The Role of RIRs in RPKI Adoption

Cecilia Testart[1] and Josephine Wolff[2]

[1]Georgia Institute of Technology
[2]Tufts University

August 2025

Abstract

Recognizing the relevance of securing inter-domain routing to protect traffic flows in the Internet, the Internet Engineering Task Force (IETF) standardized the Resource Public Key Infrastructure (RPKI), a framework to provide networks with a system to cryptographically validate routing data. Despite many obstacles, RPKI has emerged as the consensus to improve routing security and currently about 50% of routed IP address blocks are part of the system. The Regional Internet Registries (RIRs) are in charge of allocating address space in five different geographical zones and play a crucial role in RPKI: they are the roots of trust of the cryptographic system and provide the infrastructure to host RPKI certificates and keys for the Internet resources allocated in their region. Organizations and networks wanting to issue RPKI records for their address space need to follow the process from the RIR that delegated their address space. In this paper, we analyze the RIRs' implementation of RPKI infrastructure from the perspective of network operators. Based on in-depth interviews with 13 network engineers who have been involved in their organizations' efforts to adopt RPKI, we examine the RIR initiatives that have or would have most supported RPKI adoption for different types of organizations. Given RIRs have independently developed and implemented the cryptographic infrastructure as well as the tooling to issue and manage certificates, we offer recommendations on strategies that have encouraged RPKI adoption.

1 Introduction

In 2012, the IETF standardized the Resource Public Key Infrastructure (RPKI), a framework that allows networks to issue cryptographic records that can then be used to validate routing data exchanges by networks through the Border Gateway Protocol (BGP). RPKI has slowly been adopted by networks around the globe, and currently almost 50% of IP address blocks advertised in BGP are covered by RPKI records. This project focuses on trying to understand why adoption rates of RPKI are so low, given the critical security benefits it provides, and what approaches might be most effective in trying to promote adoption more widely. The barriers to RPKI adoption are not merely technical, they also include substantial legal, organizational, and political challenges, including concerns about cost, collective action, and contractual obligations.

There is significant heterogeneity in the level of RPKI adoption by different networks depending on several factors including the region, the size of the network, the type of IP and the practices of the network providers. As an example, Route Origin Authorizations (ROAs) adoption from networks in Europe, the Middle East, Central Asia (RIPE NCC zone) is more than twice the adoption level of networks from North America (ARIN zone). Furthermore, within the ARIN zone

(North America), only 18% of the IPv4 address space originated by the smallest 10% of networks is covered by RPKI records compared to 30% of the address space of the largest 10% of networks. In IPv6, there is overall more adoption but the difference between small and large organizations is more than twice as large: 29% coverage for the smallest networks versus 73% coverage for the largest ones.

The disparities in RPKI adoption levels point to different challenges and roadblocks in organizations' processes for implementing workflows to adopt RPKI. Adopting RPKI requires training for network engineers and administrators. Prior studies have pointed out legal and operational barriers to the adoption of routing security practices including RPKI. As an example, a legal agreement is required for organizations within the ARIN zone to issue RPKI records, and small organizations may not have the legal resources to handle that.

However, barriers impact organizations differently depending on organizational characteristics. For instance, organizations that originate routes in BGP for the IP address block they hold experience different management challenges from the organizations that have agreements with network providers to originate their IP address block. Similarly, the Regional Internet Registries (RIRs), which delegate IP addresses for each of the 5 regions that together cover the globe, set up the process to issue RPKI records independently, and as a result the requirements and management tools are not the same across different regions.

This paper draws on interviews with networking security stakeholders across the RPKI ecosystem to identify specific barriers that are preventing networks from issuing RPKI records to improve their routing security, and in particular, the role of the RIRs in facilitating RPKI adoption. We first discuss the role of RIRs in RPKI deployment and then identify four areas in which RIRs can play a pivotal role in this process: (1) IP resource management, (2) raising awareness and administering trainings for organizations about the importance of RPKI and how to deploy it, (3) developing tooling and software for ROA creation and monitoring, and (4) developing tools for routing monitoring and incident investigation. Finally, we discuss potential recommendations for how RIRs can more effectively engage with this process through each of those areas.

2 Background

The Resource Public Key Infrastructure (RPKI) is a framework to secure routing by providing an off-band cryptographic system to validate routing information. Despite many obstacles, RPKI has emerged as the consensus to improve routing security. Many governments and industry groups have pushed for more RPKI adoption [6, 17, 16, 13]. As of August 2025, 56% of routed IPv4 address blocks and 59% of IPv6 address blocks are covered by Route Origin Authorization (ROA) certificates.

For RPKI to work, there are two set of actions that need to be taken, one by holders of address space—the entity that has been delegated IP address block(s)—, and the other by the networks that provide Internet connectivity and transit:

1. Organizations need to issue cryptographic records following the RPKI process to protect the IP address blocks they hold. More specifically, they need to issue Route Origin Authorization certificates providing the valid Autonomous System Number (ASN) of the network authorized to originate in BGP the IP address blocks they hold;

2. Networks need to use the information in valid RPKI certificates to validate information in BGP, filtering invalid messages and effectively preventing the spread of invalid information. This step is referred to as Route Origin Validation (ROV).

Although both aspects of RPKI are essential to improve routing security, this paper focuses on the first one: the issuance of ROA certificates for of IP address blocks. We focus on this aspect for two reasons. First, without this initial step, even if most transit providers are filtering invalid BGP messages, organizations do not benefit from RPKI because it is impossible to identify invalid messages for the IP address blocks they use. Second, for the entire Internet ecosystem to benefit RPKI, the first component—issuing ROA certificates—requires widespread adoption by all organizations holding IP address blocks.

While the second component for RPKI to work, Route Origin Validation (ROV), has seen significant uptake by large transit providers and almost all Tier 1 networks filter RPKI invalid information in BGP [5] , its effectiveness is limited without comprehensive ROA coverage. This is because validation systems can only filter invalid routes for IP address blocks that are protected by a ROA. Conversely, when ROAs are in place, the current level of Route Origin Validation in the internet is already effective at limiting the spread of invalid routes. A Kentik case study of an August 2023 route leak showed that most RPKI-invalid routes were seen by less than 15% of vantage points of BGP collectors [12], demonstrating that once an address block is protected by a cryptographic record, invalid BGP messages related to it have limited impact. Therefore, for any organization to reduce its exposure to hijacks and routing misconfigurations, it is essential that it first issues ROAs to protect its IP address blocks. This action is a prerequisite for that organization, regardless of its size or function, to benefit from the broader security framework.

For broader RPKI adoption and effectiveness, *all* organizations holding IP address blocks need to issue ROA certificates, independent of organization size, place in the Internet topology or main business activity. Non-ISP organizations, such as enterprises, schools, hospitals, utility companies, and scientific and educational organizations, are a critical group that must adopt Resource Public Key Infrastructure (RPKI). Even though these organizations main business is not to provide Internet services, they often hold their own IP address space. As the holders of this address space, they are the only ones who have to issue the Route Origin Authorization (ROA) certificates necessary to protect their internet routes. Therefore, to benefit from the security RPKI provides, it is essential for these non-ISP entities to implement and deploy a suitable management process for issuing ROAs. Nonetheless, for many of those organizations, issuing ROAs can be a challenging process

When we discuss RPKI adoption, we specifically refer to the steps involving the issuance of Route Origin Authorizations. To issue ROAs, the following considerations are relevant:

- Only the documented organization holders of IP address blocks, according to one of the five Regional Internet Registries (RIRs) can issue ROAs for the address block(s) they hold.
- To issue ROAs, organizations have to follow the process determined by the RIR that delegated the address block.
- If the address space was delegated before the existence of RIRs, the organization still has to follow the RPKI process of the RIR assigned to the geographical zone of the organization. This address space is referred to as *legacy* address space.

Currently, the organizations in charge of issuing RPKI ROAs are the holders of address space. The *holders* are the only organizations allowed by RIRs to issue ROAs, even if their address space is then routed by a network provider. This paper focuses on the critical role Regional Internet Registries (RIRs) play in facilitating the adoption of RPKI by organizations that hold IP address space. Drawing on in-depth interviews with network engineers, it examines their RPKI adoption journey, identifying the challenges they have faced and the specific aspects that have supported the process. In particular, this paper assesses the barriers to wider RPKI adoption by considering

factors such as IP resource management, awareness and training, and the availability of tools for creating and monitoring ROAs and for monitoring and debugging routing incidents.

2.1 Related Work

Most related work has studied RPKI adoption from the measurement perspective. Many studies have analyzed the evolution of IP address space covered by RPKI Route Origin Authorizations (ROA) over time [4, 7, 8, 9, 10, 11, 15, 18, 19]. Other works have focused on measuring Route Origin Validation (ROV) adn its impact [10] in routing, to detect BGP hijacking [18], and to evaluate the overall readiness of the RPKI framework to improve routing security [4, 7]. In addition, other studies have focused on specific aspects related to the issuance of ROA certificates [8, 9, 11, 15], or on RPKI adoption by specific parts of the web infrastructure such as the hosting infrastructure of popular websites [19]. Drawing on large-scale internet measurements, these studies have collectively emphasized the benefits of the RPKI framework and its readiness for wider deployment despite slow adoption rates, while also issuing recommendations for specific configurations to reduce misconfigurations and increase protection

While many studies have analyzed RPKI deployment at an Internet- or RIR-wide level, a few have begun to investigate specific barriers hindering its adoption. In practice, RPKI adoption is influenced not only by the technical characteristics of certificates but by the full spectrum of an organization's processes, from legal agreements to daily routing operations. For instance, [20] specifically examined the legal barriers to RPKI adoption and explored potential ways to lower them. Similarly, [19] focused on the web ecosystem, identifying website popularity as a potential factor explaining the adoption of RPKI by hosting infrastructure. However, because these prior efforts did not deeply consider the distinctions between the types of networks and organizations behind specific address spaces, they provide limited visibility into the full range of specific obstacles encountered during the adoption process

To the best of our knowledge, this is the first user-study investigating the RPKI adoption process. We build on our previous research, which studied in-depth the characteristics of networks impacting the level of RPKI adoption at a time when coverage had already hit nearly 50%, proving it is the consensus solution to strengthen routing security. As of August 2025, 56% of routed IPv4 address blocks and 59% of IPv6 address blocks have adopted RPKI, indicating that the internet is no longer in the early adoption phase. With this interview-based study, we hope to gain deeper visibility into the specific socio-technical barriers different organizations face—from legal and organizational challenges to resource constraints—and understand how RIRs and policymakers can best tailor their efforts to assist different types of organizations in strengthening network security

3 Methodology

To understand the RPKI adoption process and the role RIRs play in it, we conducted semi-structured interviews with 11 network security specialists involved in deploying RPKI, representing 8 different organizations, including commercial ISPs and non-profit organizations. The interviews were conducted either via synchronous video call over Zoom or in person, where possible, and they were recorded for transcribing purposes. These interviews were conducted between November 2024 and June 2025. The interview process was approved by the IRB at Tufts University and Georgia Institute of Technology.

To select interview candidates, we approached industry leaders whom we had met previously at network security events and asked them to recommend other participants to us. We also contacted participants at a networking security workshop to follow up for more in-depth conversations. We

specifically sought out individuals directly involved in RPKI decision-making within their organizations—the ones driving adoption internally. We asked them to recommend other participants who shared this deep involvement, such as those deciding on implementation strategies, determining the necessary systems, tools, analysis, and monitoring to have in place for adoption, or those involved in negotiating the legal agreements required to adopt RPKI

While our interview sample size is small, we believe this initial, exploratory analysis offers a useful window into how these stakeholders have approached RPKI deployment and what has or has not worked well for them. We would also note that most of the network operators we were able to interview during this period are in North America and this shaped the RIRs that they had experience with. Therefore, many of our examples are drawn from interactions with ARIN.

Following the transcription of the interviews, we then identified common themes across these conversations and recurring challenges that participants pointed to in trying to roll out RPKI. Finally, we categorized RIR involvement according to these themes.

4 RPKI entanglement in RIRs' operation

The Regional Internet Registries (RIRs) play an essential role in RPKI. RIRs are in charge of making the backend cryptographic infrastructure work, are the cryptographic roots of trust, and host most RPKI certificates and keys for the Internet resources allocated within their respective regions. In addition, RIRs define how network operators and organizations holding address space can access and create RPKI certificates, which from the interview participants' experience has a subtantial impact on their ability to adopt RPKI. However, each of the five RIRs has independently developed and implemented its cryptographic infrastructure, as well as the specific tooling to issue and manage certificates. This independent development has led to variations in requirements, membership costs, legal agreements needed to access management portals, and the functionality of these portals across different regions. These factors directly impact the ease and rate of RPKI adoption, as organizations must follow the specific processes determined by the RIR that delegated their address block to issue Route Origin Authorizations (ROAs). This section delves into our findings regarding the crucial role RIRs play in facilitating RPKI adoption, identifying four key areas of entanglement in their operations: IP resource management, raising awareness and administering training for organizations, developing tooling and software for ROA creation and monitoring, and developing tools for routing monitoring and incident investigation.

4.1 IP resource management

The Resource Public Key infrastructure is inextricably linked with the management processes of Internet resources established by the RIRs. The RIRs are the ones that hold the root of trust of the PKI and provide IP holders the cryptographic key to issue their certificates. The distribution of these keys and the signing of certificates is done mostly through the RIR resource management portal. Therefore, factors such as membership cost and legal agreements needed to get access to the management portal and the functionality of the portal impact the adoption of RPKI.

4.1.1 The challenges

There are specific challenges organizations encounter in managing their IP resources and as RPKI adoption depends on IP resources management, it impacts RPKI adoption.The challenges encompass obstacles related to legacy address space and legal agreements, difficulties withaccount access and administrative hurdles, and the pervasive issue of oor record-keeping for IP allocations. Such

barriers highlight how the intricacies of IP resource management, often compounded by varying RIR requirements, can significantly impede an organization's journey toward securing the routing of its address space.

Legacy address space and legal agreements: When the IP address space has been directly delegated by RIRs, the relationship between the RIR and the IP address holder exists from the beginning. Organizations have to pay fees in exchange of the IP delegations. However, some IP address space was delegated before the establishment of RIRs and the distributed IP delegation system. These delegations are called *legacy* address space. This issue is particularly present in ARIN, as most of the legacy address space was delegated to US organizations, many of which in the field of education research and technology. Although no formal relationship exists between the holder of address space and ARIN for the legacy address space[1], the organizations have been able to use the address space for years without any agreement or service cost.

However, to issue RPKI records for that address space, ARIN requires of legacy address space holders to access *Full Registry Services*, for which organizations need to sign a Registry Service Agreement (RSA). Many organizations that hold legacy address space do not agree on the legal terms of the RSA, do not know that ARIN is open to negotiate the publicly available version of the RSA, or do not know how to start negotiating. According to the information publicly available from ARIN, there are still 12,382 organizations that have legacy address space and have not signed an RSA with ARIN. One participant describes a lengthy back and forth trying to get the agreement signed:

> *By signing the LRSA, the Legacy Registration Service Agreement, we give up certain rights or 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.*

Other participants in our study that had legacy resources in ARIN did not consider the legal aspect an issue for their legacy resources. One participant provided the following justification:

> *[The RSA] was not an issue for us. We already had contracts with [ARIN], so why would we not add these other the legacy [IP address blocks]? There was some hesitation at first, but our legal team just decided, why would we not? We already have contracts with them.*

Account access and administrative hurdles: Many organizations have lost the access to their ARIN account that would enable them to issue RPKI certificates. Organizations in this situation sometimes do not know how to recover their account, find it difficult to provide the requested documents or consider it a significant cost or burden. A participant who works closely with regional and smaller networks explained:

> *A fair number of [organizations] don't have access to their ARIN accounts, they have to recover the orgs (whoever was authorized to log into ARIN no longer works there) so they have to recover the organization so that's money and hassle (there's a fee to recover an org, it's not a lot but if it's a dollar that becomes a problem at a public [institution]).*

Poor record-keeping for IP allocations: Furthermore, for organizations holding large amount of address space, sometimes they do not have an exhaustive list of all the IP address blocks they

[1]Some organization have a mix of legacy address space and address space delegated by ARIN. In that case, some organizations decide to sign an agreement and get all the address space under ARIN, and some decide to treat the address space differently, not entering in agreement with ARIN for legacy address space and only pay membership fees for the address space directly delegated by ARIN.

have been delegated, which have been re-delegated, and thus may not be aware that they are lacking certificates for some of their address space. One participant described the difficult task of getting all the IP address blocks from his organization:

> *I'm trying to unravel all of the different pieces of IP space that we have. You know, where we're using things internally, and where we've delegated to customers. [It] has been a real challenge to sort all of those things out.And so what I've been doing a lot of is digging through our routing.*

Another participant recalled that the challenges of figuring out the details of IP allocations done many years ago made their adoption of RPKI slower:

> *[Most] of 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.*

4.1.2 What has worked

Despite significant hurdles in IP resource management, certain strategies and RIR initiatives have proven effective in facilitating RPKI adoption. This subsection highlights what has been helpful for organizations to streamline IP resource management and the process of issuing Route Origin Authorizations (ROAs).

Financial incentives for legacy agreements: In recent years, ARIN has negotiated with many organizations the term of the RSA, increasing significantly the number of legacy address space holders that are now members of ARIN. Multiple participants highlighted ARIN's decision in 2022 to create a financial incentive for organizations to sign their agreements for legacy IP space so that regardless of how many addresses an organization held, they would be charged a single flat fee of $200. One participant who conducted an outreach campaign to smaller networks in conjunction with ARIN's offer explained:

> *ARIN said if you get an agreement before the end of 2023 we'll let you keep the legacy fee structure, after that it goes away and you have to pay the regular prices. So we built a campaign: you'll eventually want this agreement, if you don't do it this year it's going to cost you a lot more and community-wide it's going to be a huge difference, and by the end of the year I compared some data with ARIN, and the rate people [we reached out to] got agreements was 20 times greater than the rate ARIN saw people adopting agreements for their legacy space.*

This model of partnering with RIRs to leverage their resources and information about which networks have up-to-date infrastructure and legal agreements is potentially replicable for other regions as well, though many of the legal obstacles are specific to ARIN and legacy space.

Address space from multiple RIRs: Given not all RIRs have the same approach about legacy address space and the requirements to get that address space in the IP management system, having address space from multiple RIRs can help issue ROAs when needed. As an example, one of the participants from an organization that had not signed the RSA with ARIN at the time of the interview, reported that if some customer was required to issue RPKI ROA certificates for their address space, they found a workaround using address space in other RIRs. They could allocate address space from small pools in RIPE or non-legacy address space in ARIN, both under RSA agreement and that can create ROAs:

> *Customer in [country]—the [local] government says if you want to bring IP space to play on a network operator [in this country] then you have to have a ROA for that IP space. I allocated them two IP blocks that are under the [RSA] agreement and I generated a ROA.*

Authoritative resource lists: For large organizations, having easy access to their list of resources and their RPKI status has been noted as a factor making RPKI adoption easier and faster. In large organizations, independent units may have different delegations of address space and no one unit has the full visibility of all the IP addresses of the organization. However, there is then one group leading RPKI adoption which lacks the full view of the IP address block of the organization, sometimes not even knowing which other groups in the organization have their own address space. One participant outlined their process to get the list of IP address blocks that are from their organization:

> *I [dig] through the published lists of resources. You know that you get from the delegations files from the RIRs and I've been using that as an authoritative list of the resources that are allocated to [us]. And 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.*

Having access to that list is also key for organizations that want to automate certificate issuance and management to more easily integrate ROA certificates in their operation. Indeed, as we will discuss later in section 4.3, many large organizations have internally developed tools to automate the creation and management of ROAs and only reach high levels of adoption once those tools are fully integrated in their operation.

4.2 Awareness and training

As with any technology adoption process, awareness and then training play a crucial role in the adoption process. However, in the case of RPKI deployment, the awareness and training efforts are not limited to the network or network security teams within organizations. For a successful adoption of RPKI, many other parts of the organization need to become aware of RPKI and its benefit, and even have some basic training to coordinate with customers and generally support the adoption.

4.2.1 The Challenges

Despite RPKI's critical role in securing routing and the increasing availability of RPKI awareness and training opportunities for the networking community, a significant and pervasive barrier to its widespread adoption is the lack of adequate awareness and training among organizations and their personnel. This subsection delves into the specific challenges encountered in educating diverse stakeholders about RPKI, its benefits, and its operational intricacies. These challenges range from reaching organizations that are completely unaware of RPKI's existence to the complexities of providing cross-team education within organizations and the inherent difficulty in demonstrating the tangible benefits of a security measure designed to prevent incidents.

Lack of awareness: Even with the increase adoption of RPKI, there remain many organizations that hold IP address space and are not aware of what RPKI is and how it works. Participants agreed that even ARIN's financial incentive during 2022-2023 on its own often was not sufficient to drive adoption, organizations need to be aware of what RPKI is and the benefits. Many of the organizations that should issue ROAs do not attend networking conference. The open questions is how to reach out to those organizations. One participant noted how this is not a new problem and explained:

> *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?*

Cross-team education: In addition, for many networks, the successful adoption of RPKI involves many teams or at least requires broader awareness and basic training by employees that are not part of the networking team. However, most communication raising awareness about RPKI and relevant training happens at networking conferences such as NANOG and RIPE meetings. For example, in one organization, the client-facing team knows the IP address blocks used by a client, and the networking team knows how those IP prefixes are routed (i.e., which ASNs of the organization are being used as the origin). Thus, to make sure that RPKI adoption would not cause any outage or disruption to customers, both teams needed to coordinate. However, only the networking team usually attended networking conferences such as NANOG and RIPE meetings, while the client-facing team was not even aware of RPKI or how it worked. Thus, the networking team had to educate and train the client-facing team so that they could work together and reach out to customers. Even some technical colleagues were not always well versed in the nuances of RPKI, some participants pointed out. One participant said, of enabling ROV:

> *Even turning on ROV I had to talk to people who were fairly technical because they didn't know the details of RPKI. That is a theme—that basic misunderstanding of unknowns. You might have someone who's really comfortable with BGP but they're unfamiliar with RPKI ... 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. I've had conversations with people responsible for the configuration of multihome networks who when they use the term 'origin AS' they don't know what it means.*

The role of individual champions: In these situations, several participants stressed, the work of educating and raising awareness about RPKI with relevant stakeholders fell largely to individual network engineers who were advocating for RPKI adoption and had personal relationships with the other parties whom they required buy-in from, except in cases where the RIRs stepped in to help promote adoption and raise awareness. One participant recalls the internal education efforts done at the beginning of the adoption journey:

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

And the same participant explained that once RPKI adoption started, the education effort continued for a long time:

> *I did all kinds of presentations about [RPKI]. Then there's a [company] learning portal and every time there was an opportunity, we were out there talking about it.*

Difficulty in proving RPKI's benefits: Many of the participants that had been educating others in their organization emphasized that it is hard to showcase the benefits of adopting RPKI. When RPKI works, BGP incidents are restrained and their visibility is limited, thus very few, if any, know that RPKI prevented a problem. A participant clarified this difficulty:

> *We're challenged in the RPKI space with proving the negative right? How many route leaks didn't happen because RPKI is in place.[...] And it's a hard question to answer.*

4.2.2 What has worked

Various strategies and external factors have proven successful in driving adoption and overcoming RPKI educational hurdles. This subsection highlights different channels and messages that have been effective in disseminating critical information about RPKI's relevance, benefits and operational procedures. These include the impact of highly visible routing security incidents, the influence of

regulatory attention, the role of industry-specific groups in targeted outreach, and the value of community knowledge sharing in fostering a more informed ecosystem.

High-profile security incidents: Several participants pointed to awareness and training efforts by RIRs and network operators groups to help raise awareness about the need to deploy RPKI. Many have attended talks and trainings from NANOG and RIPE. Other participants pointed to the value of specific routing security incidents to raise awareness with management about the need for routing security and motivate the allocation of resources for RPKI deployment. One participant explained:

> *We've had big hijacks in the past, this series of hijacks [...] impacted our customers in particular, so that got a lot of attention. That's how we got the buy-in for setting up this program [for RPKI adoption], we said we're going to fix routing security.*

Another participant recalled a route leak that happened when Cloudflare had already issued RPKI ROA certificates for their address space. Cloudflare had reported that RPKI was helpful in reducing the impact of the event, as networks had started doing Route Origin Validation (ROV).

> *There have been a number of really highly visible route leaks, one incident in particular, that one was really interesting, because the folks from Cloudflare, who had ROAs published at that point, on a lot of their prefixes, if not all of them. They were very much cheer-leading: "Hey, RPKI saved the day."*

Community knowledge sharing: Other participants mentioned that there were many presentations in networking conference of organizations starting to adopt RPKI. One participant that saw multiple of those presentations found that they presented different challenges in the adoption process.

> *There was a lot of [RPKI presentations], but it was okay, right. The community found it valuable. [...] And I think it's really interesting seeing the different presentations that are for different environments, right? Because you're speaking to a very, very different audience. So I do find it very interesting to go there and talk to a lot of people out there that have different challenges than I do.*

Regulatory interest: Meanwhile, others said that the U.S. government push for stronger routing security also played a major role in raising awareness with their leadership about RPKI because it was attracting regulatory attention. One participant noted:

> *The board didn't care [about RPKI] and if the FCC hadn't made a [notice of proposed rule making] about this, it wouldn't even have hit the board because there's no business impact of this.*

In other network operators, the FCC notice of inquiry (NOI) gave routing security priority within other security related topics being actively considered. One participant was tasked to interact with the policy team given the FCC NOI, confirming that routing security was being seen a priority in their organization:

> *There's a lot of security things that are being looked at by different organizations right now, and routing security is one of them. One of the other roles that I have is making sure our our policy [team] understand what we're doing and what we need, and how they should best respond to some of the things that come out of like the FCC. So I've participated in those working groups. [...] [Routing security] is definitely a priority. It's definitely on a lot of people's radar.*

Industry groups: Specific industry groups can play a significant role in reaching out to network and organizations that do not regularly attend the larges networking conferences such as NANOG.

A participant from a small network provider explained that CableLabs' recommendation to adopt RPKI was a motivation for pushing RPKI adoption in their network.

> *[We] participate in CableLabs. [...] And so, yeah, since we were doing that, it seemed like we should probably implement some of the things [CableLab's CREST working group] was recommending.*

CableLabs is a non-profit consortium of cable companies to support innovation, research and development in the cable industry. CableLabs has a working group on routing security, the Cable Routing Engineering for Security and Trust Working Group (CREST WG) which in January 2024 released a guide focusing on how to secure routing protocols and services using security practices including RPKI ROAs and ROV [3]. Other participants explained that they adopted RPKI in the process of adopting the Mutually Agreed Norms for Routing Security (MANRS) global initiative actions [1] to become MANRS-compliant. MANRS actions for Internet Service Providers (ISPs) do not require RPKI adoption but RPKI can be used to satisfy *Action 4: Facilitate routing information on a global scale* [14].

These dynamics highlight the interplay between RIRs, network operators, and policymakers in trying to drive adoption of security mechanisms like RPKI and the different, complementary roles each can play.

4.3 Tooling/software for ROA creation and monitoring

In addition to the challenges presented by raising awareness about RPKI, several participants also pointed to difficulties in evaluating the impact of issuing RPKI ROA certificates before they are in production. These tools fall into three different categories: resources for key/certificate generation, ROA creation tools, and support for monitoring ROAs and routes. Each RIR is left to figure out for itself how —- if at all —-it will support network operators with the RPKI deployment process through automated management and tools.

4.3.1 The Challenges

This subsection explores the specific challenges network operators face concerning the tooling and software required for Route Origin Authorization (ROA) creation and monitoring**. Despite the fact that RIRs are responsible for providing the infrastructure and means to issue RPKI certificates. However, for network operators to integrate ROA issuance in their operational procedures, additional steps and tools are required. The interview participants expressed their challenges with handling the currently significant manual effort required to issue ROAs, the distinct operation of each RIR, and concerns about the fragmentation and sustainability of current software tools. These issues highlight how the availability, usability, and consistency of RPKI-related software directly impact an organization's ability to efficiently secure the routing of its IP addresses.

Lack of tools: Several participants noted that especially early on in their RPKI deployment, there were not adequate tools to issue ROAs offered by the RIRs and they therefore had to devote considerable time and resources to building those tools in-house. For instance, one network operator said that when attempting to create some ROAs prior to ARIN developing an API, the process was exceedingly onerous. He explained:

> *For a while, ARIN didn't want to [provide tools for issuing ROAs]—this was an extra expense for them and an extra risk for them... I put in some new experimental ROAs a few years before [ARIN had] an API, instead they had this pretty difficult system, you had to issue yourself a private certificate, generate a key pair, upload the public key to them, sign a blob of data,*

upload it through their webpage and then they would validate it with the key so that you couldn't repudiate that you had done it. They didn't want anyone to say 'oh, I didn't make that ROA, you [ARIN] must have put it in.' [...] This was a big liability to them.

Significant manual effort: After the early years, RIRs began to develop tools to issue ROA certificates within their system, instead of having network operators issue the cryptographic certificates themselves. Most RIRs enable ROA issuance through their portal or via an API that could be used to automate certificate issuance. However, even with those tools, there still is a significant amount work required of operators to interface with those tools and issue the certificates. A participant explained:

ARIN has an API but we don't have someone to maintain any code that would touch that API so almost everything is manual but includes running a script ... to create ROAs and interface with the ARIN API.

Maintenance concerns: Another participant explained that when confronted with the need to develop tools to be able to monitor ROAs and make sure to issue new ones before their expiration date[2], it initially made their RPKI adoption process more challenging. This network operator explained:

A big concern I had when we first created ROAs was refreshing them because it was on the end user to make sure that your ROAs didn't expire, [...] similar to not having your certificate on a your website expire. Don't have your ROA expire. [...] I was quite worried about, because I definitely would need all robust automation for that and didn't have it.

At the time of our interviews though, in most RIRs ROAs are automatically updated so that type of monitoring is not needed.

Lack of standardization across RIRs: In addition, given each RIR implemented their RPKI infrastructure independently, several participants from larger operators noted the lack of standardization across different RIRs in this domain. For instance, one said:

We did start registering routes—but we ran into the problem of lack of common APIs across the RIRs. We thought briefly about whether we should use [the delegated RPKI model] ourselves, but we decided to stick with RIRs.

Another participant made it clear that there is additional burden when working with different system across RIRs, requiring them to develop tools in-house to handle address space in all RIRs:

We have space from all the RIRs. So [we need] something internal.

Unsustainable tooling ecosystem: In general, most participants communicated that there is a lack of tools to support deployment and operation of RPKI. One of the participants declared it was the biggest barrier they has

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.

Some participants felt that the lack of widely available and stable software for the different parts of RPKI made it seem less sustainable. One of them explained:

[2]Just like other cryptographic certificates, ROA have an expiration date. Certificates have expiration dates to enforce regular security updates and protect users from vulnerabilities.

A related, non-technical thing that I worry that there isn't enough validator software, and there isn't enough money going to people who write the code. [...] It's something I worry about in the ecosystem in general. [Some] write [their] own code, but maybe they'll get bored. How sustainable is it? We've seen the RIPE validator go away. FORT [validator] has come and gone and I know there's a couple others. But it's not as robust as the DNS system, where we have a lot of open source.

Mismatch with IP delegation practices: Several participants noted specific tools or features they would like to see RIRs create to make the process of issuing ROAs even easier, including automatically creating a way to delegate a ROA as part of the process to sub-delegate a prefix. One participant noted:

So today in ARIN, when I delegate a prefix, the customer .... the recipient of that prefix, can publish IRR for that prefix right in ARIN's authoritative IRR [Internet Routing Registry] because it's been delegated. Why can't they do that for ROAs? Why can't a reassignment also include a delegated RPKI? There's no reason that it shouldn't, right?

4.3.2 What has worked

This subsection highlights the software tools and approaches that supported organizations adoption of RPKI by improving the efficiency and usability of the infrastructure and enabling safe deployment.

Tooling to support ROA issuance: Overall, participants agreed that the RIRs had improved their offerings of tools and software for ROA creation, but that there was more work still to be done to make the tools even more useful and user friendly for network operators. The resources for key and certificate generation now fall within the RIR resource management system, a change which has been enormously beneficial in driving RPKI adoption. One participant explained:

By 2019 ... [ARIN] had an API, and I couldn't have [deployed RPKI] without the API.

Other participants also highlighted how much ARIN's APIs and user interface for RPKI have improved over the past several years and become significantly more user-friendly, enabling much easier RPKI deployment. In general, there was consensus that the RIRs were assuming an increasingly large responsibility for creating and improving these tools, though there was also interest in whether there could be more standardization of these tools and processes across RIRs, especially for verifying that ROAs are indeed deployed and testing what routes would be invalid given a new ROA.

Publicly available third-party tools: One participant alluded to the use of Cloudflare's RPKI validator data to find out if the validated ROA payload of a given ROA shows up, which they wouldn't have found out otherwise.

One is adding roas, and they're not showing up in Cloudflare validator. And I haven't figured out yet what's going on. I don't know how many others [public RPKI validators] are there, but I was trying to validate that these changes had showed up. And they're not for some reason. And I that is what I still have to troubleshoot. It's nice to be able to see like, what are my ROAs? Because I put it in [the ARIN portal]. But like, is it actually getting out? There are other people seeing it, that is the kind of the thing I want to be able to validate. Ripe has one [validator].

RIPE's leadership in software development: Most participants agreed that RIPE has been ahead of the curve in software development, and that their interface to create and tools to monitor ROAs and RPKI more broadly are very helpful. A participant when describing useful tools to support RPKI adoption mentioned two additional tools developed by RIPE:

RIPE has an an interface where you can look up the history of ROAs. And also, you can see when somebody created a ROA.

Testing environments: Furthermore, participants mentioned the need of trial period for Route Origin Validation, (ROV), enabling experimental testing of ROV with dedicated routers to test the ROV configuration. Many participant first study the impact of doing ROV on customers' routes before deploying ROV. A participant explained their process:

We did our analysis of which customers were sending us invalid routes. We were on the phone with those customers and the sales organization to help those customers fix their routes.

Another participant clarified that their organization tested ROV in an internal hardware testbed:

we have a test lab of of hardware, [...] that is, it does not carry customer traffic. But it's, you know, in our one of our facilities, and it's connected to the network, it can get to the Internet, so it can be fed from validators.

Third-party RPKI software: Participants also pointed to the fact that other, non-RIR, tools have emerged to help with RPKI deployment. However, many of those tools are in a precarious position with respect to funding and support. One said of validator software:

There's 2 or 3 viable open source-maintained implementations of [validator software] and none of them really have a sustainable business model. Two of them you can either get a support contract funding them or charitable contributions, but the fact that that is an important part of the ecosystem that has no sustainable business models is concerning.

The answers from the participants highlight how critical are many software tools to the adoption of RPKI. RIRs have developed many tools supporting ROA issuance but not all RIRs offer the same tools.

4.4 Tooling for routing monitoring and incident investigation

The ultimate goal of RPKI is to provide networks with records of authoritative routing data that can be cryptographically validated to dynamically verify routing information in BGP. As a consequence, RPKI certificates impact what is routed. Therefore, having access to routing data is crucial to align RPKI records with the desired routing of IP address blocks and debug when mistakes and misconfigurations happen.

4.4.1 The Challenges

All of the participants we interviewed had at some point or another monitored the routes for which they or their customers had issue ROAs. RPKI's ultimate purpose is to provide cryptographically validated routing information to filter out invalid routing information. Therefore, the direct consequence is that RPKI ROA certificates significantly influence what routes are considered valid and subsequently routed. Hence, comprehensive access to routing data becomes paramount for aligning RPKI records with intended routing behaviors and effectively debugging any misconfigurations or unforeseen changes. Many of the interview participants from large network providers had developed in-house monitoring solutions so that they could always have access to the status of their routing and RPKI objects, and even build alert systems on top of that. Other participants used a mix of paid and free tools for monitoring routing and RPKI. In addition, many participants mentioned that their need for monitoring tools has evolved as the RIRs have improved their system and as

they have become more familiar with RPKI. These difficulties underscore how the absence of robust and accessible monitoring tools can substantially impede RPKI adoption, as operators require extensive analysis and assurances to prevent service disruptions.

Fear of connectivity outages: The lack of monitoring tools may delay the adoption of RPKI because network operators or their customers may be afraid that ROAs or ROV may make routes unavailable by mistake or configuration problems. Most network operators before adopting RPKI study the impact it would have for them and their customers. Without tools that monitor routing and RPKI the analysis can take time and delay RPKI adoption. One participant stated that doing the analysis to demonstrate RPKI ROA will not cause issues in their network was the biggest barrier to adopt ROAs:

> *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. We also needed some automation to make that happen.*

Making changes visible: More broadly, participants agreed on the need for tooling that proactively alerts networks about status changes. Otherwise changes can go unnoticed for long periods of time, impacting traffic. Participants thought it would be helpful to have RIRs assist with BGP data collection to support external visibility of BGP and router configurations, as well as to learn what is originated by their own ASes in large organizations, as mentioned in section 4.1.1.

4.4.2 What has worked

This subsection focuses on tools that have proven effective in helping network operators gain visibility into their routing configurations, debug issues, and respond to incidents, ensuring the correct routing of their RPKI-covered prefixes. These methods are crucial for aligning RPKI records with desired routing behaviors and for swiftly addressing any misconfigurations that may arise and thus support RPKI adoption.

Access to global BGP data: To track RPKI adoption and its impact on routing, specially in large networks, BGP collectors platforms such as Routeviews and RIPE RIS, enable operators to have an external point of view of what is being routed by their network. Many participants mentioned the use of data from BGP collectors to find out the IP address blocks that are originated and transited by their networks.

BGP incident observatory: Some participants pointed to the MANRS Observatory as a helpful resource for near incidents and incident detection, suggesting that it might be helpful for the industry to expand on this model since it had proven useful in helping them figure out what went wrong and how to potentially prevent the next incident.

Commercial monitoring platforms: Some operators use proprietary tools such as the ones offered by Kentik, Cloudflare and BGPtools that are also based on BGP data and pair it with additional data such as traffic and RPKI status. One participant described that they had used the Kentik platform to monitor the traffic flows of their network that went towards invalid routes.

> *So in Kentik, the netflow tool, one thing you can do is it can marry the flows against RPKI status. So you can see, you know, given their view of the validators. [...] your flows to what routes were invalid.*

Another participant uses the feature from BGPtools that sends alerts when data relevant to their IP block changes:

> *BGP tools is wonderful. [...] So if you take a prefix [it] will show you all of this [data]. I also get alerts from it if something changes.*

RIPE Routing Information Service: RIPE provides a robust suite of BGP monitoring tools that have proven instrumental for network operators in debugging specific issues and ensuring their RPKI-covered routes are handled as expected. RIPE RIS (Routing Information Service) serves as a key BGP collector platform, allowing operators to gain an external perspective of what their network is routing. RIPE RIS capabilities include an interface to quickly check the ROA status of routed prefixes and a longitudinal view of the visibility of routed prefixes. Such tools are critical for identifying all the IP prefixes an organization is originating and transiting, and many participants used them to make sure RPKI records align with desired routing configurations and swiftly address any misconfigurations, thereby facilitating greater confidence and accelerating RPKI adoption.

5 Recommendations to increase RPKI adoption

Overall, our findings about the different challenges and potential solutions organizations face in trying to adopt RPKI point to some broad recommendations for RIRs and policymakers. These include developing robust, user friendly tools for both ROA creation and routing monitoring/incident investigation, as well as coordinating with industry stakeholders on education efforts, awareness campaigns, and IP resource management. In this section we consider how some of these efforts might affect lagging organizations which are known to be behind their peers in RPKI adoption rates.

5.1 Difference by regions/RIRs

Measurements studies of RPKI adoption have consistently found that RIPE's region has been driving RPKI adoption for the last decade. From our interviews, it appears that RIPE has fully embraced RPKI, making it a priority to make it work for network operators in their region. The network operators we interviewed agreed that RIPE is the Regional Internet Registry with the most user-friendly interface, the easier integration with IP resources management and the most tools to support analysis, monitoring and automation. RIPE appears to be ahead of the curve in terms of software development to support RPKI and routing operation. RIPE's meetings are also frequently mentioned as source of RPKI awareness and training.

Other RIRs can look at the big success of RIPE and replicate or leverage some of the tools to better support RPKI adoption of network operators in their region. Just as RIRs play a vital role in creating and improving tools for Route Origin Authorization (ROA) creation and management, they are equally positioned to assist with the development of software and reporting tools for routing monitoring and incident investigations. These tools are critical for network operators to debug issues with routing, a task that now inherently includes considerations for RPKI certificates and their impact. The absence of adequate monitoring tools can delay RPKI adoption, as operators require extensive analysis to confirm that issuing ROAs or performing Route Origin Validation (ROV) will not cause unintended service disruptions. While operators currently leverage public BGP collector platforms like RouteViews and RIPE RIS, as well as commercial monitoring solutions from vendors like Kentik and Cloudflare, RIRs are well-positioned to develop and provide integrated software that can proactively alert networks to status changes and enhance overall BGP visibility. Such robust RIR-provided monitoring capabilities are essential to align RPKI records with desired routing configurations and to swiftly address any misconfigurations, thereby fostering greater confidence and accelerating RPKI adoption across the internet.

Last year, the Number Resource Organization (NRO), which is the coordinating body for the five RIRs, started the NRO RPKI Program [2] to " work toward providing a robust, coordinated

and secure RPKI service". Hopefully through this program all RIRs will be able to catch up with RIPE and better support RPKI adoption by holders of address space.

5.2 Small organizations

Our previous research found out that small and medium sized organizations are lagging behind in RPKI adoption when compared with large network providers. Through the RPKI adoption journey of the network operators we interviewed, we can see how adopting RPKI is not that simple. There could be much effort and many step taken to issue that first ROA certificate and then in addition the worry that it might break connectivity. As such, awareness, training and tooling for RPKI and ROA issuance are critical to support RPKI adoption in smaller organizations.

There is a highest likelihood when compared to large network providers that small organizations are not aware of RPKI or do not have trained employees to adopt RPKI. These issue were recognized by many of our participants, whether they worked at large network providers or smaller organizations. Small organizations might not participate in the large network operators' conferences, which are the main reference for awareness and training. However, these smaller organizations may be part of other, more specific industry groups which may be good channels to reach out to many smaller organizations at the same time. As mentioned in section 4.2.2, a participant from a small network provider related how his organization participation in CableLabs had created enough awareness of RPKI and its benefits to support the decision of adopting RPKI.

Moreover, smaller organization are less likely to be able to either pay for proprietary tools or develop in-house tools to test, understand and monitor RPKI impact in their operation. Nonetheless, those tools are needed to define the ROAs that need to be created for each routes, even for small organizations the ROAs might not be straighforward. Indeed, there are many non-obvious dependencies in routing that can be impacted by the creation of a ROA. One participant recalled how a small organization by issuing a ROA for their routes without coordinating with the regional network that provided them connectivity to the broader Internet broke the Denial of Service (DoS) Protection System for the now ROA-covered routes. In that case, the issuance of the ROAs triggered the deletion of a critical piece of routing information in another routing database the DoS protection service relied upon.

5.3 Non-ISP organizations

Similar to small organizations, previous research has revealed that many non-ISP organizations such as enterprises, schools, hospitals, utility companies are lagging in RPKI adoption. Many such organizations hold address space and hence are the ones that need to issue ROA certificates to adopt RPKI. Thus, similar to small organizations in general, awareness, training and then also access to tooling for ROA planning are needed to support the RPKI adoption in these organizations.

Given non-ISP organizations even if they hold significant address space are far away from the networking field, awareness and training are challenging for the networking teams at those organizations. Unfortunately, routing security is not explicitly part of any cybersecurity certification such as the ISO 27000 family of cybersecurity standards. Thus, unless an organization has exposure to routing security initiative such as the Mutually Agreed Norms for Routing Security (MANRS) inciative or through industry-specific group, they may not be aware of how routing may impact the security of their online activities. Targeted communication through industry or sector-specific initiatives such as the White House ONCD [17] Roadmap which encourages US federal agencies to implement routing security in their procurement and train personnel are essential to reach to the non-ISP organization that should protect their address space with RPKI.

In addition, even when non-ISP organizations have address space and they need to adopt RPKI themselves, network operators provide connectivity to those organizations. As such, network operators can have a role in making those organization aware of RPKI and supporting their RPKI adoption process. In MANRS, one of the actions required from network operators referred as *Know Your Customer (KYC)* is to verify that their customers have legitimate rights to announce the IP addresses and Autonomous System Numbers (ASNs) they are using. RPKI provides a mechanism to check the IP addresses and network providers could benefit of automating the checking benefit if their customers use RPKI.

5.4 Complex IP delegation

In our previous study we found that address space that had multiple layers of delegation and sub-delegations involving different organizations was lagging behind in RPKI adoption. For address space in this categories, the link between RPKI and IP management is crucial. Therefore, reducing the barrier of integrating RPKI management with IP management will support RPKI adoption for this address space.

Most of this address space was delegated long time ago and as such documentation of delegation might be scarce. Providing an easy access to large organization to all the resources delegated to them will support RPKI adoption of those organizations. In adition, part of this space is legacy address space in the ARIN region. Hence, reducing the barriers for that space to be in the IP management system that provides access to RPKI infrastructure will support RPKI adoption. Finally, given the layering of sub-delegations in this address space, RIR could consider providing the ability for sub-delegations to issue ROAs if authorized by the direct holder of IP address space. Other parts of the RIR systems provide the ability to delegate routing record management to organizations that have the sub-delegation, but currently that is not possible with RPKI ROAs. Many participants agreed that providing this functionality will simplify the coordination process between organizations to issue ROAs.

6 Conclusions

This paper explores the critical role of Regional Internet Registries (RIRs) in facilitating the adoption of the Resource Public Key Infrastructure (RPKI) framework. Through in-depth interviews with 11 network security specialists, this study identifies the primary challenges and successes organizations encounter when issuing Route Origin Authorizations (ROAs) to secure their IP address blocks. While RPKI is recognized as the consensus solution for improving inter-domain routing security, its adoption is hampered by significant socio-technical barriers, including legal, organizational, and resource-related challenges.

Our findings highlight that RIRs are inextricably linked to the RPKI adoption process, serving as cryptographic roots of trust and providing the essential infrastructure for managing certificates. The independent development of this infrastructure by each RIR has led to disparities in tools, processes, and legal requirements, creating an inconsistent experience for network operators, especially those managing resources across multiple regions. Successful adoption efforts have often been driven by a combination of factors. Financial incentives from RIRs, highly visible routing security incidents, and regulatory attention from bodies like the U.S. government have all served as powerful motivators for organizations to prioritize RPKI. Furthermore, industry-specific groups like CableLabs play a vital role in reaching smaller or non-ISP organizations that may not attend major networking conferences.

To accelerate RPKI adoption, especially among lagging organizations such as small businesses, non-ISPs, and those with complex IP delegations, our findings point to several recommendations for RIRs and policymakers. RIRs should continue to develop robust, user-friendly, and standardized tools for ROA management and routing monitoring. Efforts like the NRO RPKI Program are promising steps toward harmonizing services across all RIRs. Coordinating on targeted awareness campaigns and simplifying legal and administrative hurdles for legacy address space holders are also crucial. RIRs have a pivotal role in RPKI adoption and by learning from successful strategies, RIRs can significantly lower the barriers to entry, enabling a more secure and resilient global routing ecosystem for all organizations.

Acknowledgments

This work is based on research sponsored by U.S. NSF grant OAC-2419735. The views and conclusions are those of the authors and do not necessarily represent endorsements, either expressed or implied, of NSF.

References

[1] Mutually Agreed Norms for Routing Security (MANRS). https://manrs.org/.

[2] Number Resource Organization (NRO) RPKI Program. https://www.nro.net/technical-coordination/nro-rpki-program/, 2024.

[3] CableLabs. Cybersecurity Framework Profile for Internet Routing. https://www.cablelabs.com/specifications/CL-GL-RS-Profile, January 2024.

[4] Chung, T., Aben, E., Bruijnzeels, T., Chandrasekaran, B., Choffnes, D., Levin, D., Maggs, B. M., Mislove, A., Rijswijk-Deij, R. v., Rula, J., and Sullivan, N. RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins. In *Proceedings of the Internet Measurement Conference* (Amsterdam, Netherlands, Oct. 2019), IMC '19, Association for Computing Machinery, pp. 406–419.

[5] Cloudflare. Is BGP safe yet? https://isbgpsafeyet.com/.

[6] Forum Standaardisatie. Secured internet routing of Dutch government by end of 2024. https://www.forumstandaardisatie.nl/nieuws/secured-internet-routing-dutch-government-end-2024, 2023.

[7] Gilad, Y., Cohen, A., Herzberg, A., Schapira, M., and Shulman, H. Are We There Yet? On RPKI's Deployment and Security. In *Proceedings 2017 Network and Distributed System Security Symposium* (San Diego, CA, 2017), Internet Society.

[8] Gilad, Y., Sagga, O., and Goldberg, S. MaxLength Considered Harmful to the RPKI. In *Proceedings of the 13th International Conference on Emerging Networking EXperiments and Technologies* (New York, NY, USA, 2017), CoNEXT '17, ACM, pp. 101–107. event-place: Incheon, Republic of Korea.

[9] Hlavacek, T., Jeitner, P., Mirdita, D., Shulman, H., and Waidner, M. Behind the Scenes of RPKI. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (New York, NY, USA, Nov. 2022), CCS '22, Association for Computing Machinery, pp. 1413–1426.

[10] Iamartino, D., Pelsser, C., and Bush, R. Measuring BGP Route Origin Registration and Validation. In *Passive and Active Measurement* (Cham, 2015), J. Mirkovic and Y. Liu, Eds., Lecture Notes in Computer Science, Springer International Publishing, pp. 28–40.

[11] Li, Y., Zou, H., Chen, Y., Xu, Y., Ma, Z., Ma, D., Hu, Y., and Xie, G. The Hanging ROA: A Secure and Scalable Encoding Scheme for Route Origin Authorization. In *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications* (London, United Kingdom, May 2022), IEEE Press, pp. 21–30.

[12] Madory, D. A Tale of Two BGP Leaks. https://www.kentik.com/blog/a-tale-of-two-bgp-leaks/, August 2023.

[13] MANRS. RPKI Week. https://manrs.org/resources/events/rpki-week/, year=2021.

[14] MANRS. MANRS Actions for Network Operators. https://manrs.org/wp-content/uploads/2021/09/MANRS-Network-Operators-Actions-v2.5.2.pdf, 2021.

[15] Oliver, L., Akiwate, G., Luckie, M., Du, B., and claffy, k. Stop, DROP, and ROA: effectiveness of defenses through the lens of DROP. In *Proceedings of the 22nd ACM Internet Measurement Conference* (New York, NY, USA, Oct. 2022), IMC '22, Association for Computing Machinery, pp. 730–737.

[16] Rosenworcel, J. FCC Chairwoman Proposes Internet Routing Security Reporting Requirements. `https://docs.fcc.gov/public/attachments/DOC-402579A1.pdf`, 2024.

[17] White House. National Cybersecurity Strategy Implementation Plan. `https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf`, 2023.

[18] Wählisch, M., Maennel, O., and Schmidt, T. C. Towards detecting BGP route hijacking using the RPKI. *ACM SIGCOMM Computer Communication Review 42*, 4 (Aug. 2012), 103–104.

[19] Wählisch, M., Schmidt, R., Schmidt, T. C., Maennel, O., Uhlig, S., and Tyson, G. RiPKI: The Tragic Story of RPKI Deployment in the Web Ecosystem. In *Proceedings of the 14th ACM Workshop on Hot Topics in Networks* (New York, NY, USA, Nov. 2015), HotNets-XIV, Association for Computing Machinery, pp. 1–7.

[20] Yoo, C. S., and Wishnick, D. Lowering Legal Barriers to RPKI Adoption. *SSRN Electronic Journal* (2019).