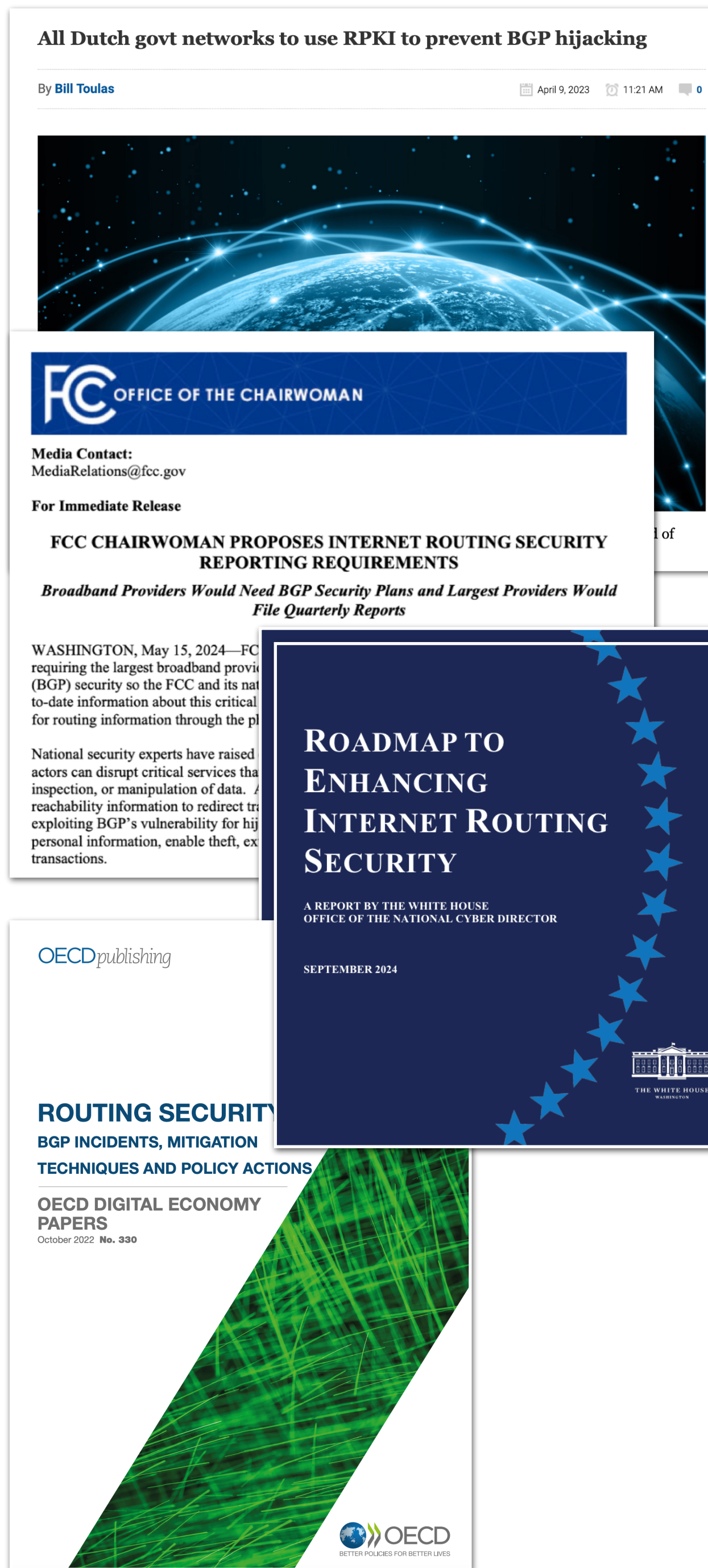
What is RPKI?

- IETF-standardized framework to cryptographically validate routing data.
- Off-band system allowing networks to issue Route Origin Authorization (ROA) certificates for their IP address blocks.
- Networks can use ROAs to perform Route Origin Validation (ROV), filtering invalid BGP messages and preventing misconfigurations and hijacks.



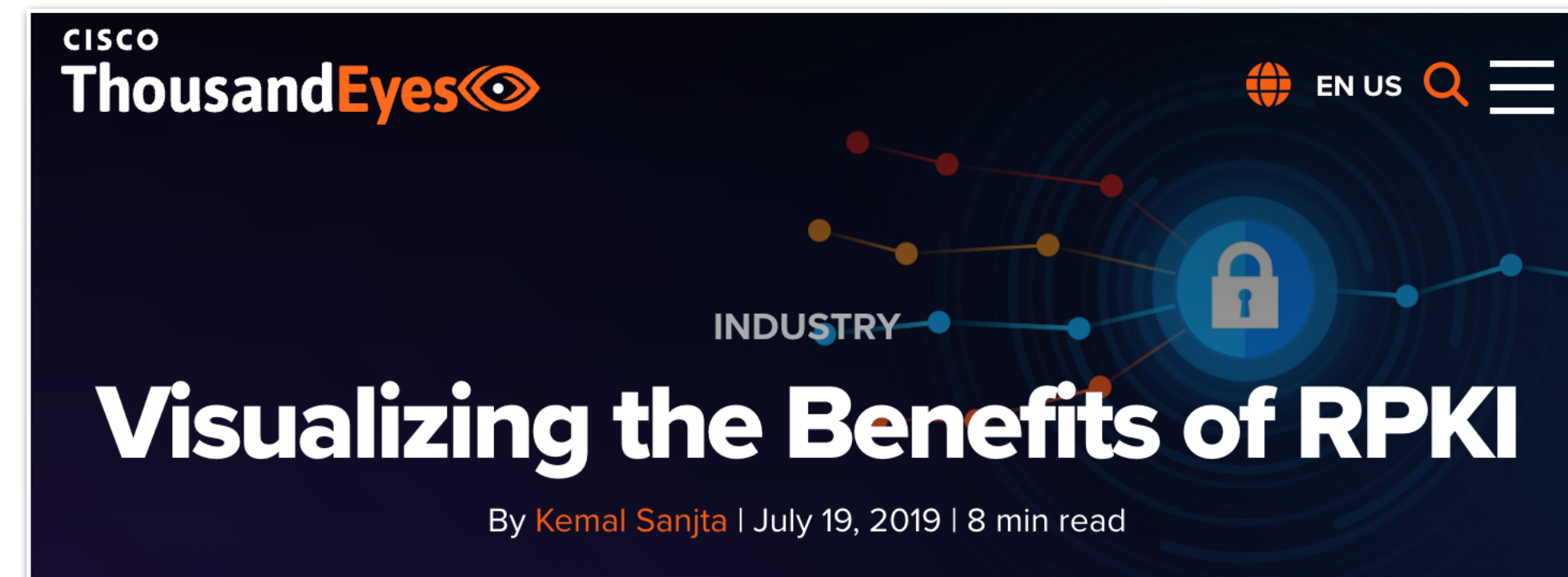
Why is it Critical?

- RPKI is the consensus solution to improve inter-domain routing security.



Why is it Critical?

- RPKI is the consensus solution to improve inter-domain routing security.
- It significantly reduces exposure to BGP hijacks and unintended routing misconfigurations.



SUMMARY

Over the last several weeks, some of the most prominent digital companies, including Amazon and most recently Apple experienced issues with their services. While the types of services each of these companies differ, the common thread was that they were a direct result of problems with the Border Gateway Protocol (BGP) that more than any other technology makes the Internet a resilient network. A key factor across these incidents was that they were quite costly for the companies involved.

fastly

War story: RPKI is working as intended



Job Snijders
Principal Software Engineer,
Fastly

November 05, 2024

CDN & Delivery

Security



To be very forward, this really is a story about something that turned out to be a problem at all. But sometimes boring stories deserve to be told. To provide context for this one, we have to go back to February 2008. Back then - through no fault of its own - one of the world's most popular video-sharing platforms suffered a multi-hour outage, interrupting millions of video viewings. The impact was significant that even mainstream media reported extensively on what was an arcane routing incident. But, nowadays we're hearing less and less about incidents like these, even though the Internet is bigger than ever. Three weeks ago, the target of a BGP hijack, similar to what happened in 2008, but this time barely anyone noticed. Why is that? Something has changed. In this article, I'll delve into one of the Internet's most remarkable, yet untold, success stories.

« kentik

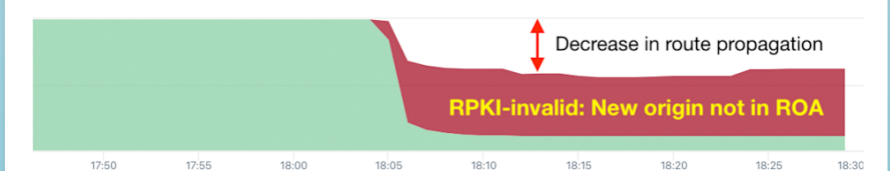
How much does RPKI ROV reduce the propagation of invalid routes?

Doug Madory & Job Snijders

August 24, 2022 [Internet Analysis](#) [RPKI](#)

Reachability / Visibility

Percentage of Kentik's BGP vantage points with routes to the monitored prefixes.



« kentik

TABLE OF CONTENTS

Summary

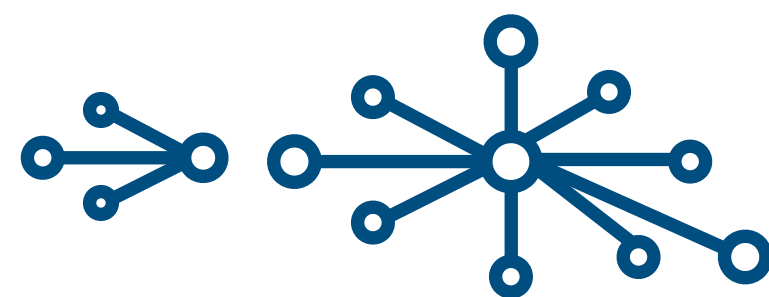
Subscribe

Our analysis from earlier this year estimated that the majority of internet traffic now goes to routes covered by ROAs and is thus eligible for the protection that RPKI ROV offers. This analysis takes the next step in understanding RPKI ROV deployment by measuring the rejection of invalid routes.

Motivation: RPKI adoption barriers



Region



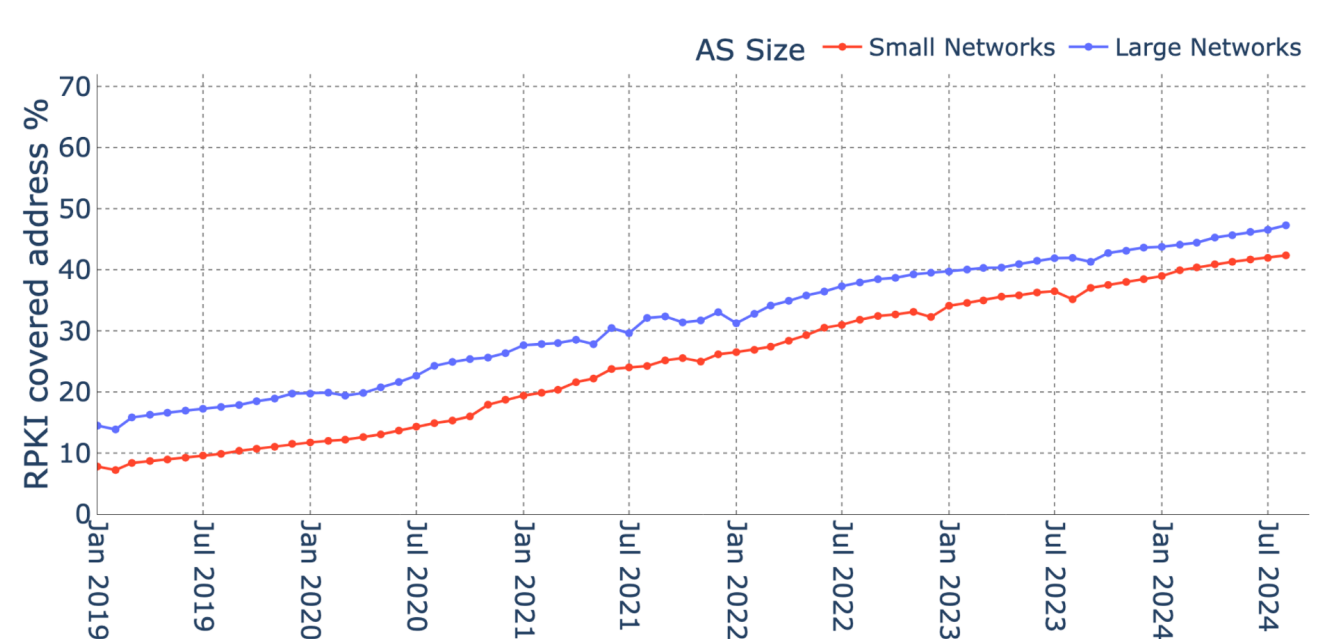
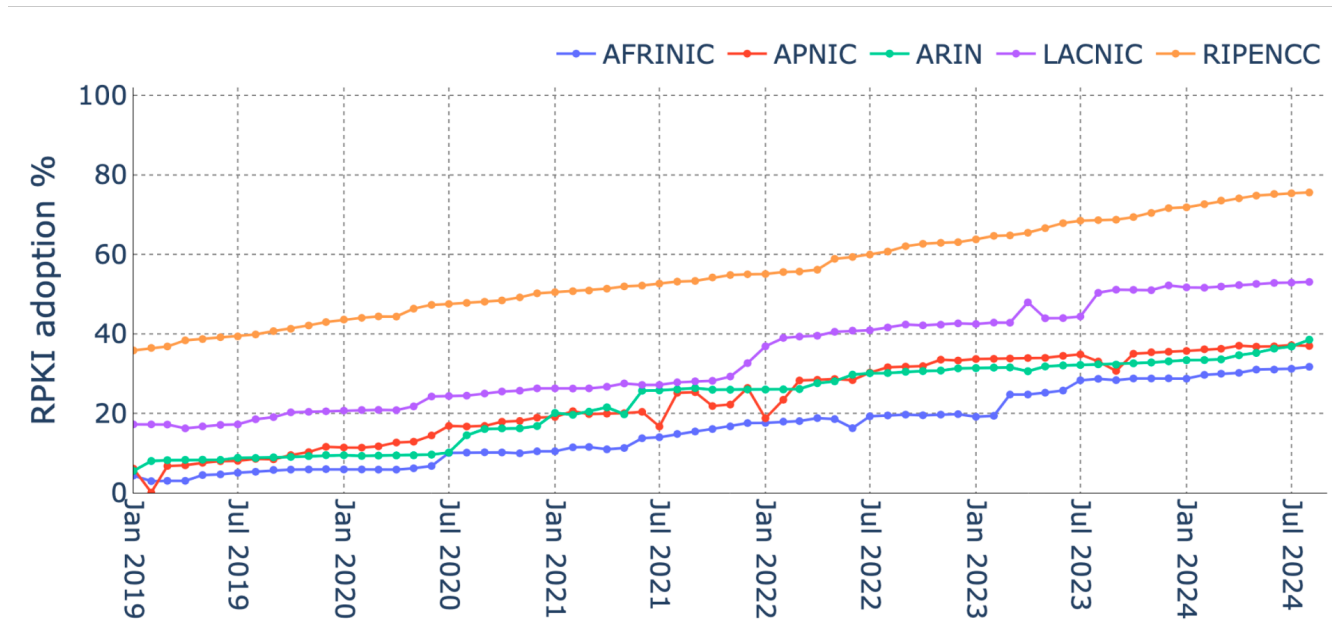
Size



Type

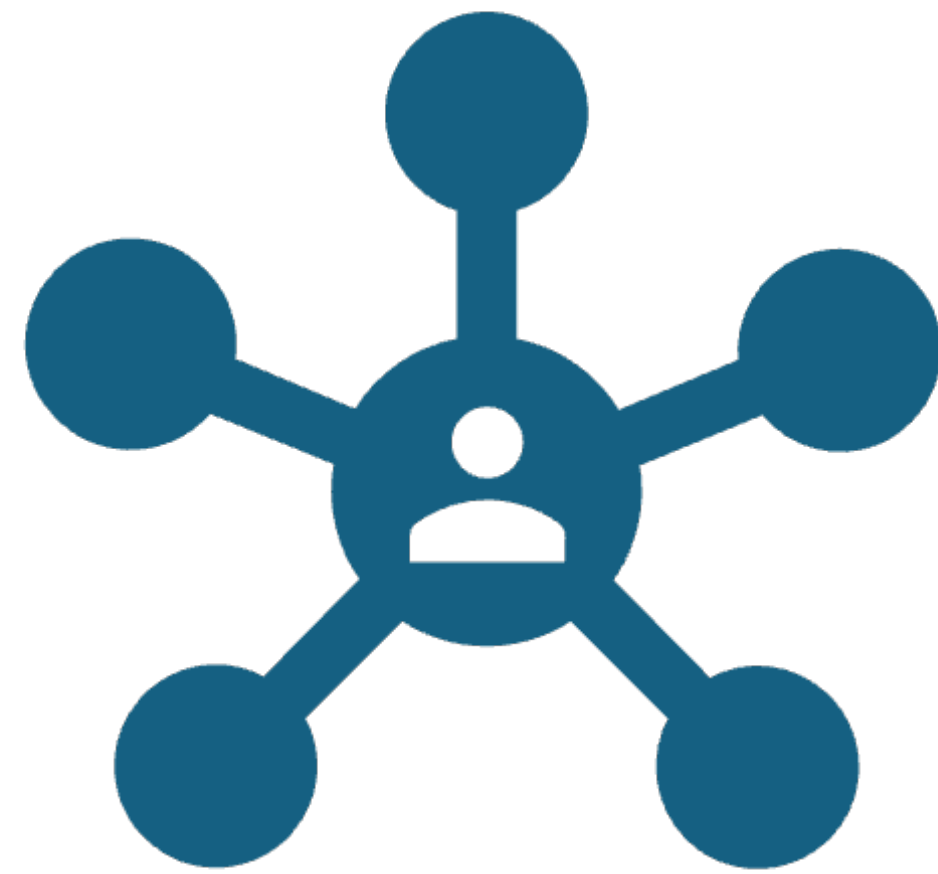
8.0.0.0/8

IP delegation



BGP.Tools labels	RPKI cov.%
Government	20.3
Academic	23.84
Mobile Data/Carrier	46.04
Server Hosting	51.19
Home ISP	45.06
Satellite Internet	85.84

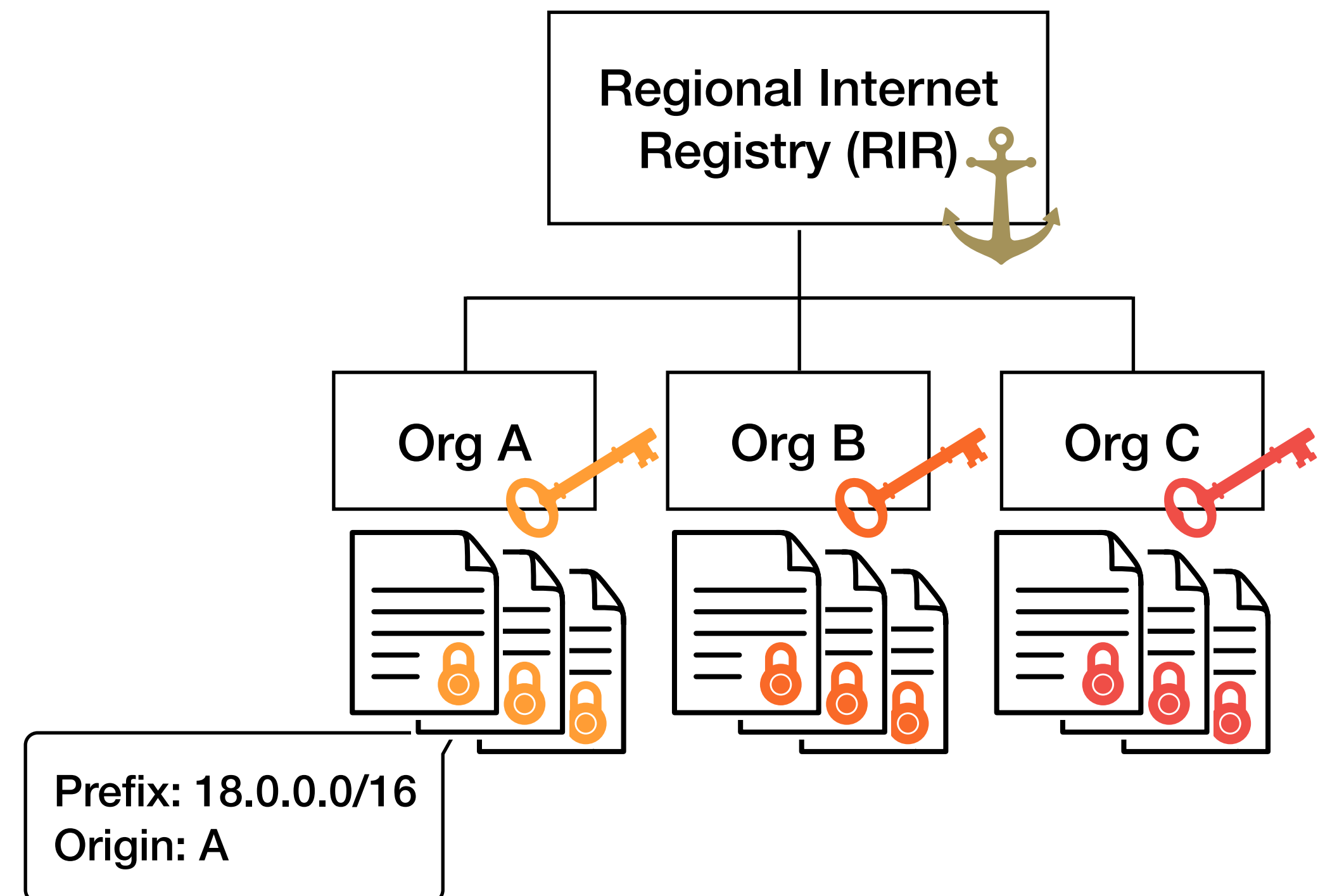
Methodology: A First-of-its-Kind User Study



- **Who:** 13 network operators substantially involved in RPKI decision-making.
- **Questions:** Role, RPKI status, challenges, what has helped.
- **Geographical Context:** Most interviewees were in North America.

This study focus: The Role of RIRs

- RIRs are the cryptographic roots of trust for the RPKI system.
- They provide the essential infrastructure to host RPKI certificates and keys for the Internet resources they allocate.



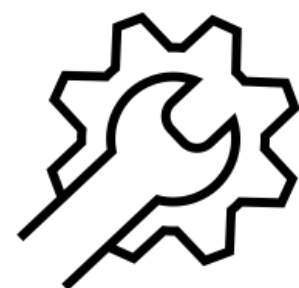
Four key areas where RIRs play a pivotal role



IP resource management



Awareness and training



Tooling for ROA creation and monitoring



Tooling for routing monitoring and incident investigation

Challenges with IP Management

*“our prefixes [that] are not covered by ROAs [...] is because of the years and years of **IP allocation and poor record keeping**. And then that's a big challenge.”*

*“A fair number of **[organizations]** don't have access to their **ARIN accounts**, they have to recover the orgs [..] so that's money and hassle [...]”*

*“By **signing the LRSA**, [...] [we] give ARIN certain rights that they don't have right now with that space. And that's been going back and forth between us and them, for you know at **least a year, if not 2 now**. [...] So until that gets sorted out, we're not really doing any [RPKI] ROAs.”*

RPKI & IP Resource Management

- For participants, streamlining IP management supported RPKI adoption.
 - Financial incentives
 - Authoritative resources lists
 - Having address space in multiple RIRs

The screenshot displays the ARIN Account Manager interface. On the left is a sidebar menu with options: Dashboard, Tickets, Your Records (expanded), Point of Contact Records (selected), Organization Identifiers, Associations Report, IP Addresses, ASNs, Routing Security, Transfer Resources, Payments & Billing, Downloads & Services, and Ask ARIN. The main content area is titled 'Point of Contact Record'. It features a green success message: 'POC was created. Your user account is not linked to this POC. Linking allows you to manage the POC.' with a 'Link to This POC' button. Below this is a 'POC Info' section containing details for a Point of Contact named 'Joe Route' associated with 'ROUTE8-ARIN'. The contact information includes a company name (None Specified), address (123 Main Street, Chantilly, VA 20151, United States), email (joeroute2024@gmail.com), and phone number (+1-309-543-5374 office). Public comments mention a website and NOC hours. The 'Other Info' section shows the record was registered and last modified on 01-11-2024 at 14:51:55.

ARIN

Feedback Welcome,

ACCOUNT MANAGER

Dashboard

Tickets

Your Records

Point of Contact Records
Manage POCs linked to your account

Organization Identifiers
Manage Org IDs and Org POCs

Associations Report
Records connected to your account

IP Addresses

ASNs

Routing Security

Transfer Resources

Payments & Billing

Downloads & Services

Ask ARIN
Create a help desk ticket

Point of Contact Record

✓ POC was created. Your user account is not linked to this POC. Linking allows you to manage the POC.

[Link to This POC](#)

POC Info

Point of Contact Info

POC: ROUTE8-ARIN
Name: Joe Route

Contact Info

Company Name: None Specified
Address: 123 Main Street
Chantilly, VA 20151
United States
Email Address: joeroute2024@gmail.com
Phone Number: +1-309-543-5374 (office)

Public Comments: http://www.example.net
Standard NOC hours are 7:00 AM to 11:00 PM EST

Other Info

Registered Date: 01-11-2024 14:51:55
Last Modified Date: 01-11-2024 14:51:55

Challenges with Awareness and Training

*“Just because you're a **routing jockey** doesn't mean you're familiar **with RPKI**. I had to educate some people that it's not going to knock some people off the network.”*

*“So the age old question is, **how do you teach people about NANOG that don't know about NANOG?** How do you reach people? How do you reach out to Joe's Bait & Tackle Internet service?”*

*“We were already talking about moving towards RPKI. I was doing **presentations and education of upper management** to get their buy-in.”*

RPKI Awareness and Training

- Factors that have driven adoption:
 - High-profile incidents.
 - Regulatory interest
 - Industry groups
 - Community sharing

kentik

What can be learned from recent BGP hijacks targeting cryptocurrency services?

Doug Madory
Director of Internet Analysis

September 22, 2022 [Internet Analysis](#) [Network Security](#) [Cloud](#)

Reachability / Visibility
Percentage of Kentik's BGP vantage points with routes to the monitored prefixes

BGP visualization showing the propagation of a malicious route

100%
50%
0%

20:00 20:30 21:00 21:30 22:00 22:30 23:00 23:30 Aug 18th

2022-08-17 to 2022-08-18 (UTC 1 minute increments)

MALICIOUS ROUTE

LEGITIMATE ROUTE

FCC OFFICE OF THE CHAIRWOMAN

Media Contact:
MediaRelations@fcc.gov

For Immediate Release

FCC CHAIRWOMAN PROPOSES INTERNET ROUTING SECURITY REPORTING REQUIREMENTS
Broadband Providers Would Need BGP Security Plans and Largest Providers Would File Quarterly Reports

WASHINGTON, May 15, 2024—FCC Chairwoman Jessica Rosenworcel today proposed requiring the largest broadband providers to file confidential reports on Border Gateway Protocol (BGP) security so the FCC and its national security partners can for the first time collect more up-to-date information about this critical internet routing intersection. BGP is the technology used for routing information through the physical and digital infrastructure of the internet.

National security experts have raised concerns that, by accessing vulnerabilities in BGP, bad actors can disrupt critical services that rely on the internet and result in misdirection, interception, inspection, or manipulation of data. A bad network actor may deliberately falsify BGP

CableLabs

INFORMED™
BLOG | by CableLabs

Resource Public Key Infrastructure (RPKI)

Improving the Resilience of Cable Networks Through RPKI

Tao Wan Distinguished Technologist, Security

Jan 24, 2022

Google

Experience and observations in deploying Cloud scale routing security

NANOG 93

Anees Shaikh

Challenges Issuing ROAs

*“I will say, probably the biggest challenge right out of the gate was just the **lack of actual tools and or software programs to help you monitor all of this**. It was, and still is sort of, you need this for this part and that for that part. And if you want to see if it's working, you need this other thing, and so on.”*

*“We did start registering routes---but we ran into the problem of **lack of common APIs across the RIRs**.”*

Tooling for issuing RPKI ROAs

- Participants praised user-friendly interface for manual ROA creation and API.
- RIPE ROA 'testing' ability and software development enabling faster RPKI adoption.
- Third-party tools such as Cloudflare Validator allow participants to debug issues

The image displays two screenshots of web interfaces for creating and managing Route Origin Authorizations (ROAs).

The top screenshot shows the ARIN ACCOUNT MANAGER interface for 'RPKI: Create ROA'. It includes a sidebar with navigation links like Dashboard, Tickets, and Routing Security. The main form, titled 'Create a Route Origin Authorization (ROA)', contains fields for 'Origin AS' (399970), 'Prefix' (with a 'Max Length' dropdown), 'Prefixes' (with an 'Additional Prefix' button), and 'ROA Name'. A 'Next Step' button is at the bottom right. A note at the bottom explains that a ROA is a cryptographically signed object authorizing an AS to originate a prefix.

The bottom screenshot shows the RIPE NCC RPKI Dashboard. It features a navigation bar with links like 'Manage IPs and ASNs', 'Analyse', 'Participate', 'Get Support', 'Publications', and 'About Us'. The dashboard displays '2 BGP Announcements' (2 Valid, 0 Invalid, 0 Unknown) and '2 ROAs' (2 OK, 0 Causing problems). A table titled 'Route Origin Authorisations (ROAs)' lists two entries, both with 'VALID' status. The table has columns for 'Origin AS', 'Prefix', and 'Current Status'. The footer includes social media links and a list of links like Home, Sitemap, Contact Us, etc.

Challenges monitoring routing

*“I'm trying to **unravel all of the different pieces of IP space** that we have.[...] And so what I've been doing a lot of is digging through our routing.”*

*“I use just a ton of **hand shell scripts**, with grep CIDR and dumping routing tables. **Every day**, you know, I go through and pull out what [is] originating from my ASNs.”*

*“So the main barriers for ROA were that we needed to **get our hands around the data**. We needed to understand the data and we needed to **convince people it wasn't going to cause any outage**.”*

Support for Routing Monitoring and Incident Investigation

RIPE NCC

IPs & ASNs Analyse Community Membership Events Training Docs About

Statistics Internet Measurements DNS Raw Datasets Archived Projects Sponsorship

RIPE Atlas

RIPEstat

RIS

Documentation

RIS Peers List

RIS Peering Policy

RIS Data Access

RIS Commercial Use

RIPE IPMap

Internet Traffic Maps

Analyses and Use Cases

Home / Analyse / Internet Measurements / RIS

Routing Information Service (RIS)



ROUTE VIEWS 6447

HOME ABOUT FAQ PEERING TOOLS COLLECTORS

PAPERS SUPPORTERS BLOG CONTACT

University of Oregon RouteViews Project

RIS is a routing data collection platform

Events Acknowledgements About Contacts

Global Routing Intelligence Platform

Select an event type

All MOAS Sub-MOAS New Edge Defcon

Select an event suspicion level

All Suspicious Grey Benign

Select time period (UTC now: Sep 19, 2025 2:33 PM)

From: Sep 18, 2025 10:33 AM

To: Sep 19, 2025 10:33 AM

Predefined ranges

Search by prefix/ASN/tags

Search by prefix/ASN/tags

Search

Events List

Potential Victims	Potential Attackers	Largest (Sub)Prefix	# Prefix E...	Start Time	Duration	Suspicion	Category	Type
AS44444	AS203	116.50.56.0/24	1	2025-09-19 12:10	15 min	High	Default Tr Worthy	moas
AS367	AS56	132.22.0.0/16	1	2025-09-19 11:15	ongoing	High	Default Tr Worthy	moas
AS210846 AS6206	AS42241110	45.133.174.0/24	1	2025-09-19 10:15	5 min	High	Default Tr Worthy	moas
AS6206	AS42241110 AS42241101	185.155.170.0/24	1	2025-09-19 10:15	5 min	High	Default Tr Worthy	moas
AS215929 AS6206	AS42241110	62.164.177.0/24	1	2025-09-19 10:15	5 min	High	Default Tr Worthy	moas

MANRS OBSERVATORY

OVERVIEW HISTORY COMPARISON ROA STATS ABOUT

99%
0.0% →

89%
1.1% ↗

89%
0.0% →

87%
0.1% ↗

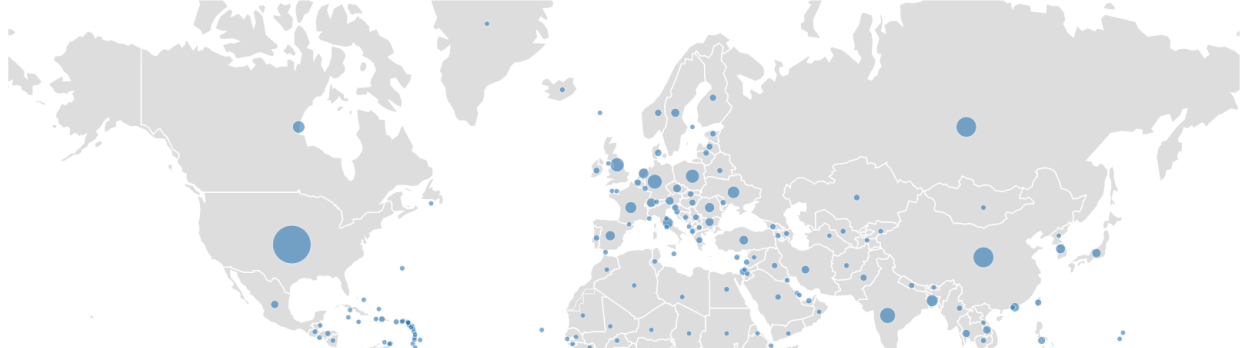
47%
0.1% ↗

● Ready ● Aspiring ● Lagging ● No Data Available

Global view

Size: # of ASNs | Incidents | Culprits

Region: Country | UN Regions | UN Sub-Regions | RIR Regions



Kentik Map

Filters 0 Time Range (UTC) Last 4 weeks and 2 days

View Kube View Logical Map Details

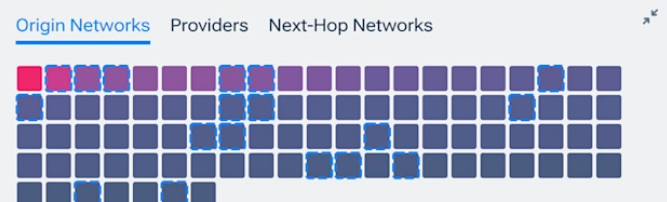
Clouds

Amazon Google Microsoft Azure IBM Cloud

507 Mbps 2304 Mbps

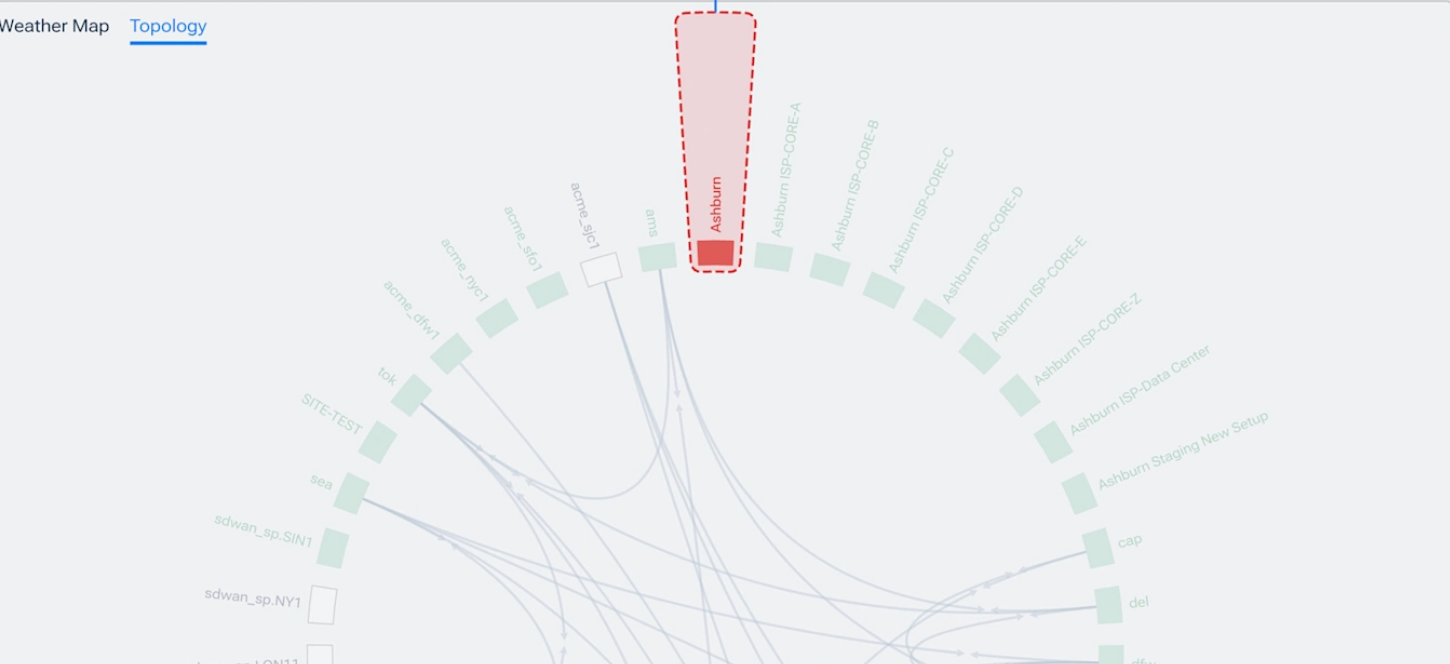
Internet

Origin Networks Providers Next-Hop Networks



On Prem

Weather Map Topology



Site Details

Ashburn

Type Data Center

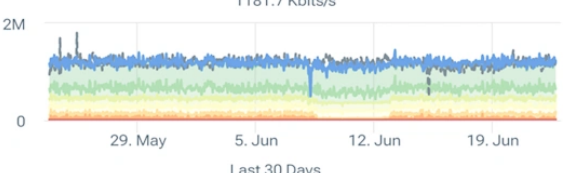
Address 21715 Filigree Ct, Ashburn, VA 20147, USA, Ashburn, Virginia, 20147, United States

View Topology

Internal Map Details

Traffic

All Traffic Application Avg bits/s



1181.7 Kbits/s

Application

Historical Total: 7 days back

Total

https

GRE

Average Kbits/s

Devices

Critical

Health

Critical

Ingress Interface Capacity

aws-proxmox-02-pub-vif-s3: GigabitEthernet1 1

241%



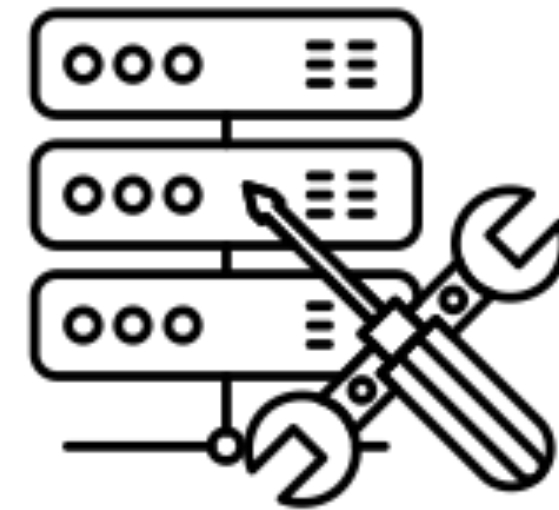
Capacity (1 Gbits/s)

Recommendations



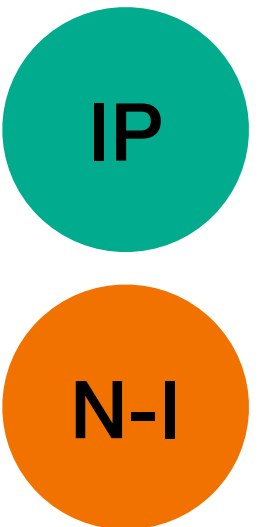
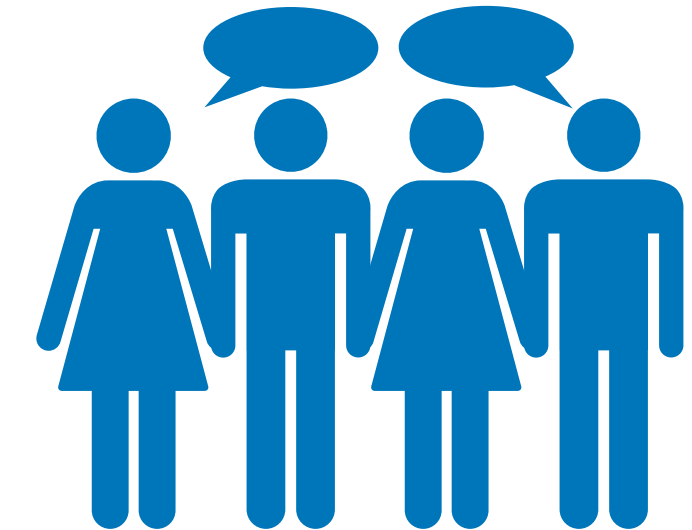
New channels for awareness and training

- Specific industry groups
- Cybersecurity standard training
- Connectivity provider



More software tools for RPKI

- Testing of ROAs
- Signaling of missing ROAs
- Signaling of changes in ROAs



Community knowledge sharing

- RPKI adoption journey
- Integration with operation
- Decision-making analysis

Conclusions

- RIRs are uniquely positioned to support RPKI adoption.
- There are successful strategies
 - RIPE's leadership

