ru-RPKI-ready: the Road Left to Full ROA Adoption

Deepak Gouda
deepakgouda@gatech.edu
Georgia Institute of Technology
Atlanta, USA

Romain Fontugne
romain@iij.ad.jp
IIJ Research Laboratory
Tokyo, Japan

Cecilia Testart
ctestart@gatech.edu
Georgia Institute of Technology
Atlanta, USA

Abstract

Resource Public Key Infrastructure (RPKI) has emerged as a standard for enhancing the security of Internet routing. Currently, more than 50% BGP prefixes are covered by RPKI Route Origin Authorizations (ROAs), enabling networks to validate the origin of prefix advertisements in BGP. Despite this progress, ROA adoption remains non-uniform, with key stakeholders encountering significant barriers in the adoption process. In this paper, we combine a product adoption framework with data-driven analysis of global RPKI adoption to identify persistent disparities and pinpoint the stages of the adoption process that hinder broader growth. Our study reveals that, although RPKI awareness has grown, the complexity of planning and deploying ROAs remains a significant challenge. Since no unified workflow and documentation exist for ROA planning, many organizations are left without clear operational guidance. To address this challenge, we propose a systematic framework for ROA planning and introduce `ru-RPKI-ready`, a platform designed to provide data and insights to facilitate ROA planning. Using `ru-RPKI-ready`, we characterize the routed address space not covered by RPKI ROAs. We find that 47% IPv4 and 71% IPv6 prefixes not in RPKI could be covered with minimal technical effort. Our analysis also reveals that if as few as ten organizations were to take the necessary actions, the global ROA coverage could increase by 7% for IPv4 and 19% for IPv6.

CCS Concepts

• **Networks** → **Network measurement**; **Network security**.

Keywords

Product Adoption Process, Routing Security, RPKI, ROA Planning

ACM Reference Format:
Deepak Gouda, Romain Fontugne, and Cecilia Testart. 2025. `ru-RPKI-ready`: the Road Left to Full ROA Adoption. In *Proceedings of the 2025 ACM Internet Measurement Conference (IMC '25), October 28–31, 2025, Madison, WI, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3730567.3764452

1 Introduction

Society increasingly relies on the Internet as a critical infrastructure, and the Internet relies on inter-domain routing for transmitting information globally across independent networks. Unfortunately, the Border Gateway Protocol (BGP), the *de facto* routing protocol of the Internet, is vulnerable to attacks and misconfigurations as it lacks a built-in mechanism for validating the information networks share and use to select global routes for data traffic. This is a major security problem potentially allowing for surveillance, loss of traffic, or other forms of interference [19, 30, 31, 42, 45]. Furthermore, attackers have leveraged this vulnerability to steal cryptocurrencies and fake traffic on multiple occasions over the past years [16, 17, 29, 51].

The Internet Engineering Task Force (IETF) has worked to standardize additional protocols to secure BGP. In 2012, the IETF standardized the Resource Public Key Infrastructure (RPKI), a framework that provides a mechanism for networks to issue cryptographic records that can then be used to validate data in BGP messages. The Regional Internet Registries (RIRs) are the *trust anchors* of this specialized PKI, providing to organizations the certificates allowing them to issue records for their allocated resources. Holders of address space can issue Route Origin Authorizations (ROAs)—cryptographic records that authorize Autonomous System Numbers (ASNs) to originate IP address blocks in BGP.

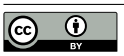
Networks can cryptographically validate ROAs and use that data to verify the origin of incoming BGP advertisements. Indeed most Tier-1 and large transit providers verify the information in BGP, effectively dropping route announcements invalid with respect to ROAs. The RPKI and ROAs thus provide a trustworthy route origin database, a crucial building block for improving BGP security.

Despite the clear security benefits RPKI and ROAs provide by limiting the spread of routing incidents and attacks [30, 59], many networks have yet to fully adopt RPKI. In March 2024, the US Federal Communications Commission (FCC) released a proposal highlighting the importance of RPKI adoption in securing the routing infrastructure [50]. Even with the policy advisory, the adoption of RPKI is not universal [46, 60]. While about half of the routed prefixes are not covered by RPKI ROAs (Figure 1), we currently lack a broad understanding of the current state of where we stand in the adoption of RPKI, what specific barriers are preventing networks from issuing RPKI records, and how to best support RPKI adoption.

In this paper, we examine the current state of RPKI adoption, the adoption process for an organization, and the reasons preventing organizations from engaging in RPKI. We also provide practical guidance and tools to help organizations adopt RPKI and analyze the steps required to address the half of the routed prefixes not covered by ROAs.

Our key contributions are:

- We frame RPKI adoption through the lens of technology and product adoption processes to better understand the different perspectives of organizations engaging with RPKI and the various stages they encounter during this adoption journey.
- With our understanding of the product adoption process, we highlight two critical gaps organizations face during the RPKI



IMC '25, Madison, WI, USA

ACM ISBN 979-8-4007-1860-1/2025/10
https://doi.org/10.1145/3730567.3764452

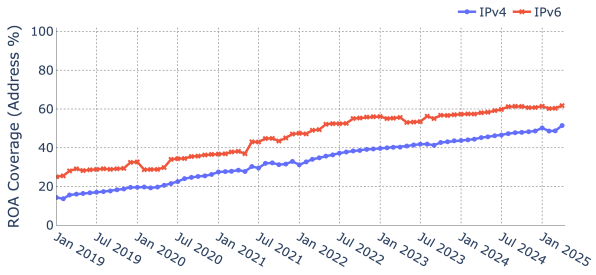


Figure 1: The percentage of routed address space covered by ROAs has witnessed a 2.5×-3× growth since 2019

adoption process–*(i)* lack of a recommended ROA planning pipeline, *(ii)* necessary data and guidance during the planning.
- We collect feedback from multiple network operators and RIRs to create a structured guide on planning ROAs, along with `ru-RPKI-ready`, to help network operators make informed decisions when issuing ROAs.
- We characterize the address space currently not covered by ROAs and discover that a significant proportion of prefixes not yet covered by ROAs—nearly half in IPv4 and over 70% in IPv6—could be secured with minimal technical effort if organizations were to take action.

Our data is available at https://doi.org/10.5281/zenodo.17237911. The ROA planning platform and the code to generate the data are accessible at https://github.com/ISS-GT/ru-RPKI-ready-Code.

2 Background and Related Work

In this section, we discuss various aspects of RPKI adoption and prior studies related to this topic. We also provide a table of terminologies used throughout the paper and outline a roadmap for the remaining sections.

2.1 RPKI

RPKI is designed to secure routing by providing an off-band, cryptographically verifiable system for validating BGP information. Currently, RPKI is mainly used to manage cryptographic records asserting which network is authorized to announce prefixes in BGP, and requires two key actions to be effective:

(1) Holders of address space must issue Route Origin Authorizations (ROAs) specifying which ASNs are authorized to originate the prefixes in BGP;
(2) Networks must use ROAs to validate information from BGP advertisements, filtering invalid messages, and effectively preventing the spread of invalid information. This step is referred to as Route Origin Validation (ROV).

In addition, ROA issuance requires RIR members to activate RPKI in their respective RIR portals. This activation creates a Resource Certificate (defined in Table 1) for the allocated space, which is needed to cryptographically sign ROAs.

While both the registration of ROAs and the deployment of ROV are essential to realize the benefits of RPKI, this paper primarily focuses on ROA adoption. Over the past six years, the percentage of address space covered by ROAs has increased dramatically (Figure 1). The routing community has shown massive support and is in consensus regarding the security benefits of adopting RPKI. The implementation of ROV has further bolstered the benefits of RPKI by limiting the propagation of *RPKI-Invalid* prefixes, thus containing the impacts of BGP misconfigurations and hijack attempts [33, 34].

Recognizing these benefits, policymakers and governments are increasingly mandating RPKI adoption as a part of the broader routing security strategies [50, 56]. The Regional Internet Registries (RIRs), together with community initiatives like MANRS[1], have played an important role in driving awareness and supporting the adoption of RPKI [3, 24, 35, 36, 58, 66]. Despite this momentum, a significant number of organizations, including several critical ones, remain unengaged with RPKI.

This persistent gap raises fundamental questions: Why are so many organizations still not adopting RPKI, and what are the barriers preventing them from participating in RPKI? To answer these questions, it is necessary to take a broader view of the adoption landscape, considering not only the current state of RPKI deployment but also the specific steps and challenges organizations face throughout the adoption process. In this work, we utilize established frameworks from Product and Innovation Management to analyze the adoption of RPKI in detail. These frameworks help us understand the lifecycle of a new product, from its conception and development to its eventual adoption among the wider masses. By adopting this perspective, we can identify the areas where organizations encounter obstacles and suggest actions that may enhance their engagement with RPKI. We further discuss these frameworks and their relevance to RPKI in §3. In Table 1, we provide a list of terms and their definitions that will be used throughout the paper.

2.2 Related Work

Several studies have investigated the coverage and operational characteristics of ROAs in the global IP address space [7, 13, 15, 20, 21, 27, 44, 60, 62, 63]. Some of these works have studied ROA coverage as an initial step to analyze the impact of ROV [21] in routing and to detect BGP hijacking [62]. Other works have focused on specific aspects of ROA management, such as identifying ROA configuration errors and operational problems [12, 15, 20], evaluating the computational cost of ROA validation [27], and the potential impact of AS0 as origin in a ROA to limit the exploitation of unused address space [44].

Equally relevant, other works have examined the broader implementation and adoption of the the full RPKI framework–including both ROAs and ROV–with the goal of evaluating its effectiveness in improving overall routing security [7, 13]. In 2015, Wahlisch *et al.* measured ROA coverage of popular web servers [63] and emphasized the need for a deeper understanding of the low RPKI adoption rates in these critical address spaces. They find that ROA adoption is inversely proportional to website popularity, largely because CDNs were not issuing ROAs for their address space. The authors suggest that some operators may not want to reveal the resources they manage and, hence, choose not to issue ROAs.

[1] Mutually Agreed Norms for Routing Security (MANRS) is a global initiative promoting industry best practices to enhance BGP routing security by encouraging the adoption of technical and operational measures, including RPKI deployment.

Terminology	Description
Resource Certificate (RC)	Cryptographic certificates in the RPKI framework that attest to the certificate holder's right to use specific Internet resources such as ASNs and IP addresses
Route Origin Authorization (ROA)	An RPKI certificate signed by an RC specifying which ASN is authorized to originate one or more prefixes in BGP
Direct Owner	Organizations receiving address space allocations directly from an RIR
Delegated Customer	Organizations receiving a reallocated address space from the Direct Owners
MOAS Prefix	Multi-Origin AS prefix, a prefix originated from multiple distinct ASNs
Leaf Prefix	A prefix with no routed sub-prefix
Organizational-Awareness	An organization is considered aware of the RPKI system, if at least one of its prefixes covered by a ROA in the past 12 months (*RPKI-Aware* organization)
RPKI-Ready Prefixes	Prefixes covered by an RC, are Leaf, and not reassigned to a Delegated Customer
Low-Hanging Prefixes	RPKI-Ready Prefixes owned by RPKI-Aware organizations
(Non) RPKI-Activated Prefixes	Prefixes (not) exclusively present in the RCs owned by RIRs

Table 1: Definitions and terminologies used in the paper

The first comprehensive longitudinal study of RPKI adoption was conducted by Chung et al. [7] in 2019, who concluded that RPKI was "ready for the big screen." Since then, the RPKI ecosystem has evolved, and its adoption has increased manyfold. In particular, changes in regulatory requirements for issuing ROAs for legacy prefixes in ARIN [8, 26], along with significant improvements to the tools and infrastructure provided by the RIRs for ROA management [1, 18, 57, 61], have played a crucial role in raising awareness and accelerating adoption across the Internet. More recently, Testart et al. [60] performed longitudinal analyses, focusing on the identification of barriers that continue to impede broader RPKI deployment. In this paper, we build upon the previous work by providing an updated longitudinal perspective on the current state of RPKI adoption, with a particular emphasis on prefixes that remain uncovered by ROAs. Our analysis leverages frameworks from technology and product adoption research, enabling us to systematically identify not only the barriers that hinder RPKI adoption, but also to pinpoint the specific stages in the adoption process where organizations are most likely to encounter these obstacles. By developing a more nuanced understanding of the sequence and nature of these barriers, we aim to provide actionable recommendations and to estimate the concrete steps and efforts required to extend RPKI coverage to prefixes currently not covered by ROAs.

2.3 Roadmap

The rest of the paper is organized as follows. In §3, we present the technology adoption lifecycle and product adoption process to provide a framing on how we study RPKI adoption in the rest of the paper. §4 examines the current state of RPKI adoption and explores the barriers organizations face, using these adoption models as a lens. In §5, we present practical solutions–a systematic framework and publicly available dataset with a search tool interface –to address key challenges in RPKI adoption. In §6, we use our platform to analyze prefixes not yet covered by ROAs and provide a foresight into the efforts needed to engage these prefixes in the RPKI ecosystem. Finally, §7 discusses the limitations of our approach, potential improvements, and the broader impact of our platform on routing security.

3 Primer on Technology Adoption

In this section, we outline the frameworks utilized to analyze the adoption of technology within an ecosystem, as well as the various steps an organization undergoes when adopting a new product. By understanding these frameworks, we can gain insights into the current stage of RPKI adoption and the process organizations experience while integrating RPKI.

3.1 Technology Adoption Lifecycle

The *Technology Adoption Lifecycle* [49], introduced by Everett Rogers and popularized by Geoffrey Moore in *Crossing the Chasm* [37], is a theory of how new ideas and technologies spread over time. The framework divides technology adopters into five categories based on their attitudes towards adoption:

(1) Innovators (2.5%): The enthusiasts; first to realize the potential and adopt new technology
(2) Early Adopters (13.5%): The visionaries; early to recognize the value of new technology
(3) Early Majority (34%): The pragmatists; adopt new technology only after it has proven its value and become more established
(4) Late Majority (34%): The conservatives; adopt technology only after wide-scale adoption
(5) Laggards (16%): The skeptics; typically resistant to change, often preferring traditional solutions

In this lifecycle, each group influences the next in the adoption process. The model highlights that technology adoption is not uniform *i.e.,* different groups adopt at different rates, and each group has unique motivations and barriers.

RPKI in the context of Technology Adoption Lifecycle: In early 2025, 49.3% of organizations holding direct allocations of IP address space have issued at least one ROA, and 44.9% have issued ROAs for all their address space. RPKI ROA adoption has thus progressed beyond the Innovators and Early Adopters stage and is in the Early Majority stage. On the ROV side, several major players in the routing ecosystem, including large service providers and cloud platforms, have implemented ROV in their routers, effectively dropping invalid routing announcements. As a result, the spread of incorrect routing announcements has been significantly reduced [34, 48, 59].

In this work, we focus on the ROA side of RPKI; however, both the adoption of ROA and ROV have contributed to the maturity and benefits of RPKI adoption, making the technology transition from being a niche solution to a standard practice in the industry. Indeed, some cloud service providers now require their customers to issue RPKI ROA certificates to avail their services [9, 10]. Further, many governments are promoting the adoption of RPKI in their countries. As an example, in the US, the Federal Communications Commission (FCC) passed a ruling in May 2024 requiring Internet Service Providers (ISPs) to develop a plan to increase RPKI adoption (ROAs and ROV) with the goal of improving routing security in the country [50].

As RPKI adoption continues to grow, it is anticipated that the Late Majority and Laggards will begin their adoption process. However, these groups can still face challenges at all stages of the technology adoption process. Given the proven benefits of RPKI to overall Internet security [32, 55] supporting RPKI adoption of the late majority is key to improving the security of inter-domain routing. To assess the effort required to gain widespread adoption of RPKI, in the next section, we present the different stages of product adoption that will provide a framework to analyze where in the adoption process are the prefixes not yet covered by RPKI.

3.2 Product Adoption Process

While the Technology Adoption Lifecycle provides a macro-level view of how technologies are adopted across an ecosystem, Everett Rogers' *Diffusion of Innovation* framework provides a model of the micro-level journey of an individual or organization adopting a new technology [49]. This journey, known as the *Product Adoption Process* or *Innovation-Decision Process*, describes the stages an entity goes through from first learning about a technology to fully adopting it. The process consists of five stages:

(1) Knowledge (Awareness): The entity becomes aware of the new technology and potential benefits
(2) Persuasion (Interest): The entity forms a positive or negative opinion about the technology
(3) Decision (Planning and Evaluation): The entity decides to adopt the technology and begins planning for adoption (or rejects it entirely)
(4) Implementation (Trial and Deployment): The entity adopts the technology
(5) Confirmation (Adoption): The entity finalizes the decision and seeks reinforcement that the choice was correct

Roger's framework connects the broader lifecycle of technology adoption to the specific steps an organization must take to adopt a new technology. Each stage builds on the previous one, and successful adoption requires the entity to navigate all five stages.

RPKI in the context of Product Adoption Process: In the following, we frame the RPKI in the Product Adoption Process and discuss what parts of it can be measured to provide some insight into which organizations might be in which stage.

(1) Awareness: Organizations must first become aware of RPKI as a technology to secure their routing infrastructure. Community initiatives by RIRs, industry blogs, and working groups like MANRS [3, 24, 35, 36, 58, 66] played an essential role in making RPKI more of a mainstream technology. A clear (and measurable) sign of an organization's RPKI awareness is the issuance of a ROA. Although awareness is possible without a ROA issuance, it provides an estimation of awareness for the address space that is not yet covered by ROAs.
(2) Persuasion: Previous studies [34, 48, 59] that have demonstrated the benefits of RPKI adoption–particularly in mitigating the impact of routing misconfigurations and hijacks–have played a significant role in shaping organizations' positive outlook on RPKI. Other than directly interviewing the people in charge of creating ROAs in an organization, it is very hard to get a sense of the persuasion step, making it difficult to assess on a wide scale.
(3) Planning and Evaluation: In this decision step, organizations evaluate the feasibility of adopting RPKI. This includes planning ROAs for their prefixes, understanding the impact of ROAs on their routing services, and addressing technical and administrative barriers. To the best of our knowledge, there are no current best practices for planning the ROA issuance process, and the potential consequences of issuing a ROA for a given prefix before issuing one for a related (sub)prefix. These issues are not well understood, as evidenced by the persistent presence of routed invalid prefixes–often resulting from operators making selective or temporary exceptions in response to customer misconfigurations[2]. In §5.1 we propose a set of steps to support ROA planning and then in §6 we study routed prefixes not yet covered by RPKI through that lens.
(4) Implementation: Once an organization decides to issue ROAs, it engages in the implementation of the RPKI infrastructure provided by the RIR that delegated its address space to the organization. In this step, the organization interacts with all aspects needed to implement the technology, including legal agreements, interacting with the RIR resource management portal or provided API, and coordinating with third parties who may be impacted by the adoption (ideally, these dependencies are identified during the planning stage). Here again, measuring this step at scale is challenging. However, since each RIR has independently implemented the RPKI infrastructure for its region and designed how organizations issue and manage ROAs, comparing the adoption levels of similar organizations across RIRs would provide us with some insight into the impact of RIR's design decisions on ROA adoption.
(5) Adoption: Organizations reinforce the decision by monitoring the benefits of issuing the RPKI ROAs and maintaining them.

[2]The Internet Health Report [23] provides a daily list of RPKI invalid prefixes and their level of overall visibility in BGP.

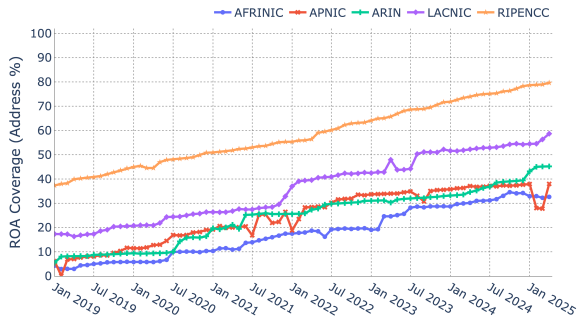


Figure 2: ROA coverage of routed IPv4 address space among the five RIRs; RIPE consistently has the highest adoption among all RIRs

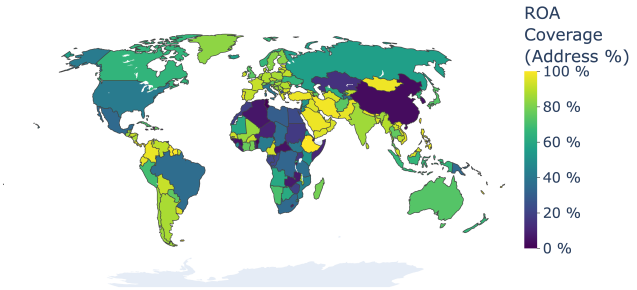


Figure 3: Country-wise ROA Coverage of IPv4 address space in April 2025; Middle Eastern nations have the highest coverage, while China has the lowest among large nations

In this paper, we focus on three key steps of the product adoption process in the context of RPKI: *(i)* RPKI Awareness, *(ii)* ROA Planning *(iii)* ROA Deployment; as they relate to disparities in RPKI adoption, which we identify and discuss in the next section.

4 RPKI Adoption

In this section, we study the current state of ROA adoption. We take a data-driven approach and study the distribution of ROA-covered prefixes to gain insights into adoption disparities that we then associate with challenges in the different parts of the adoption process.

4.1 Current State of RPKI Adoption

As of April 2025, 51.5% of the routed IPv4 address space and 61.7% of the routed IPv6 address space are covered by ROA certificates. In terms of prefix count, 55.8% of the routed IPv4 prefixes and 60.4% of the routed IPv6 prefixes are covered by ROAs. This progress is the result of significant efforts in recent years, with coverage increasing by 2.5× to 3× over the past 6 years (Figure 1). Despite these advances, 40 to 50% of the routed address space remains uncovered by ROAs. More importantly, from an organizational perspective, there are notable disparities in adoption rates depending on geographic region, organizational size, and business sector.

RIR-wise ROA coverage metrics: RPKI adoption varies significantly across the five Regional Internet Registries (RIRs) (Figure 2). RIPE has the highest ROA adoption rate, with about a 20-30% additional level of adoption compared to the next RIR. RIPE reached a 50% adoption rate (by IPv4 address space) in January 2021, and by April 2025, almost 80% of its routed IPv4 address space was covered by ROAs. LACNIC is the RIR with the second-highest level of adoption, reaching nearly 60% of the routed IPv4 address space as of April 2025. Then APNIC and ARIN have had similar levels of adoption, accounting for approximately 40% of the routed IP address space with ROAs in 2025. Finally, AFRINIC has lagged behind but is still following a similar rate of adoption, and currently almost 35% of the AFRINIC routed IPv4 address space is covered by ROAs. RIPE and LACNIC actively engage in outreach, training, and community events that we hypothesize increase the awareness and effectively communicate the benefits of RPKI [24]. In addition, the introduction of user-friendly tooling and improvements to ROA management infrastructure [1, 61] may support network operators in planing and issuing ROAs easily.

Country-wise ROA coverage metrics: A more granular analysis of the geographic distribution reveals significant variation in RPKI adoption at a country level (Figure 3). Middle Eastern and Latin American nations exhibit high rates of ROA adoption, while adoption in Asia and Africa lags behind. For example, China, owns 8.9% of all routed IPv4 address space and 16% of all routed IPv6 address space but has 3.23% and 0.1% of its address space covered by ROAs, respectively.

Organization size: The largest ASNs are the primary drivers of RPKI adoption. In Figure 4 we plot the percentage of large and small networks across different RIRs that originate at least 50% ROA-covered address space. We define a large network as an ASN in the top one percentile of all ASNs based on the amount of originated address space (measured in unique /24s). Conversely, an ASN is categorized as small if it is in the other 99%. Figure 4a reveals that the top 1% of ASNs, typically owned by major networking or technology companies, exhibit the highest rates of RPKI adoption. When examining adoption by RIR in Figure 4b, we observe that in RIPE, LACNIC, and ARIN, larger ASes have significantly higher ROA adoption rates than smaller ASes.

Smaller networks are more likely to lack awareness due to economical and human resources constrains. In addition, even when small networks might be aware of RPKI, they may not have access to the expertise needed to plan and evaluate RPKI adoption. Similarly, usually regulatory pressure is not directed toward smaller players, reducing their incentive to deploy security practices. As a result, it is harder for smaller networks to make progress with RPKI adoption.

Interestingly, in APNIC and AFRINIC, small ASNs have more adoption than their larger counterparts. Our manual investigation suggests that in APNIC, this reverse trend is primarily due to large telecom networks such as China Unicom and China Mobile, which, despite originating vast amounts of IPv4 addresses, have not engaged with RPKI.

In AFRINIC, the underlying reasons are very different. AFRINIC, as an organization, is facing significant governance and economic issues. Operators in AFRINIC increasingly face long delays in IP allocation and IP management change requests due to the poor operating conditions of AFRINIC caused by governance problems,

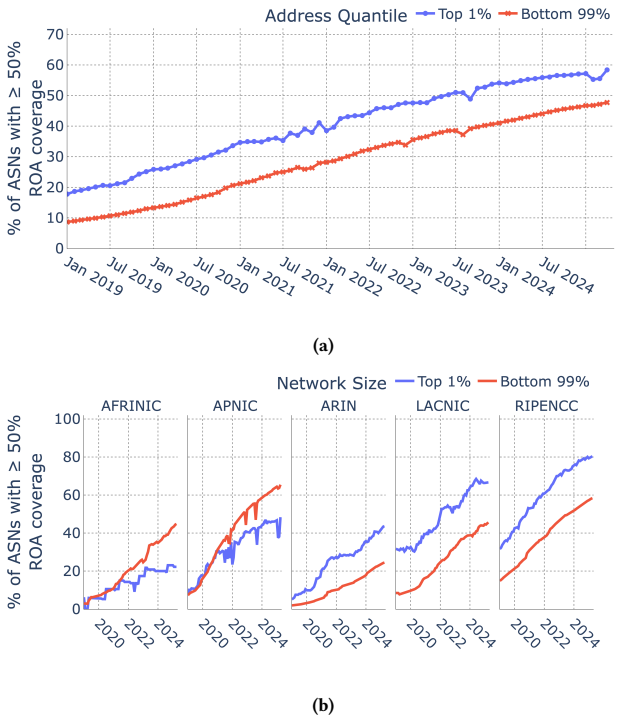


Figure 4: RPKI adoption in Large *vs.* Small ASes

Business Category	Num ASN	Num Prefix	ROA Prefix %	ROA Address %
Academic	1769	17271	27.13	26.84
Government	544	3581	21.45	23.34
ISP	2958	392624	78.88	56.36
Mobile Carrier	45	22367	37.01	51.17
Server Hosting	657	65590	73.51	88.90

Table 2: IPv4 ROA Coverage by Business Categories; Academic & Government ASes have the lowest coverage while Hosting providers have the highest

litigious, and financial conditions since 2021 [11, 38, 53]. The challenges faced by AFRINIC may hinder networks from issuing RPKI records using AFRINIC's infrastructure.

Business-wise ROA coverage metrics: We find significant disparities in the level of RPKI adoption by the business sector of organizations. Using publicly available datasets such as PeeringDB and ASdb [47, 67], we classify ASes based on the business sector of their owner organizations. Since comprehensive classification remains a challenge due to the inconsistencies in categorization methods, we study ASes that have a consistent categorization across the two different business classification datasets. We find that government and educational institutions exhibit low adoption rates across both PeeringDB and ASdb. Specifically, government ASes have an adoption rate of 21%, while educational institutions reach only 27% (Table 2). These rates are significantly lower than server

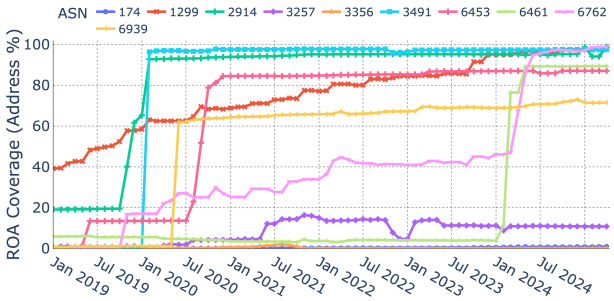


Figure 5: IPv4 RPKI Adoption of Tier-1 ASNs over time

hosting networks and ISPs, which stand at 74% and 79% respectively. The disparity in RPKI adoption rates by business sectors reveals the different communication channels, expertise and incentive inherent to organization in different sectors. In this case, hosting providers and ISPs are much more likely to have greater awareness of RPKI, expertise and incentives to implement routing security measures, as these directly impact the reliability and security of their core business operations. In contrast, government and educational networks are farther removed from core networking operations, increasing the lack of awareness, access to training and incentives, likely contributing to their low adoption rates.

ROA adoption of Tier-1s The adoption of RPKI by Tier-1 networks varies significantly, even though they are all large network providers with sizable network engineering teams. In Figure 5 we plot the ROA coverage of the routed IPv4 address space of select Tier-1 networks over time to shed light on the Tier-1 RPKI adoption journey. Many Tier-1 networks experience a rapid increase in coverage from low to high levels within a few months, as indicated by the more vertical part of their curves. However, there are some that slowly increase the ROA coverage of their address space, while others, as of April 2025, are still well below 20% of ROA adoption. We manually investigate these networks and find that there are significant differences in how they operate and manage their address space in relation to the address space their customers use. In the networks with low or no adoption, we see significant sub-delegation (re-allocation or re-assignment) of address space. As a consequence, many customers of those networks originate sub-prefixes of the Tier-1 networks. In this situation, it is crucial to plan the ROA deployment in coordination with customers to prevent availability issues once the ROA is published. We contact Tier-1 operators and confirm that coordinating with their customers significantly slows down their RPKI adoption. In addition, we learn that for some of the sub-delegated address space, the contractual relationship requires the customer to actually initiate the request to issue ROAs, even if the provider will issue the ROAs using the RIR portal or API [28].

Reversing RPKI adoption We find that some networks maintain a high ROA coverage for several months, possibly years, before experiencing a sharp decline, or occasionally zero ROA coverage. This decline may result from an organization's decision to intentionally revoke their ROAs or simply an expiration of the certificates that were subsequently not renewed. Figure 6 shows the case of five

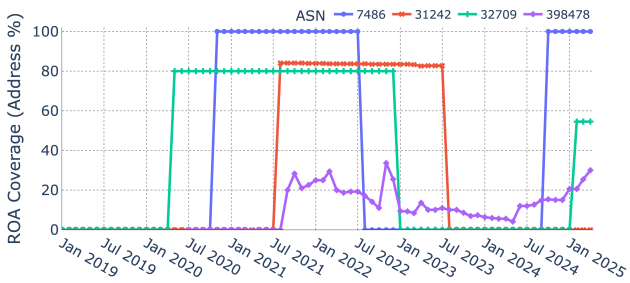


Figure 6: Several networks have issued ROAs for their address space and later dropped them

ASNs that either had a full or a significant level of RPKI adoption, for many months—some of them for years—and then reduced their ROA coverage to a very low level. This pattern suggests that even after an initial commitment to RPKI, there are still poorly understood operational or organizational factors that can lead to a reversal of adoption (the confirmation step at the end of the adoption process was not successful). One plausible explanation is that organizations may issue ROAs but fail to actively maintain or renew them upon expiry, resulting in unintended lapses or loss of coverage. Further investigation is needed to fully understand the underlying causes of this phenomenon.

4.2 Insights about RPKI Adoption Process

The disparities in RPKI adoption levels offer insights into the challenges and drivers of RPKI adoption.

4.2.1 The lack of RPKI awareness. Although measuring an organization's RPKI awareness is not possible at scale, we can infer that in groups lagging in adoption, there is less awareness of either the technology itself or its benefits. In the diffusion of innovations theory, Rogers argues that diffusion is the process by which an innovation is communicated through certain channels over time among the participants in a social system [49]. Community and closeness within a social system will support communication and, therefore, awareness of innovation.

In our analysis of RPKI adoption by different characteristics of organizations, we note significant disparities by geography and business sectors, both characteristics that would impact the community of the organizations. We hypothesize that the higher adoption rates in RIPE and LACNIC can be attributed to the proactive initiatives by these RIRs and working groups like Mutually Agreed Norms for Routing Security (MANRS) to promote RPKI adoption through outreach programs and training sessions [24, 35, 58].

Within a geographical region, we still find notable differences between countries' adoption rates, which can also relate to country-specific channels of communication and incentives such as a shared market and regulation. For instance, most Chinese organizations have been slow to adopt RPKI ROA, which can be attributed to a lack of incentives from the government or the local market to encourage its implementation.

We also find that RPKI adoption rates vary significantly across different business sectors. Although it might also relate to the size of organizations in terms of address space used, business sectors also share unique communication channels, pointing at a potential lack of awareness about RPKI in some sectors. For instance, organizations whose main business sector is not directly related to Internet services are less likely to have representation in the networking forums of RIRs or regional network operators' groups, such as NANOG, limiting their exposure to RPKI-related discussions and initiatives. Targeted campaigns in regions or sectors with low adoption rates could address the lack of RPKI awareness for specific groups of organizations.

4.2.2 The challenge of planning ROAs. Our study of RPKI adoption shed light on how RPKI ROAs for prefixes with small prefix length, such as the ones originated by large networks, can impact the availability of longer prefixes within the covering prefix and/or can reduce operational flexibility of networks, impacting traffic engineering but also security practices (*e.g.,* DDoS protection services (DPS) using BGP and Remotely Triggered Black Hole (RTBH)). Additional ROAs need to be issued for the same prefixes to allow for some of those practices.

Since RPKI can significantly impact the network operations, the ability to successfully plan ROAs is critical to encourage adoption. The slower journey of some Tier-1 networks reveals that even with expertise, successfully planning and adopting ROAs can take time as coordination with customers and adjustment to operational practices take time. Furthermore, the fact that some organizations with 100% ROA adoption roll back their adoption to almost 0% after more than a year indicates that the potential consequences of issuing ROAs are not widely understood. To the best of our knowledge, there are no current best practices for planning the ROA issuance process. To facilitate ROA planning, in section 5 we propose a flowchart outlining steps to consider during ROA planning and develop a system that consolidates relevant information about routed prefixes for these planning steps.

4.2.3 Difficulties in ROA Deployment. Even when an organization has decided to adopt RPKI, deployment can take some time and may deter initial efforts to adopt RPKI, as organizations discover all the steps and procedures needed to issue ROAs. As RIRs independently set up their RPKI infrastructure and procedures, comparing the adoption of RPKI between RIRs for similar organizations provides insights into the barriers encountered during the deployment stage. When examining the ROA coverage of the largest ASNs by RIR (see Figure 4b), the two RIRs with the lowest adoption level impose more resource and time-consuming procedures than the other RIRs. In ARIN, for organizations holding legacy address space, they first need to sign a legal agreement before being able to use ARIN IP management and RPKI infrastructure to issue ROAs, which has already been noted as a barrier to RPKI adoption [65]. AFRINIC requires the creation of a Business PKI certificate first to get access to RPKI services [2], which requires additional technical expertise compared to other RIRs' systems. Furthermore, we hypothesize that a lack of technical expertise for ROA deployment is one of the reasons behind the lower overall adoption of the non-top 1% ASNs and the organizations holding address space whose business sectors are not directly related to Internet services, such as academia and government. Comparing RIR procedures for issuing RPKI ROAs

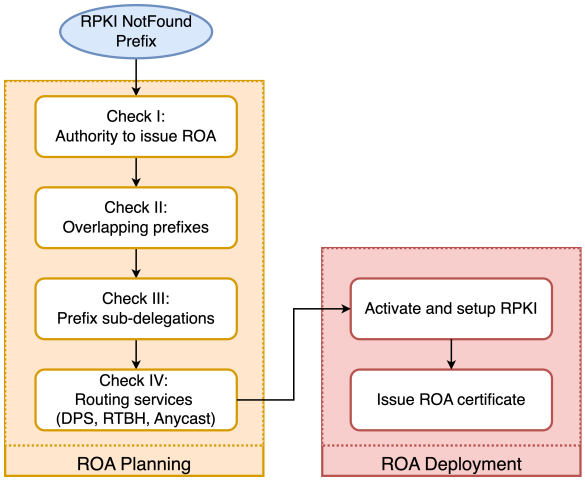


Figure 7: Structured flowchart for ROA planning & deployment

can help identify areas of the ROA adoption deployment process that could be improved to encourage further adoption.

5 Facilitating ROA Planning

Despite the growing adoption of RPKI, there is a lack of guidance for ROA planning. In this section, we address two key challenges: *(i)* the lack of a ROA planning framework and, *(ii)* the absence of a comprehensive platform to assist network operators during the ROA planning process.

5.1 A Procedure for ROA Planning

Although neither Best Current Practices (BCP) nor other guidance documents exist on how to plan ROAs, some relevant information is scattered across RFCs and tutorials: RFC 6482 discusses the standard technical profile of a ROA [25], RIR tutorials and RFC 9319 provide recommendations on using `MaxLength` attribute and what ROAs should be issued while using DDoS protection services [6, 14], and RFC 9455 provides recommendations on the number of prefixes that should be in each ROA [64].

To support ROA planning, we propose a framework for planning ROAs that identifies a set of critical factors that network operators must consider when issuing ROA certificates. Figure 7 presents the procedure consisting of several steps that should be resolved to plan ROA(s) for a prefix.

We conducted an iterative process, contacting network operators and RIRs to develop this framework. Through discussions and feedback requests, we identified the key considerations an organization should make while planning ROAs[3]. We stopped after we had a few interactions without corner cases modifying the steps.

In this section, we present our ROA planning framework and discuss the key elements that require attention during the ROA planning process.

[3]We had in-depth discussions with six routing security experts from North America, Europe, Asia, and Oceania. These participants included individuals from major network providers, academic networks, and experts on RPKI infrastructure and tooling. We also presented a preliminary version of the framework and requested feedback from more than 20 network engineers.

5.1.1 Authority to issue ROA:. The first step in planning for an organization that wants to issue ROAs is to determine whether it has the authority to issue ROAs for the prefix in question. At the time of writing, only organizations with direct delegation of address space from RIRs can issue ROAs and host them in the public RIR RPKI repositories [5, 41]. Organizations holding sub-delegations of address space may request the holders of the direct delegation (Direct Owner) to issue ROAs for their prefixes. If the Direct Owner implemented a delegated CA model—hosting a RPKI repository and providing a signing engine for their and their customers' RPKI certificates—organizations with sub-delegation can also use that infrastructure to issue their ROAs. The Hosted CA model accounts for more than 90% of all Validated ROA Payloads (VRPs), and prefixes not covered by ROAs are typically not under a Delegated CA (as Delegated CAs are generally proactive about ROA management).

5.1.2 Overlapping routed prefixes: A ROA for a prefix impacts routing announcements of the same prefix or more-specific prefixes covered by the initial prefix. In this step, the organization wanting to issue ROAs should identify all routed prefixes that match or are covered by the prefix in question. This is important because ROAs for these prefixes may need to be issued either first or concurrently, to prevent any impairment of the reachability of the related IP addresses. To minimize the risk of making legitimate routes RPKI-Invalid, ROAs for the longest (most specific) prefixes should be issued first.

5.1.3 Sub-delegations: When a holder of an address space (partially or fully) *sub-delegates* a block of IP addresses to another organization, the contractual relationship between the two organizations may modify which organization has the ability to request ROA issuance. Some organizations will issue ROAs only if the customer requests them. In most cases, for prefixes with re-delegations, coordination between the organizations is needed to prevent any impact on the routing traffic and services.

5.1.4 Routing services. As described in §4.2.3, routing practices such as DDoS protection services, RTBH, and anycast may be impacted by the issuance of ROAs. Prefixes supporting these services may require multiple ROAs to reflect their unique routing configurations, as they may be originated from different ASNs or under specific operational circumstances.

The flowchart in Figure 7 ensures that the most relevant factors are accounted for, presenting actions in a structured order to plan ROAs, minimizing loss of availability and operational risk. That said, there is an important limitation to this flowchart: ROAs from an organization may affect the routing-related services contracted by the upstream provider (or provider of the provider), without the organization being aware of these services. For example, a regional network might contract DDoS protection services to cover all its traffic, including that of its customer ASes. Our flowchart is designed to be more general-purpose, addressing most criteria visible from public routing data. Nevertheless, internal routing services and traffic engineering must also be considered during the planning and deployment phases of ROAs.

To follow the checks outlined in the procedure proposed above, organizations need to collect organization-level and routing-level information, which may require accessing multiple distinct databases

and building a hierarchy of prefixes. To address this challenge, we built a platform designed to provide operators with the publicly available data required to implement this procedure effectively. The next section describes the platform.

5.2 ru-RPKI-ready: A Platform for ROA Planning

To consolidate data and insights required to execute the flowchart presented in §5.1, and plan ROAs effectively, we developed ru-RPKI-ready. Figures 12, 13 and 14 in the appendix provide screenshots of the ru-RPKI-ready user interface.

By combining this platform with the systematic procedure, we aim to facilitate the RPKI adoption process for network operators by structuring and providing the necessary information for decision-making. In the following section, we provide an overview of the platform, its features, and how it supports ROA planning.

5.2.1 Feature overview: ru-RPKI-ready provides a user interface where a user can:

(i) search for a specific prefix and get the corresponding delegation and routing data, such as the organization with direct allocation, origin ASNs, and several tags which we discuss in §5.2.2;

(ii) search for a specific organization to find the set of prefixes directly allocated to the organization;

(iii) search for a specific ASN and find the set of prefixes originated by the ASN and the ROA coverage of all announced prefixes;

(iv) generate the configuration needed to create corresponding ROAs (according to the publicly available information the tool gathers) and the order in which they should be issued to prevent rendering other routes invalid.

```
"216.1.81.0/24": {
    "RIR": "ARIN",
    "Direct Allocation": "Verizon Business",
    "Direct Allocation Type": "ALLOCATION",
    "Customer Allocation": "NBCUNIVERSAL MEDIA",
    "Customer Allocation Type": "REASSIGNMENT",
    "RPKI Certificate": "29:92:C2:35:B0:89...",
    "Origin ASN": "701",
    "ROA_covered": "False",
    "Country": "US",
    "Tags": ["ROA Not Found", "RPKI_Activated", "
        Reassigned", "Same SKI (Prefix, ASN)", "Leaf", "
        ROA Org", "Large Org", "(L)RSA"]
}
```

Listing 1: ru-RPKI-ready data for 216.1.81.0/24.

5.2.2 Feature description: Listing 1 provides a view of the tool data for prefix 216.1.81.0/24. We describe the main features below. We provide a complete list of ru-RPKI-ready tags and their description in Appendix B.2.

(1) **Prefix RPKI State:** The platform identifies if the prefix is in an RPKI Resource Certificate, as indicated by RPKI-Activated or Non RPKI-Activated tag. It also identifies the RPKI status of a prefix-origin pair indicated as RPKI Valid, RPKI NotFound, RPKI Invalid, or RPKI Invalid, more-specific.
(2) **Ownership Structure:** The platform identifies the organization holding the direct allocation of the prefix, referred to as the *Direct Owner*. This organization has the authority to issue ROAs for the prefix. If the prefix (or a sub-prefix) has been further delegated to customer organizations, the platform lists those organizations and tags the prefix according to the allocation type in WHOIS (*e.g.,* Reassigned, see §5.2.3).
(3) **Routing Information:** A prefix is tagged as Leaf if it does not have any routed sub-prefix. In contrast, a prefix is tagged Covering if it has a routed sub-prefix. If the routed sub-prefix has been reassigned to a customer organization, it is additionally tagged as External, signaling the need for external coordination while issuing ROAs. Further, if the prefix and origin ASN are present in the same RPKI Resource Certificate, we assign the Same SKI (Prefix, ASN) tag, indicating that the prefix and origin ASN are managed by the same entity.
(4) **Organization Characteristics:** We categorize the Direct Owners as Large, Medium or a Small sized organization based on the number of routed prefixes they have been directly allocated[4]. If the Direct Holder in the past year has routed at least one ROA-covered address block that it has been directly allocated, we tag it as Organization-Aware.
(5) **ROA Configuration and Prioritization:** The platform suggests the recommended ROA configuration for each prefix, including the origin ASN and max-length attribute. It also recommends the order in which ROAs should be issued based on the overlapping address spaces.
(6) **ARIN-specific Tags:** We classify a prefix as Legacy if it belongs to the legacy address space. Additionally, if the Direct Owner of an ARIN prefix has signed the Resource Service Agreement (RSA) or Legacy Resource Service Agreement (LRSA) with ARIN, we assign the tag (L)RSA. If they have not signed the agreement, we assign the tag Non-(L)RSA.

5.2.3 Datasets and Methodology. We utilize several datasets to examine the routing and organizational characteristics of a prefix.

BGP Data: We fetch the set of routed IPv4 and IPv6 prefixes from all Routeviews and RIPE RIS route collectors [39, 43]. We drop all prefixes that are seen by fewer than 1% of route collectors, as these prefixes are typically intended for internal traffic engineering. We filter out IPv4 prefixes with a prefix length more specific than /24 and IPv6 prefixes more specific than /48. These hyper-specific prefixes are not expected to be routed [52] and hence are not considered for ROAs. We filter out prefixes from our dataset that are part of the IANA reserved address space and should not be advertised in BGP [22]. We also filter out prefixes originated by bogon ASes since these ASes are IANA reserved and should not be originating prefixes in BGP.

RPKI Data: We use the list of validated ROAs from the RIPE FTP server to infer the RPKI status of each routed prefix-origin ASN pair [40]. We also use the RPKIviews archive to fetch the Resource Certificates corresponding to each routed prefix [54].

WHOIS: We use the Bulk WHOIS dataset to find the owners of an address block and the corresponding allocation status values. We fetch data from the five RIRs—AFRINIC, APNIC, ARIN, LACNIC, RIPE, and three NIRs—JPNIC, KRNIC, and TWNIC. The Bulk

[4]An organization is categorized as Large if it falls within the top 1 percentile of organizations by the number of routed prefixes it owns. If the organization is not in the top one percentile but owns more than one routed prefix, it is categorized as Medium. Organizations that own only one routed prefix are considered Small. We repeated our analysis using routed address space instead of the prefix count and observed consistent trends in our results. For simplicity, we categorize organizations based on prefix count.

WHOIS data of JPNIC does not include allocation status information, but the WHOIS query responses do. Thus, we query the JPNIC WHOIS dataset for each prefix individually and retrieve the organization name and allocation status. We utilize the IP prefix hierarchy to identify direct allocations from RIRs to sub-delegations to other organizations[5].

IANA Legacy Addresses: We use the list of IPv4 assignments made by IANA to identify which address blocks are considered *Legacy* [22].

ARIN RSA Data: We use the ARIN Resource Registry Service to identify which address blocks have been registered with an RSA or LRSA agreement with ARIN [4].

Identifying Organizational Awareness: To identify if an organization is aware of RPKI and has issued ROAs before, we use historical routing data to check if, in the past year, the organization has routed at least one ROA-covered prefix that it has been directly allocated. For a given organization, we take monthly snapshots of the routing table and check if, among the set of routed prefixes it holds directly, any prefix has a covering ROA.

Order of issuing ROAs: We prioritize issuing the ROAs for the most-specific prefixes first. Next, we order the covering prefixes and advise issuing the ROA only after all routed sub-prefixes are already covered by ROAs.

By providing these tags and additional data, `ru-RPKI-ready` platform simplifies the ROA issuance process and ensures that network operators have access to the necessary data and tools in one place.

6 Prefixes without ROAs

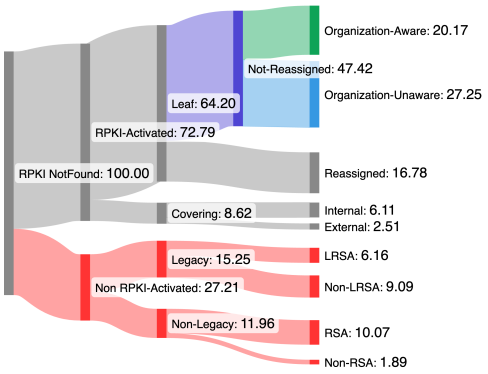
Using `ru-RPKI-ready`, we analyze the prefixes not currently covered by ROAs to understand the efforts and complexities required to issue ROAs for the remaining 45% of prefixes. The process of planning and issuing ROAs is not uniform across all prefixes. As discussed in the previous section, several factors must be considered when planning a ROA. While planning for some prefixes is straightforward, others require more effort, such as inter-organizational communication or administrative processes, which are captured by the tags of `ru-RPKI-ready`.

In this section, we examine the tags assigned by `ru-RPKI-ready` to the prefixes routed on 1 April, 2025. We first focus on the prefixes for which planning ROAs is relatively simple (§6.1). Following this, we examine the opposite end of the spectrum, discussing the most challenging prefixes to issue ROAs for (§6.2) to highlight the different levels of difficulties and varying efforts required to achieve full ROA coverage. Figure 8 displays the Sankey diagrams, which show the percentage of IPv4 and IPv6 prefixes in various categories for each of the planning steps outlined in the flowchart in Figure 7.

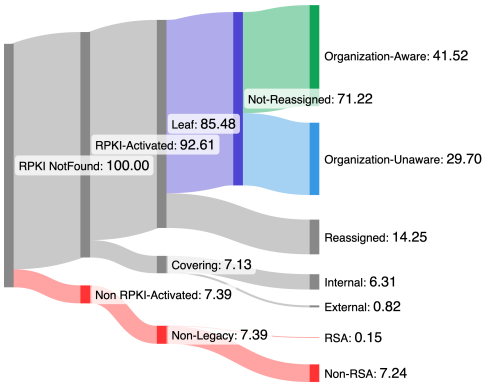
6.1 RPKI-Ready Prefixes

The complexities of ROA planning often arise from intricate routing and address delegation structures. However, by leveraging the tags generated by `ru-RPKI-ready`, we identify a substantial set of prefixes that do not face these complications. We term these *RPKI-Ready* prefixes, defined as those prefixes *(i)* RPKI-activated (as evidenced by being in RPKI Resource Certificates), *(ii)* without

[5]We note that the five RIRs use different nomenclature for prefix allocation types. `ru-RPKI-ready` reports the allocation type from WHOIS.



(a) IPv4 prefixes



(b) IPv6 prefixes

Figure 8: Percentage of routed IPv4 and IPv6 prefixes not covered by ROAs in each category of `ru-RPKI-ready`; RPKI-Ready prefixes (marked purple) and Low-Hanging prefixes (marked green) have a simpler ROA planning stage in comparison to other categories of prefixes.

routed sub-prefixes, and *(iii)* not reassigned to customers. Issuing ROAs for these prefixes should be straightforward.

Low-Hanging Prefixes: As discussed in §3, even with *RPKI-Ready* prefixes, there may be a lack of awareness that impedes RPKI adoption. Within the *RPKI-Ready* prefixes, we define the *Low-hanging fruit* prefixes as those delegated to organizations that have issued at least one ROA in the past year, indicating that the organization is aware of RPKI and how to issue ROAs. Of all *RPKI-Ready* prefixes, 42.4% (20.1% of all *RPKI NotFound* IPv4 prefixes) are *Low-Hanging fruit* prefixes, meaning they are *(i) RPKI-Ready* and *(ii)* from an organization that is aware of RPKI (Figure 8a). For IPv6, 58.3% of *RPKI-Ready* prefixes (41.5% of all *RPKI NotFound* IPv6 prefixes) are *Low-Hanging fruit* prefixes (Figure 8b).

We investigate the organizations behind these *low-hanging fruit* prefixes and find that Korea Telecom, Telecom Italia, and China Mobile collectively hold over 20% of all *Low-Hanging* IPv4 address space, while the top twenty organizations account for 60%, mostly in

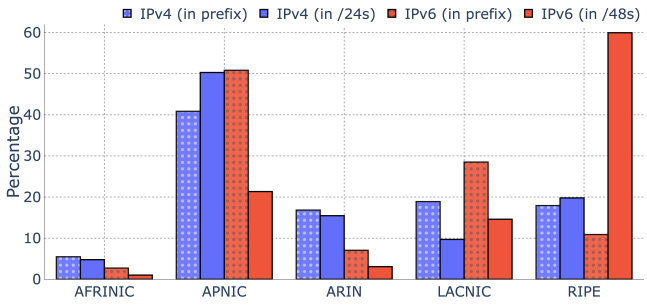


Figure 9: % of RPKI-Ready prefixes and address space by RIR

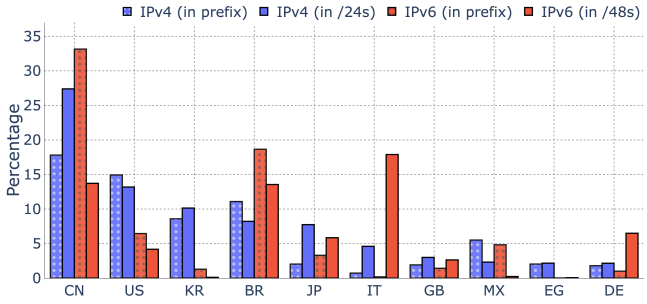


Figure 10: % of RPKI-Ready prefixes and address space by Country

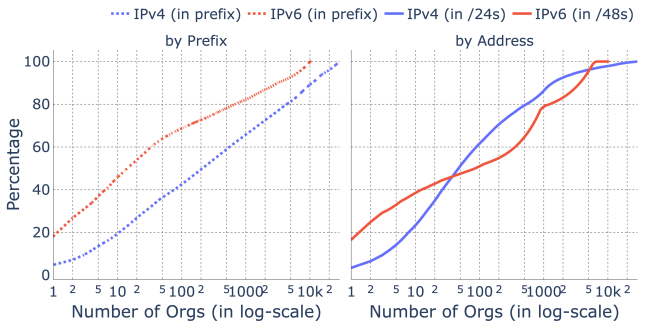


Figure 11: CDF of RPKI-Ready prefixes and addresses by Organization; 10 largest organizations own more than 20% and 40% of the RPKI-Ready IPv4 and IPv6 prefixes respectively

Org Name	% RPKI-Ready Pfx (v4)	Issued ROAs Before
China Mobile	4.82	True
UNINET	2.38	True
China Mobile Comms Corp	2.29	False
TPG Internet Pty Ltd	2.19	True
CERNET	1.87	False
CenturyLink Comms, LLC	1.45	True
Korea Telecom	1.13	True
Optimum	1.12	True
Korean Education Network	1.10	True
TE Data	1.02	False

Table 3: Organizations with most RPKI-Ready v4 prefixes

APNIC. Across RIRs, Cloud Innovation (AFRINIC), Korea Telecom (APNIC), Centurylink Communications (ARIN), UNINET (LACNIC), and Telecom Italia (RIPE) are the largest holders of *Low-Hanging* IPv4 address space.

RPKI-Ready Prefixes: Using `ru-RPKI-ready`'s tags, we quantified and analyzed the characteristics of all *RPKI-Ready* prefixes. Among routed IPv4 prefixes lacking ROAs, 47.4% are *RPKI-Ready*, and more than half of these are held by large organizations (top 1% by routed address space). Similar to the *Low-hanging fruit* prefixes, these prefixes are predominantly concentrated in the APNIC region, especially in China and Korea (Figure 9, Figure 10). In the IPv6 space, *RPKI-Ready* prefixes account for 71.2% of all *RPKI NotFound* prefixes, with APNIC and LACNIC regions—and particularly China and Brazil—being the major contributors.

We note that while issuing ROAs for *RPKI-Ready* prefixes should generally be easy, if they are not *low-hanging fruits*, the organization with authority to issue ROAs might still lack awareness or might not have "activated" RPKI in the respective RIR portal.

Large vs Small Organizations: We compare the allocation of *RPKI-Ready* prefixes between large and small organizations. Large organizations are defined as the top 1% by number of routed prefixes, while small organizations own only a single routed prefix. In the IPv4 space, large organizations originate at least 169 prefixes. Remarkably, 40% of all *RPKI-Ready* prefixes are owned by just 76 organizations. Organizations such as China Mobile, China Unicom, and the China Education and Research Network (CERNET) dominate this list. We include the top 10 organizations in Table 3. The top ten organizations alone account for 19.4% of all *RPKI-Ready* IPv4 prefixes. If these ten organizations issued ROAs for their prefixes, the global IPv4 ROA coverage would increase from 57.3% to 61.2% (a 6.8% improvement). In IPv6, there is even greater concentration, as six organizations hold 40% of *RPKI-Ready* prefixes (Table 4), with China Mobile, China Unicom, and CERNET collectively owning 30.5%. If the top ten organizations issued ROAs for their *RPKI-Ready* prefixes, IPv6 ROA coverage would increase from 63.4% to 75.3% (an 18.9% improvement).

To assess the effort required to support organizations with *RPKI-Ready* prefixes, we analyze the distribution across organizations and plot the CDF in Figure 11. The list of small organizations comprises 28k entities in IPv4 and 17k entities in IPv6. Collectively, these organizations account for only 5.2% of *RPKI-Ready* prefixes in IPv4 and 8.9% of *RPKI-Ready* in IPv6. While *RPKI-Ready* prefixes have a lower barrier for ROA issuance, the process is not straightforward for all prefixes. The following section explores more challenging cases for ROA issuance.

6.2 Prefixes not RPKI-Activated

In contrast to *RPKI-Ready* prefixes, `Non RPKI-Activated` prefixes require the organization to first activate RPKI tools in the RIR portal before being able to issue ROAs.

Among all *RPKI NotFound* prefixes, 27.2% of IPv4 prefixes are `Non RPKI-Activated`, indicating that their Direct Owner has not yet activated RPKI for these prefixes. Notably, 15.2% of these `Non`

Org Name	% RPKI-Ready Pfx (v6)	Issued ROAs Before
China Mobile	18.21	True
China Unicom	8.59	True
Vodafone Idea Ltd. (VIL)	4.12	True
TIM S/A	3.00	False
KDDI CORPORATION	2.91	True
CERNET IPv6 Backbone	2.35	False
Huicast Telecom Limited	1.80	False
IP Matrix, S.A. de C.V.	1.74	True
OOREDOO TUNISIE SA	1.74	False
CERNET2	1.36	False

Table 4: Organizations with most RPKI-Ready v6 prefixes

`RPKI-Activated` prefixes belong to the legacy address space, which often faces additional administrative and policy hurdles. Interestingly, 16.6% of the *RPKI NotFound* prefixes are associated with organizations that have already signed ARIN's LRSA or RSA agreements, yet have not completed RPKI activation in their resource management portal.

A significant share of the largest `Non RPKI-Activated` routed IPv4 prefixes is held by major U.S. federal institutions, including the *DoD Network Information Center*, *Headquarters, USAISC*, *USDA*, and *Air Force Systems Networking*. These institutions also dominate the `Non RPKI-Activated` routed IPv6 prefixes, with the *DoD Network Information Center* and *Headquarters, USAISC* collectively holding 50% of these prefixes. Because these institutions have not yet signed the necessary agreements with ARIN, ROAs cannot be easily issued for their prefixes. The challenges associated with `Non RPKI-Activated` prefixes underscore the need for targeted efforts to address the administrative and procedural barriers that hinder their inclusion in the RPKI ecosystem.

7 Discussion

The adoption of RPKI and the widespread issuance of ROAs are essential steps towards securing the global Internet routing system. In this paper, we examined the current landscape of RPKI adoption through the lens of technology and product adoption lifecycles, illustrating how organizations progress from initial awareness to experimentation and ultimately to mainstream deployment. Our data-driven analysis reveals that despite significant growth in RPKI coverage, persistent gaps in adoption still exist.

Organizations often encounter non-technical barriers during the process of RPKI adoption, and these obstacles are inherently difficult to quantify. Such barriers include a lack of awareness, inadequate expertise to evaluate and plan adoption, insufficient incentives, and the complexity of coordinating across multiple administrative domains. Challenges can indeed arise at various stages of the product adoption process: from the fact that little is known about RPKI outside the networking community, to the poorly understood benefits and the lack of tools to test and plan adoption.

Our findings reveal that the challenges of RPKI adoption extend well beyond initial awareness. The planning and deployment of ROAs present technical and administrative complexities that are not yet fully addressed by existing documentation or operational guidelines. In particular, we find that the absence of a structured planning procedure creates significant barriers, especially for smaller organizations, who may lack the resources or expertise to navigate the process effectively. Encouraging and supporting RPKI adoption for these organizations is particularly pressing, as they are lagging behind when compared to the top 1% of organizations in terms of address space.

To address these challenges, we propose a structured framework for ROA planning, including a systematic flowchart, and introduce a platform that consolidates all relevant data and operational guidance for network operators. By providing a unified resource for ROA planning, this platform aims to lower the barriers for organizations of all sizes, foster best practices, and support the continued growth of the RPKI ecosystem.

Using `ru-RPKI-ready` we characterized the routed address space not yet covered by ROAs and found that a significant fraction of this space could be secured with minimal planning. Conversely, another substantial portion requires organizations to sign agreements with RIRs and navigate policy barriers, particularly for the legacy address space. These obstacles suggest that achieving 100% ROA coverage may not be as easy as it may seem. Nevertheless, it is crucial for organizations to secure the address space supporting critical services.

Limitations: It is important to note that `ru-RPKI-ready` should not be the sole resource for ROA planning and deployment. Currently, `ru-RPKI-ready` generates tags and configurations based on publicly available BGP feeds from the latest month. Operators must also verify their internal announcements and private peering sessions, which are not visible to us. Depending on their internal traffic engineering, operators may need to issue additional ROAs to cover these scenarios.

Future work: Networks may announce certain routes sporadically, for example, due to DDoS mitigation, load balancing, or experimental services. Such transient announcements may not appear in the latest BGP snapshots and, as a result, may not be captured by `ru-RPKI-ready`. To improve our recommendations, we would like to incorporate historical routing data to identify prefixes that require temporary or event-driven ROAs.

8 Conclusions

Although more than 50% of the routed address space is currently covered by RPKI ROAs, RPKI adoption is far from being mastered. The processes for planning ROA adoption and understanding the full range of interactions between RPKI adoption and network operations are still poorly understood, which continues to limit faster adoption by early- and late-majority organizations.

To support the RPKI adoption process, we propose a framework to plan RPKI ROA adoption. We also make publicly available a tool that utilizes BGP, RPKI, and WHOIS data to propose ROAs for prefixes currently not in RPKI based on the framework. We then use this tool to study all the routed address space not yet in RPKI and find that a significant portion of it (41% for IPv4 and 71% for IPv6) can be directly issued in RIR portals. However, most organizations managing those prefixes in RIR portals appear not to be aware of RPKI, as they have not issued any ROA in the last 12 months.

Combining the results of our ROA planning tool with the improved understanding of RPKI adoption stages and barriers provides guidance for targeted recommendations and actions that can encourage RPKI adoption for different organizations. We hope that our findings, dataset, and tools will inform future research, guide operational management, and encourage collaborative improvements across the Internet community to realize the full potential of RPKI. We argue that the security and stability of the Internet's routing infrastructure depend on broad, consistent, and correct RPKI adoption. Achieving this goal will require ongoing technical innovation, community engagement, and the development of effective policies. Our work provides a foundation for these efforts by identifying key obstacles, proposing practical solutions, and offering a roadmap for accelerating RPKI deployment worldwide.

Acknowledgments

This work is partly supported by the National Science Foundation grant OAC-2419735, a Google Research gift, and the Internet Initiative Japan (IIJ) Internship program. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation, Google, or IIJ. We thank Google for their generous support.

References

[1] RIPE Network Coordination Centre 2024. *New Resource Certification (RPKI) Dashboard*. RIPE Network Coordination Centre. https://www.ripe.net/about-us/news/new-resource-certification-rpki-dashboard/ Accessed: 2025-09-22.

[2] AFRINIC. 2023. AFRINIC's RPKI. Retrieved May 13, 2025 from https://afrinic.net/resource-certification

[3] ARIN. 2024. Enhance Your Routing Security Using ARIN's Hosted RPKI. Retrieved January 23, 2024 from https://www.arin.net/announcements/20240709/

[4] ARIN. 2025. ARIN Resource Service Registry. Retrieved January 21, 2025 from https://ftp.arin.net/pub/resource_registry_service/networks.csv

[5] ARIN. 2025. RESOURCE PUBLIC KEY INFRASTRUCTURE. Retrieved April 29, 2025 from https://www.arin.net/resources/manage/rpki/rpki.pdf

[6] Network Startup Resource Center. 2020. Route Origin Authorisation: Creating ROAs. https://learn.nsrc.org/bgp/creating_roas

[7] Taejoong Chung, Emile Aben, Tim Bruijnzeels, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, Roland van Rijswijk-Deij, John Rula, and Nick Sullivan. 2019. RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins. In *Proceedings of the Internet Measurement Conference (IMC '19)*. Association for Computing Machinery, Amsterdam, Netherlands, 406–419. https://doi.org/10.1145/3355369.3355596

[8] John Curran. 2024. Update to ARIN's RPKI Service Access. Retrieved September 22, 2025 from https://www.arin.net/announcements/20240624/

[9] Amazon Web Services Documentation. 2025. Bring your own IP addresses (BYOIP) to Amazon EC2. Retrieved Nov 13, 2024 from https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-byoip.html

[10] Google Cloud Documentation. 2025. Bring your own IP addresses. Retrieved May 2, 2025 from https://cloud.google.com/vpc/docs/bring-your-own-ip

[11] Monika Ermert. 2025. Afrinic crisis forces reform of global IP address management. Retrieved May 13, 2025 from https://www.heise.de/en/news/Afrinic-crisis-forces-reform-of-global-IP-address-management-10367454.html

[12] Romain Fontugne, Amreesh Phokeer, Cristel Pelsser, Kevin Vermeulen, and Randy Bush. 2023. Rpki time-of-flight: Tracking delays in the management, control, and data planes. In *International Conference on Passive and Active Network Measurement*. Springer, 429–457.

[13] Yossi Gilad, Avichai Cohen, Amir Herzberg, Michael Schapira, and Haya Shulman. 2017. Are We There Yet? On RPKI's Deployment and Security. In *Proceedings 2017 Network and Distributed System Security Symposium*. Internet Society, San Diego, CA. https://doi.org/10.14722/ndss.2017.23123

[14] Yossi Gilad, Sharon Goldberg, Kotikalapudi Sriram, Job Snijders, and Ben Maddison. 2022. The Use of maxLength in the Resource Public Key Infrastructure (RPKI). RFC 9319. https://doi.org/10.17487/RFC9319

[15] Yossi Gilad, Omar Sagga, and Sharon Goldberg. 2017. MaxLength Considered Harmful to the RPKI. In *Proceedings of the 13th International Conference on Emerging Networking EXperiments and Technologies (CoNEXT '17)*. ACM, New York, NY, USA, 101–107. https://doi.org/10.1145/3143361.3143363 event-place: Incheon, Republic of Korea.

[16] Dan Goodin. 2018. How 3ve's BGP hijackers eluded the Internet—and made $29M. https://arstechnica.com/information-technology/2018/12/how-3ves-bgp-hijackers-eluded-the-internet-and-made-29m/.

[17] Dan Goodin. 2022. How 3 hours of inaction from Amazon cost cryptocurrency holders $235,000. https://arstechnica.com/information-technology/2022/09/how-3-hours-of-inaction-from-amazon-cost-cryptocurrency-holders-235000/.

[18] Brad Gorman. 2024. *ARIN RPKI Updates and Upcoming Enhancements*. American Registry for Internet Numbers. https://www.arin.net/blog/2024/04/09/rpki-updates/ Accessed: 2025-09-22.

[19] Rahul Hiran, Niklas Carlsson, and Phillipa Gill. 2013. Characterizing Large-Scale Routing Anomalies: A Case Study of the China Telecom Incident. In *Passive and Active Measurement*, David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell, Moni Naor, Oscar Nierstrasz, C. Pandu Rangan, Bernhard Steffen, Madhu Sudan, Demetri Terzopoulos, Doug Tygar, Moshe Y. Vardi, Gerhard Weikum, Matthew Roughan, and Rocky Chang (Eds.). Vol. 7799. Springer Berlin Heidelberg, Berlin, Heidelberg, 229–238. https://doi.org/10.1007/978-3-642-36516-4_23

[20] Tomas Hlavacek, Philipp Jeitner, Donika Mirdita, Haya Shulman, and Michael Waidner. 2022. Behind the Scenes of RPKI. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*. Association for Computing Machinery, New York, NY, USA, 1413–1426. https://doi.org/10.1145/3548606.3560645

[21] Daniele Iamartino, Cristel Pelsser, and Randy Bush. 2015. Measuring BGP Route Origin Registration and Validation. In *Passive and Active Measurement (Lecture Notes in Computer Science)*, Jelena Mirkovic and Yong Liu (Eds.). Springer International Publishing, Cham, 28–40. https://doi.org/10.1007/978-3-319-15509-8_3

[22] IANA.org. 2025. IANA IPv4 Address Space Registry. Retrieved January 21, 2025 from https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml

[23] Internet Initiative Japan Inc. 2023. Internet Health Report. https://ihr-archive.iijlab.net.

[24] LACNIC. 2023. Evolution of RPKI: Towards Higher Levels of Security in Regional Routing. Retrieved January 23, 2024 from https://blog.lacnic.net/en/interconnection/evolution-of-rpki-towards-higher-levels-of-security-in-regional-routing

[25] Matt Lepinski, Derrick Kong, and Stephen Kent. 2012. A Profile for Route Origin Authorizations (ROAs). RFC 6482. https://doi.org/10.17487/RFC6482

[26] Eva Li. 2025. ARIN adjusts RSA to align with global IP resource management. Retrieved September 22, 2025 from https://btw.media/all/internet-governance/arin-adjusts-rsa-to-align-with-global-ip-resource-management/

[27] Yanbiao Li, Hui Zou, Yuxuan Chen, Yinbo Xu, Zhuoran Ma, Di Ma, Ying Hu, and Gaogang Xie. 2022. The Hanging ROA: A Secure and Scalable Encoding Scheme for Route Origin Authorization. In *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*. IEEE Press, London, United Kingdom, 21–30. https://doi.org/10.1109/INFOCOM48880.2022.9796844

[28] Lumen 2025. . Lumen. https://assets.lumen.com/is/content/Lumen/rpki-customer-notification?Creativeid=1c967bb7-1321-4be8-92c0-74097e840849

[29] Doug Madory. 2018. BGP Hijack of Amazon DNS to Steal Crypto Currency. https://dyn.com/blog/bgp-hijack-of-amazon-dns-to-steal-crypto-currency/.

[30] Doug Madory. 2018. Learning from recent major BGP routing leaks. https://www.slideshare.net/apnic/learning-from-recent-major-bgp-routing-leaks.

[31] Doug Madory. 2019. Large European Routing Leak Sends Traffic Through China Telecom. https://blogs.oracle.com/internetintelligence/large-european-routing-leak-sends-traffic-through-china-telecom.

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

[33] Doug Madory and Job Snijders. 2024. How much does RPKI ROV reduce the propagation of invalid routes? https://www.kentik.com/blog/how-much-does-rpki-rov-reduce-the-propagation-of-invalid-routes/.

[34] Doug Madory and Job Snijders. 2024. RPKI ROV Deployment Reaches Major Milestone. https://www.kentik.com/blog/rpki-rov-deployment-reaches-major-milestone/.

[35] MENOG. 2023. BGP Operations and Security Training Course. Retrieved January 23, 2024 from https://www.menog.org/meetings/menog-23/workshops/

[36] Robbie Mitchell. 2020. Community comes together to make deploying RPKI easier. Retrieved January 23, 2024 from https://blog.apnic.net/2020/04/06/community-comes-together-to-make-deploying-rpki-easier/

[37] G.A. Moore. 2002. *Crossing the Chasm: Marketing and Selling Disruptive Products to Mainstream Customers*. HarperCollins. https://books.google.com/books?id=yJXHUDSaJgsC

[38] Milton Mueller, Vagisha Srivastava, and Brenden Kuerbis. 2021. A Fight Over Crumbs: The AFRINIC crisis. Retrieved May 13, 2025 from https://www.internetgovernance.org/2021/08/19/a-fight-over-crumbs-the-afrinic-crisis/

[39] RIPE NCC. 2023. *Routing Information System (RIS)*. https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris

[40] RIPE NCC. 2025. Index of /rpki/. Retrieved January 29, 2025 from https://ftp.ripe.net/rpki/

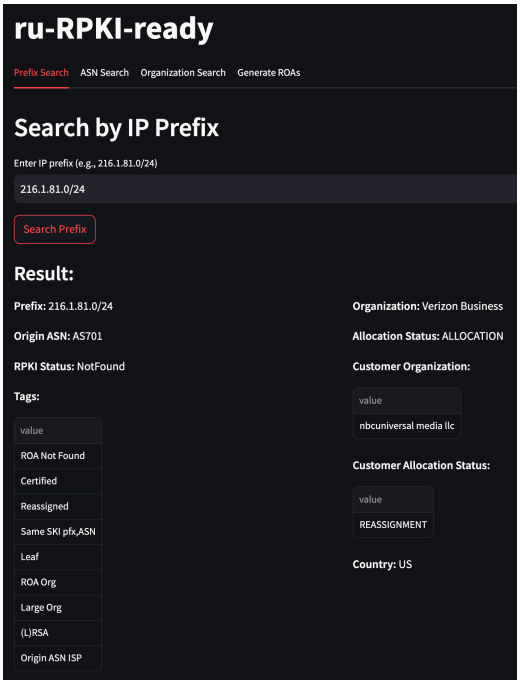


Figure 12: ru-RPKI-ready UI (search results for prefixes)

[41] RIPE NCC. 2025. Using the RPKI system. Retrieved April 29, 2025 from http://ripe.net/manage-ips-and-asns/resource-management/rpki/using-the-rpki-system/

[42] Lily H. Newman. 2018. Why Google Internet Traffic Rerouted Through China and Russia. https://www.wired.com/story/google-internet-traffic-china-russia-rerouted/.

[43] University of Oregon. 2022. *University of Oregon Route Views Project.* https://www.routeviews.org/routeviews/

[44] Leo Oliver, Gautam Akiwate, Matthew Luckie, Ben Du, and kc claffy. 2022. Stop, DROP, and ROA: effectiveness of defenses through the lens of DROP. In *Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22).* Association for Computing Machinery, New York, NY, USA, 730–737. https://doi.org/10.1145/3517745.3561454

[45] Pierluigi Paganini. 2017. BGP hijacking - Traffic for Google, Apple, Facebook, Microsoft and other tech giants routed through Russia. https://securityaffairs.co/wordpress/66838/hacking/bgp-hijacking-russia.html.

[46] Christina Paladeau. 2023. The Challenges of RPKI-ROA Diffusion in Research and Education. Retrieved April 29, 2025 from https://manrs.org/2023/11/the-challenges-of-rpki-roa-diffusion-in-research-and-education/

[47] PeeringDB. 2024. The Interconnection Database. Retrieved January 29, 2024 from https://www.peeringdb.com/

[48] Carlos Rodrigues and Vasilis Giotsas. 2022. Helping build a safer Internet by measuring BGP RPKI Route Origin Validation. https://blog.cloudflare.com/rpki-updates-data/.

[49] E.M. Rogers. 1962. *Diffusion of Innovations, 5th Edition.* Free Press. https://books.google.com/books?id=9U1K5LjUOwEC

[50] Jessica Rosenworcel. 2024. *FCC Chairwoman Proposes Internet Routing Security Reporting Requirements.* FCC. https://docs.fcc.gov/public/attachments/DOC-402579A1.pdf

[51] Sojun Ryu. 2022. Post Mortem of KlaySwap Incident through BGP Hijacking. https://medium.com/s2wblog/post-mortem-of-klayswap-incident-through-bgp-hijacking-en-3ed7e33de600.

[52] Khwaja Zubair Sediqi, Lars Prehn, and Oliver Gasser. 2022. Hyper-specific prefixes: gotta enjoy the little things in interdomain routing. *SIGCOMM Comput. Commun. Rev.* 52, 2 (jun 2022), 20–34. https://doi.org/10.1145/3544912.3544916

[53] Simon Sharwood. 2023. Africa's internet registry has sometimes needed financial assistance to keep operating, could fail, warns ARIN head. Retrieved May 13, 2025 from https://www.theregister.com/2023/02/22/afrinic_failure_warning_apnic_link/

[54] Job Snijders. 2023. RPKIViews. https://www.rpkiviews.org

[55] Job Snijders. 2024. War story: RPKI is working as intended. https://www.fastly.com/blog/war-story-rpki-is-working-as-intended.

[56] Forum Standaardisatie. 2023. Secured Internet routing of Dutch government by end of 2024. Retrieved January 28, 2024 from https://www.forumstandaardisatie.nl/nieuws/secured-internet-routing-dutch-government-end-2024

[57] Anton Strydom. 2024. *APNIC Products: 2023 in review.* APNIC. https://blog.apnic.net/2024/02/15/apnic-products-2023-in-review/ Accessed: 2025-09-22.

[58] Massimiliano Stucchi. 2022. RPKI Tutorial:MANRS RPKI Week. Retrieved January 23, 2024 from https://manrs.org/wp-content/uploads/2022/07/2022-07-04-RPKI-Week-Tutorial.pdf

[59] Cecilia Testart, Philipp Richter, Alistair King, Alberto Dainotti, and David Clark. 2020. To Filter or Not to Filter: Measuring the Benefits of Registering in the RPKI Today. In *Passive and Active Measurement (Lecture Notes in Computer Science)*, Anna Sperotto, Alberto Dainotti, and Burkhard Stiller (Eds.). Springer International Publishing, Cham, 71–87. https://doi.org/10.1007/978-3-030-44081-7_5

[60] Cecilia Testart, Josephine Wolff, Deepak Gouda, and Romain Fontugne. 2024. Identifying Current Barriers in RPKI Adoption. *SSRN Electronic Journal* (2024). https://doi.org/10.2139/ssrn.4948317

[61] Alfredo Verderosa. 2025. *MiLACNIC: Improvements in Resource Management and Security.* LACNIC. https://blog.lacnic.net/en/resource-management/ Accessed: 2025-09-22.

[62] Matthias Wählisch, Olaf Maennel, and Thomas C. Schmidt. 2012. Towards detecting BGP route hijacking using the RPKI. *ACM SIGCOMM Computer Communication Review* 42, 4 (Aug. 2012), 103–104. https://doi.org/10.1145/2377677.2377702

[63] Matthias Wählisch, Robert Schmidt, Thomas C. Schmidt, Olaf Maennel, Steve Uhlig, and Gareth Tyson. 2015. RiPKI: The Tragic Story of RPKI Deployment in the Web Ecosystem. In *Proceedings of the 14th ACM Workshop on Hot Topics in Networks (HotNets-XIV).* Association for Computing Machinery, New York, NY, USA, 1–7. https://doi.org/10.1145/2834050.2834102

[64] Zhiwei Yan, Randy Bush, Guanggang Geng, Ties de Kock, and Jiankang Yao. 2023. Avoiding Route Origin Authorizations (ROAs) Containing Multiple IP Prefixes. RFC 9455. https://doi.org/10.17487/RFC9455

[65] Christopher S. Yoo and David Wishnick. 2019. Lowering Legal Barriers to RPKI Adoption. *SSRN Electronic Journal* (2019). https://doi.org/10.2139/ssrn.3308619

[66] Marilyn Zhang. 2019. Advanced Routing and RPKI workshop at the MMIX 2019 Peering Forum. Retrieved January 23, 2024 from https://blog.apnic.net/2019/03/21/register-for-advanced-routing-and-rpki-workshop-at-the-mmix-2019-peering-forum/

[67] Maya Ziv, Liz Izhikevich, Kimberly Ruth, Katherine Izhikevich, and Zakir Durumeric. 2021. ASdb: a system for classifying owners of autonomous systems. In *Proceedings of the 21st ACM Internet Measurement Conference* (Virtual Event) *(IMC '21).* Association for Computing Machinery, New York, NY, USA, 703–719. https://doi.org/10.1145/3487552.3487853

A Ethics

This work does not raise any ethical concerns.

B Appendix

B.1 `ru-RPKI-ready` User-Interface

The current user interface of `ru-RPKI-ready` consists of four tabs that allow users to search for specific IPv4 or IPv6 prefixes, ASNs that originate prefixes in BGP, organizations that hold address space, and a list of ROAs that need to be created to secure a prefix with a covering ROA.

For each prefix, we provide information on the Direct Owner, Delegated Customers, Origin ASN(s), and a list of tags generated by the platform. For a given ASN, we offer details about the owning organization as well as the list of prefixes originated by that ASN and the ROA coverage for those prefixes. Additionally, we provide a list of organizations whose prefixes originate from the ASN. This data will be useful for studying the prefixes that the ASN originates, but cannot issue ROAs for. We also provide a "Generate ROA" page that lists a set of ROAs that must be created for a given prefix. The list should be followed serially to avoid the risk of invalidating routed sub-prefixes.

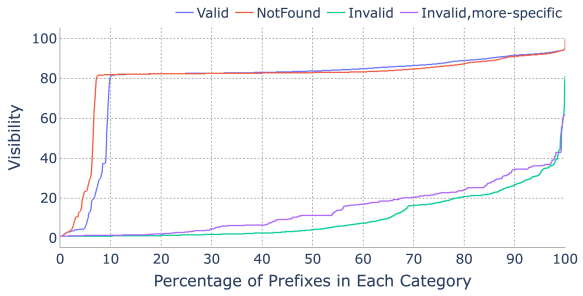


Figure 15: Visibility of routed IPv4 prefixes by RPKI status; RPKI Invalid prefixes have significantly lower visibility; Data: 1 April, 2025

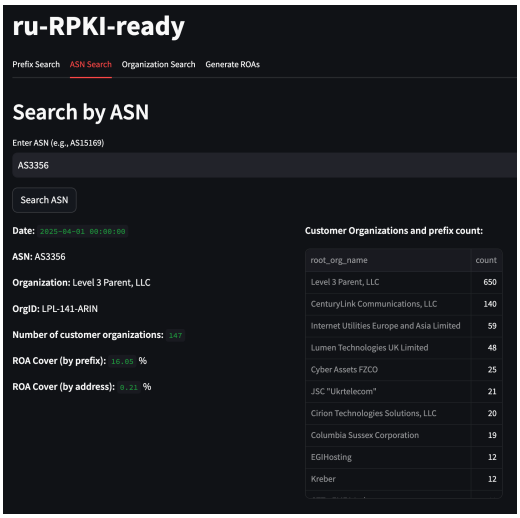


Figure 13: ru-RPKI-ready UI (search results for ASNs)

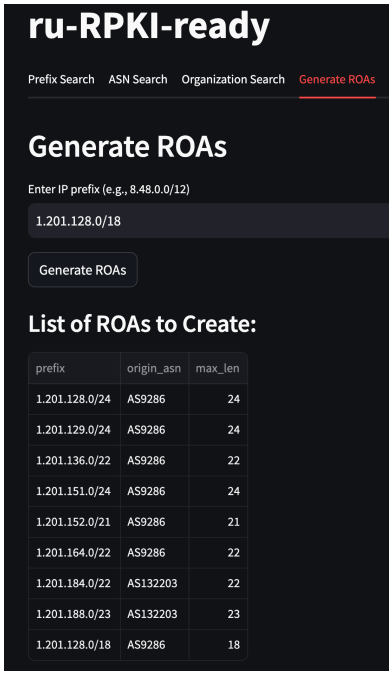


Figure 14: ru-RPKI-ready UI (generating ROA configurations)

B.2 ru-RPKI-ready Tags

In this section, we describe the tags assigned to prefixes and organizations in ru-RPKI-ready.

- **RPKI Valid/Not Found/Invalid/Invalid, more-specific:** The RPKI status of a prefix-origin pair.
- **(Non) RPKI-Activated Prefix:** Denotes if the prefix is (not) exclusively present in an RC owned by the RIR
- **Leaf Prefixes:** Prefixes that do not have a routed sub-prefix
- **Covering Prefixes:** Prefixes with a routed sub-prefix
- **Reassigned:** Address blocks in which a part or the complete address space has been reassigned or further sub-allocated to a customer
- **Internal/External Covering Prefixes:** Prefixes in which a routed sub-prefix is owned by the same organization or has been reassigned to a customer
- **Legacy:** The prefix is part of the legacy address space
- **(L)RSA/Non-(L)RSA:** Denotes if the prefix belongs to an organization that has signed an RSA or LRSA with ARIN for the address block
- **Large/Medium/Small Org:** An organization is categorized as *Large* if it is in the top 1 percentile of organizations in terms of the number of routed prefixes. If the organization is not in the top one percentile but owns more than one routed prefix, it is categorized as *Medium*. Organizations that own only one routed prefix are considered *Small* organizations.
- **Organization Aware:** The organization routed at least one directly-allocated ROA-covered address block in the past year
- **Same/Diff SKI (Prefix, Origin ASN):** Denotes if the prefix and ASN are present in the same RPKI Resource Certificate or different. Presence in the same certificate indicates that a single entity owns both the prefix and the origin ASN and hence has more control over the routing operations.

B.3 Impact of Route Origin Validation on the visibility of BGP prefixes

The RPKI status of a prefix has a significant impact on its global visibility. BGP origin hijacks or sub-prefix hijacks targeting ROA-covered prefixes result in the announcements becoming *RPKI Invalid*. The major transit providers deploying ROV drop these invalid announcements and limit their spread and impact, resulting in their low visibility. In Figure 15, we can observe that more than 90% of *RPKI-Valid* and *RPKI-Not Found* prefixes have a visibility of more than 80% *i.e.,* they are observed by more than 80% BGP route collectors. In contrast, less than 5% of the *RPKI-Invalid* prefixes have a visibility of more than 40%. Thus, the deployment of ROV among the large Tier-1 networks has s significant impact on the propagation of *RPKI-Invalid* prefixes.