

# The Threat Landscape of IP Leasing in the RPKI Era

Weitong Li, Yongzhe Xu, and Tijay Chung  
Virginia Tech

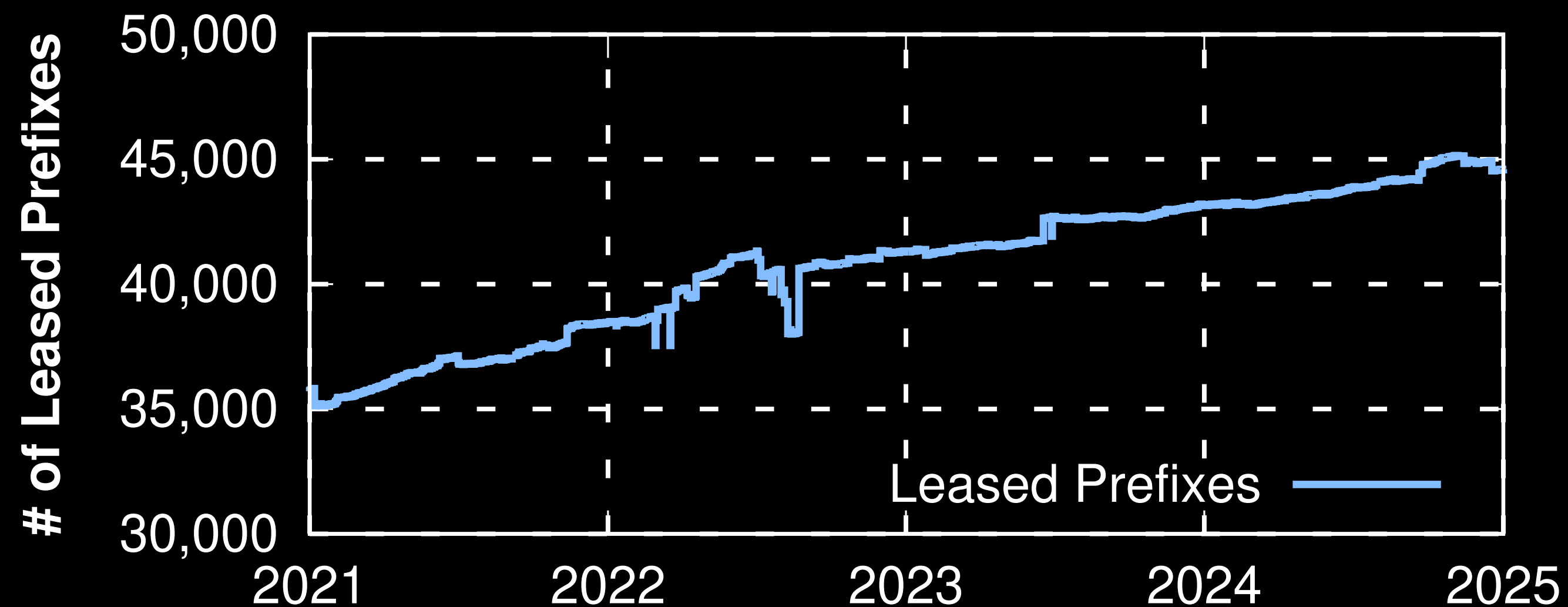
Paper accepted to Oakland'26

# The Raise of IP Leasing

- Due to the shortage of IPv4 spaces, people turn to lease IP spaces for their business.
- The leasing could go through “leasing brokers”, or directly between lessors and lessees.
- There’s no transit services between lessor, lessee, and brokers.

# The Raise of IP Leasing

- Based on the methodology of previous method [1], we exam Whois and IRR to obtain the number of leased IP spaces.
- The Number of leased prefixes raise from 35K to 45K in past 4 years.



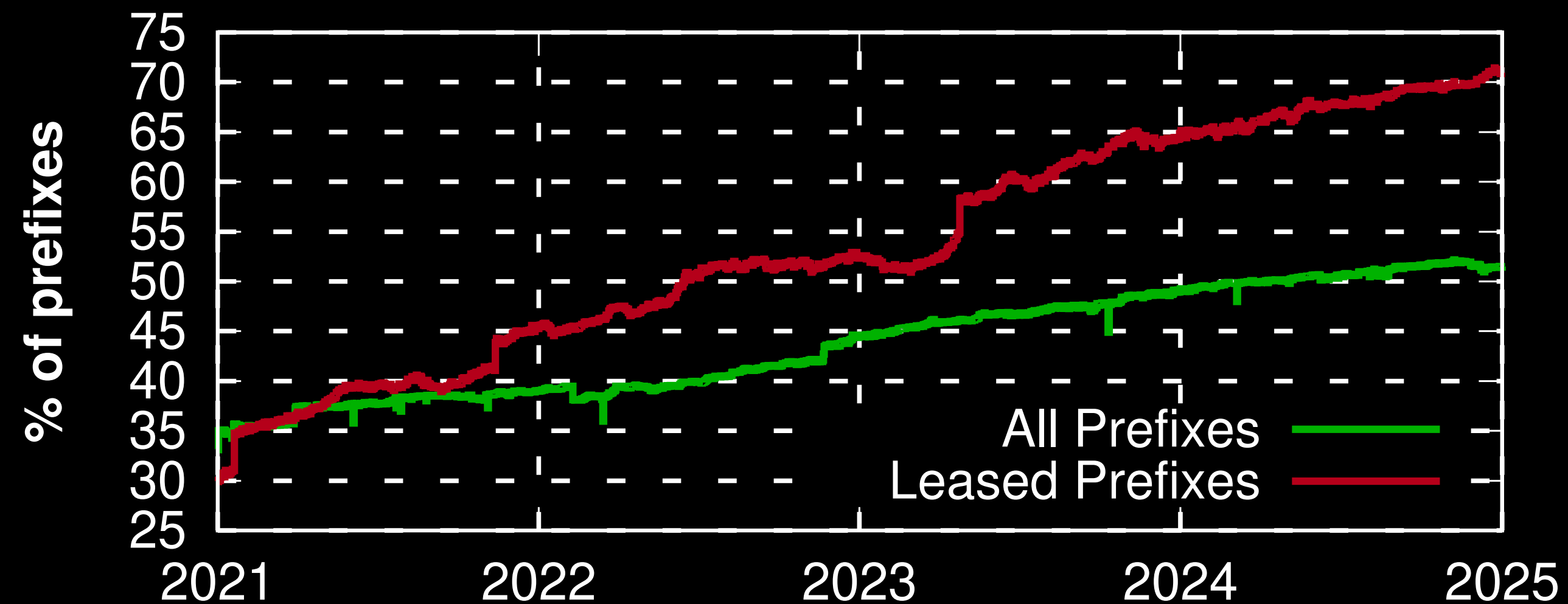
[1] IMC'24 Du, et. al , Sublet Your Subnet: Inferring IP Leasing in the Wild.

# The Deployment of RPKI

- The Resource Public Key Infrastructure (RPKI) is introduced to secure BGP and prevent origin hijack.
- To deploy RPKI:
  1. Resource holders **register ROA** certificates which list IP prefixes and ASNs authorized to announce.
  2. ISPs do Route **Origin Validation (ROV) to filter** BGP announcements where the origin ASN does not match with ROA origin for that prefix.

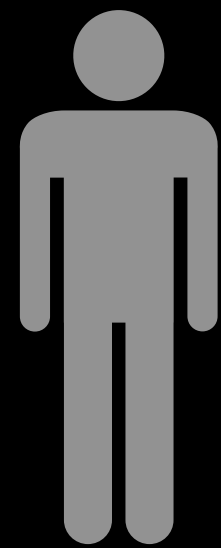
# The Deployment of RPKI

- Overall ROA coverage on IPv4 is over 50%.
- Leased prefixes are more likely to have ROAs.



# ROA Management

Resource Owner  
Registered in RIRs



ACCOUNT MANAGER RPKI: ROAs

Org ID: ARINL Hosted RPKI: Overview ROAs Certified Resources IRR Auto-Manager

The Org ID has the following Route Origin Authorizations (ROAs) in ARIN's RPKI Repository.

Route Origin Authorizations

Filter ROAs by Origin AS or Prefix.

Resource:  Search ROAs

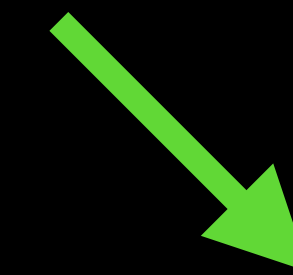
Example: AS64496 or 64496, 2001:DB8::/48 or 192.0.0.0/24

Create ROA

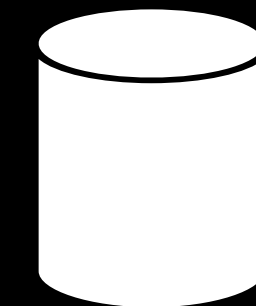
Origin AS	Prefixes	ROA Name
None found		

A Route Origin Authorization (ROA) is a cryptographically signed object, made by the authenticated resource holder, that states the authorized Origin ASN for a prefix or set of prefixes.

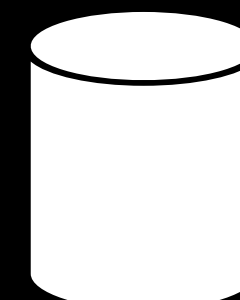
ARIN auto-renews ROAs created using the Hosted RPKI service so that they persist until manually deleted.



RIR's public repos



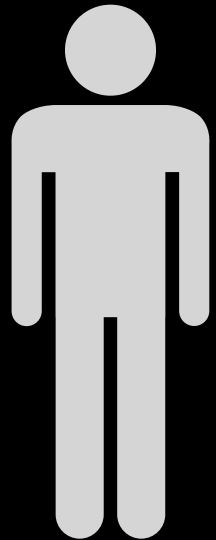
Own RPKI publication points



# ROA during IP Leasing

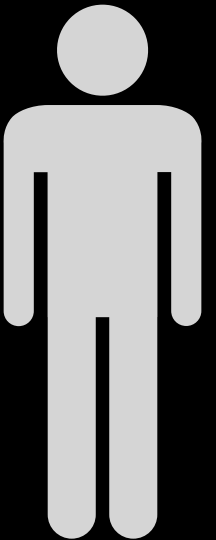
Resource Owner  
Registered in RIRs

45.3.0.0/20, AS 4385



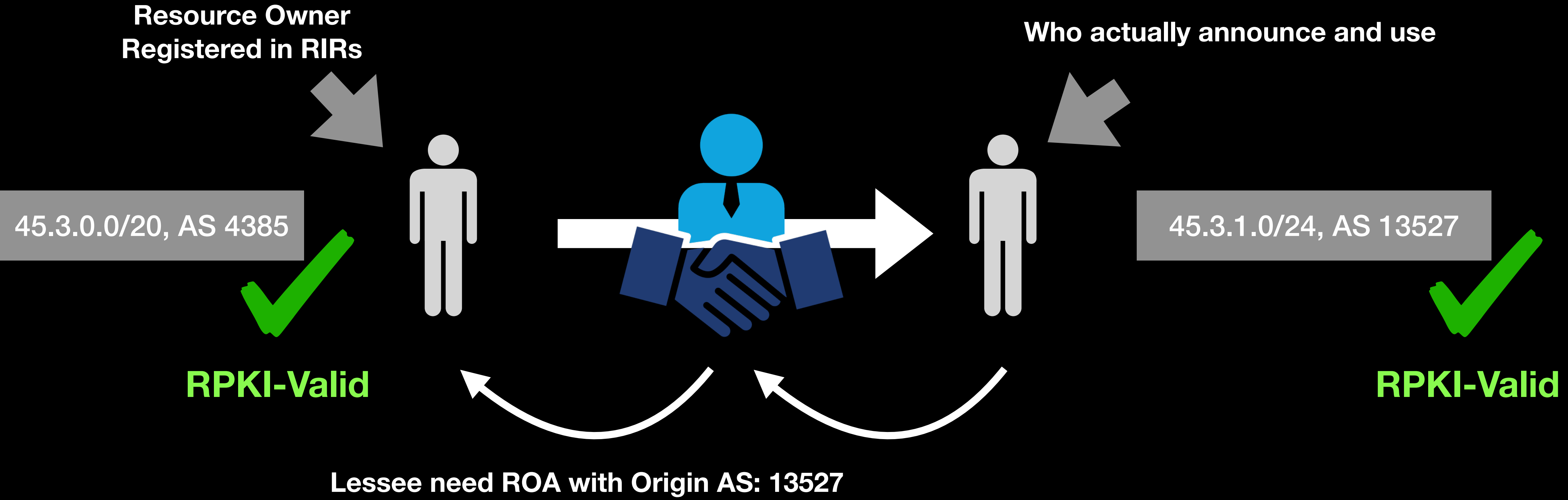
Who actually announce and use

45.3.1.0/24, AS 13527



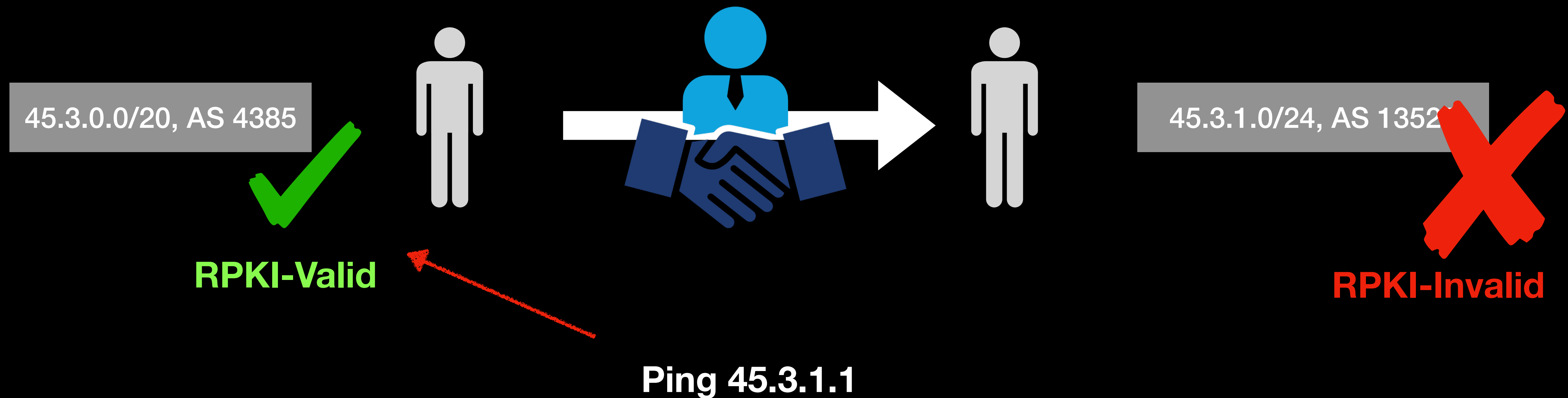
The screenshot shows the ARIN RPKI: ROAs interface. It includes a sidebar with navigation options like Dashboard, Tickets, Your Records, IP Addresses, ASNs, Routing Security, Transfer Resources, Payments & Billing, Downloads & Services, and Ask ARIN. The main content area is titled 'RPKI: ROAs' and shows a search filter for 'Resource' with a 'Search ROAs' button. Below the search area is a table with columns for 'Origin AS', 'Prefixes', and 'ROA Name', which currently shows 'None found'. A 'Create ROA' button is visible at the bottom right of the table area.

# ROA during IP Leasing



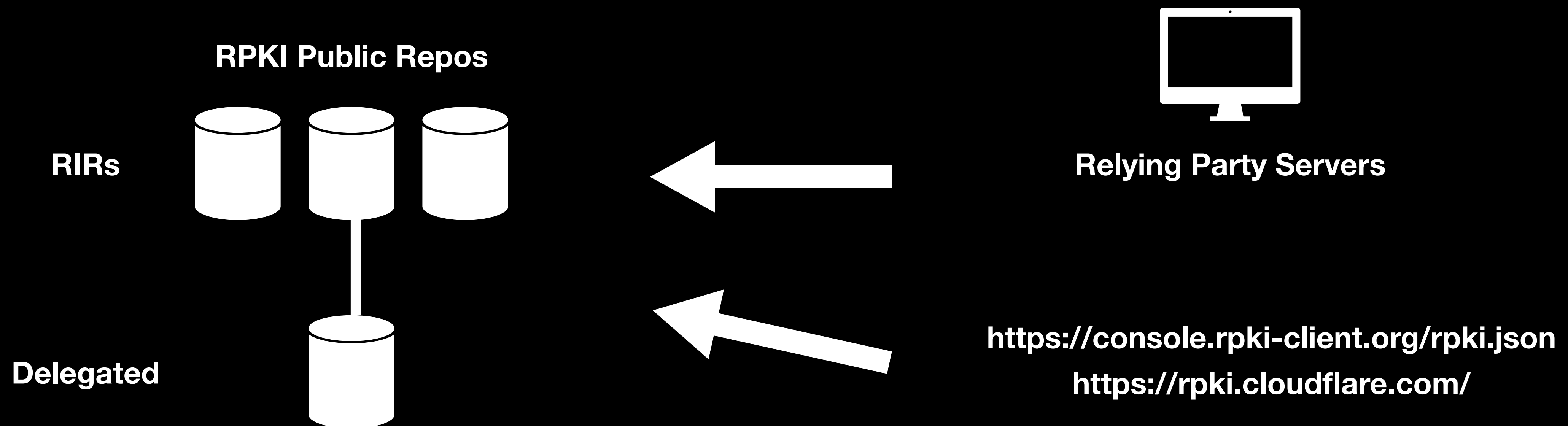
# Threat: A Rouge Lessor

- If the lessor forget (or **intentionally not**) to configure ROA for lessee, lessee's announcement will be filtered from ROV networks.
- And traffic will re-route to lessor with less-specific prefixes.



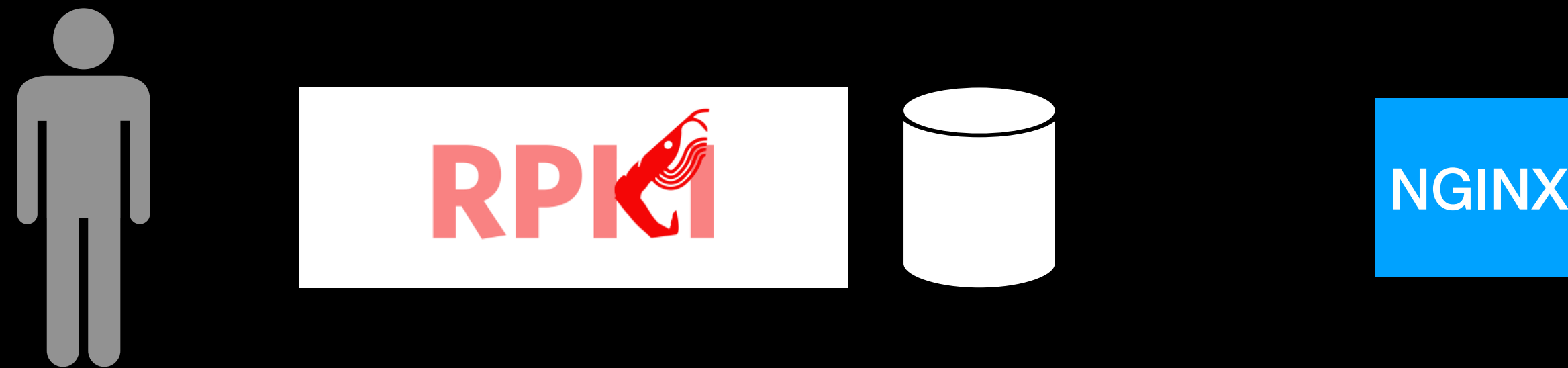
# ROA Monitoring

- Due to the threat, brokers and lessees need to keep monitoring ROAs, whether deploy validation servers themselves or checking public servers regularly.



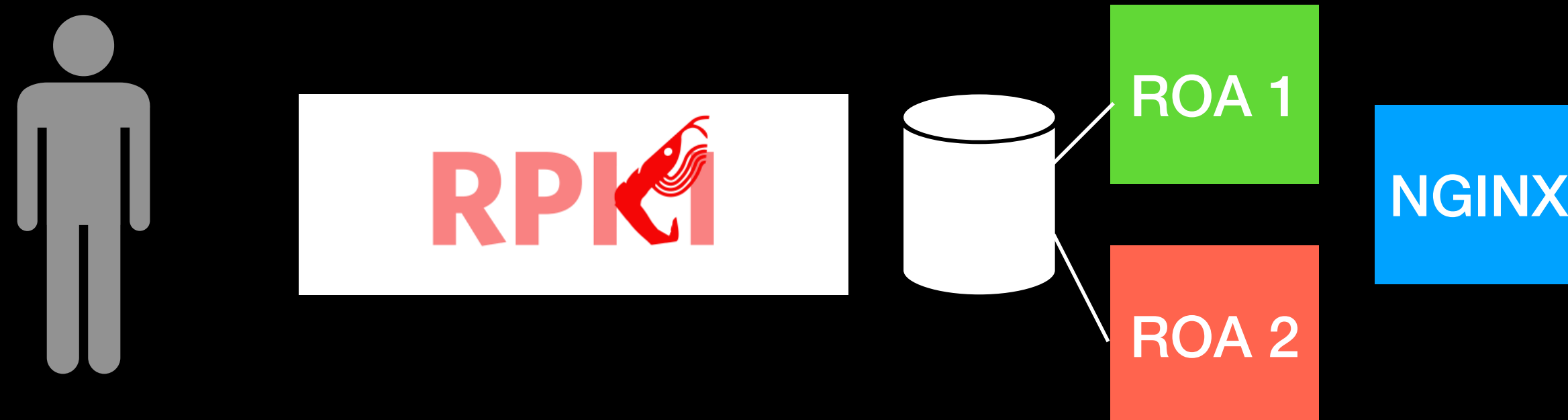
# Evade ROA Monitoring

- However, ROA is not always globally consistent.
- When the rogue lessor deploy its own publication point server, the lessor can present different files to different validators.

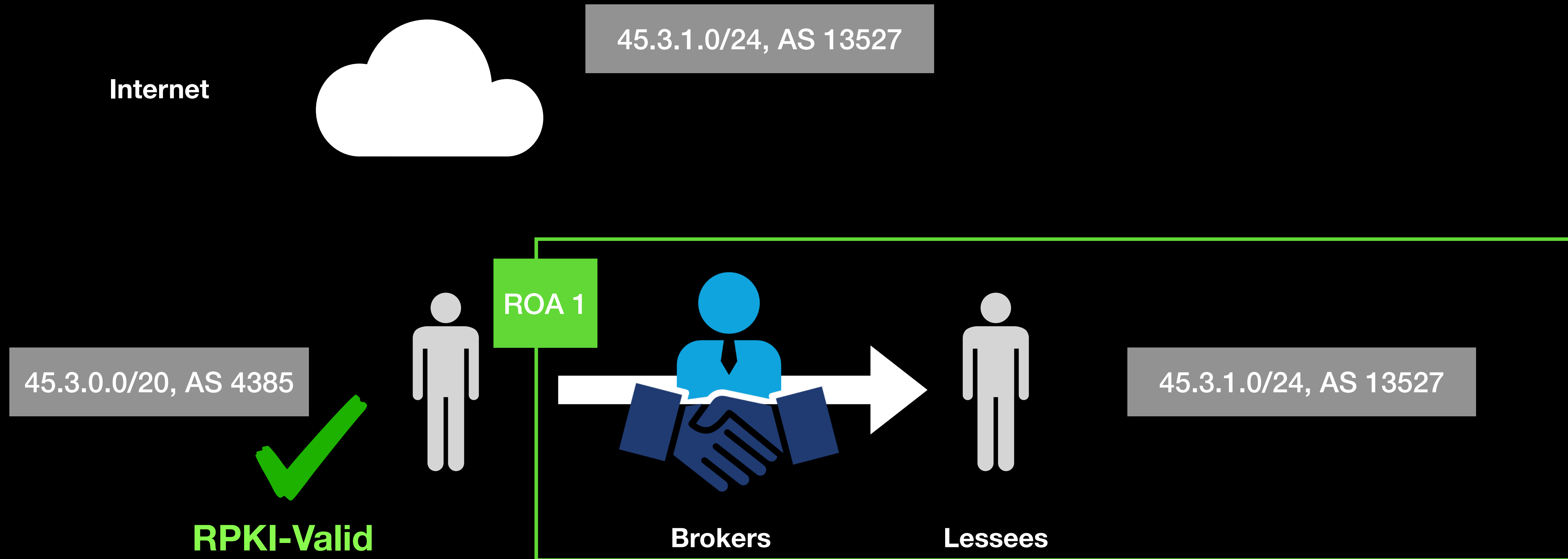


# Evade ROA Monitoring

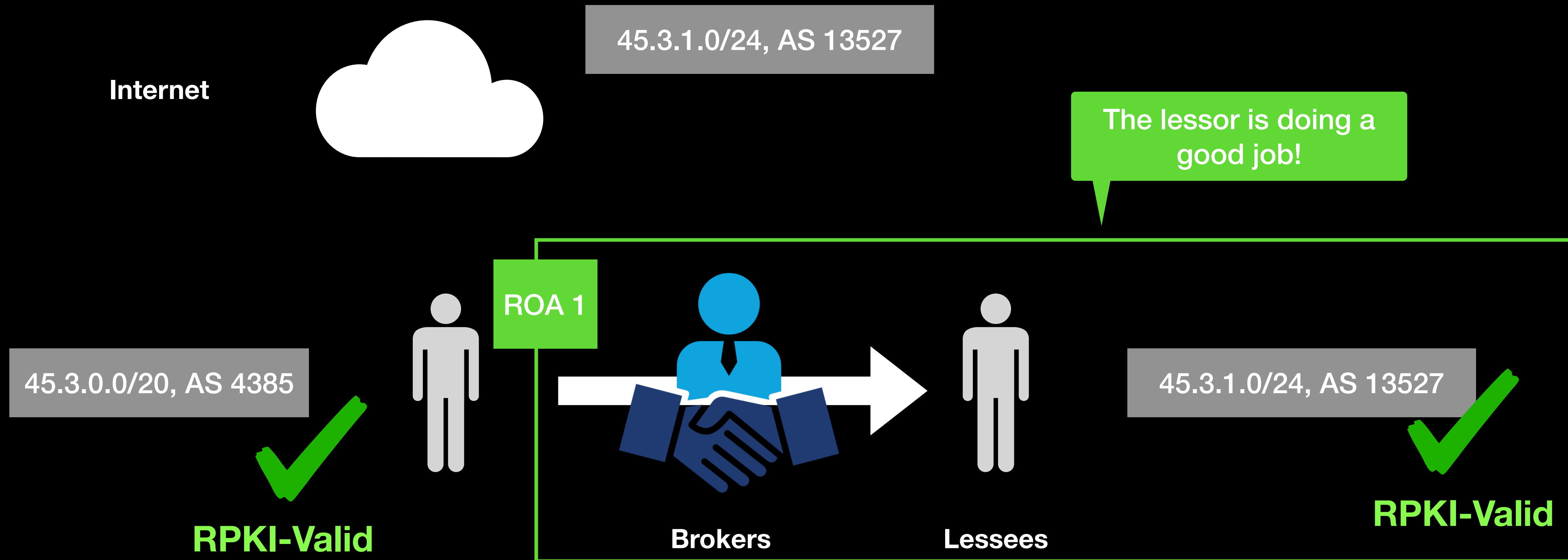
- However, ROA is not always globally consistent.
- When the rogue lessor deploy its own publication point server, the lessor can present different files to different validators.



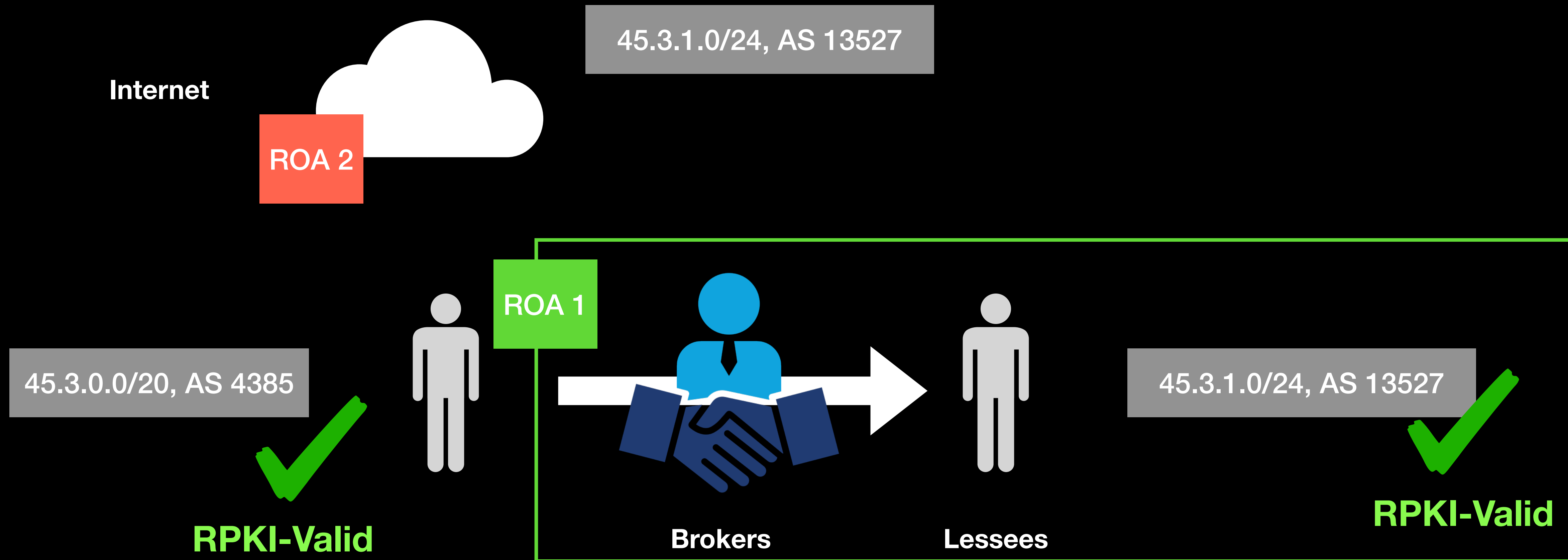
# Evade ROA Monitoring



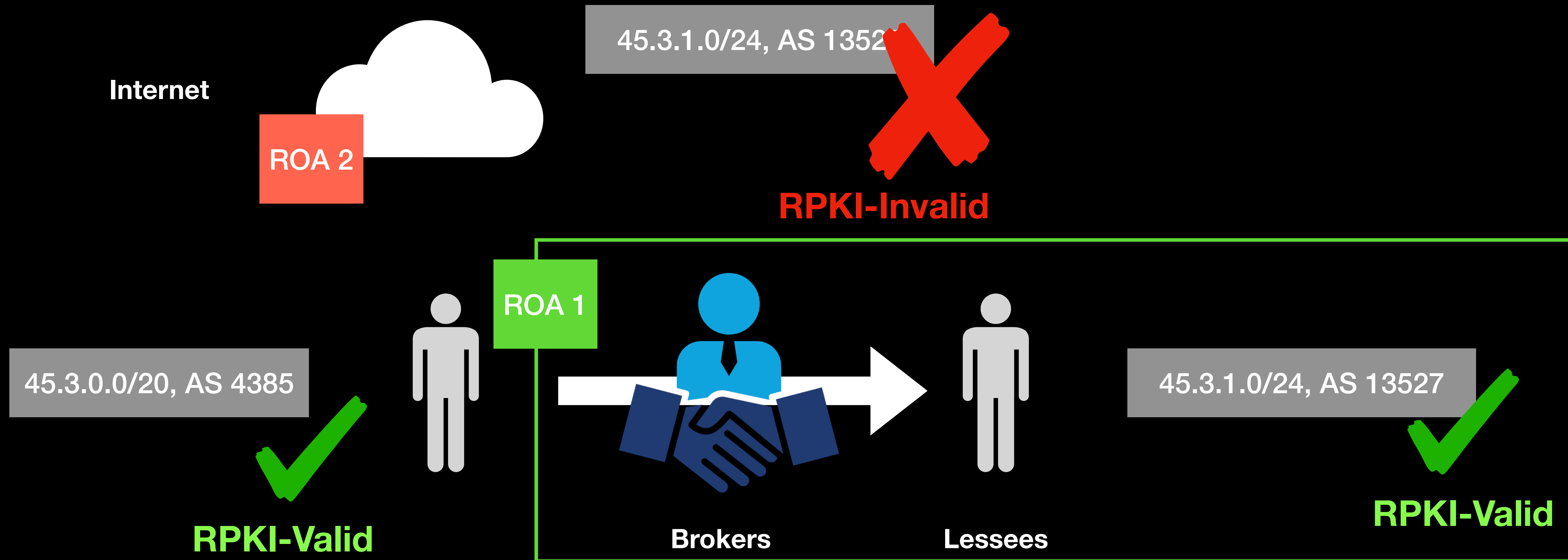
# Evade ROA Monitoring



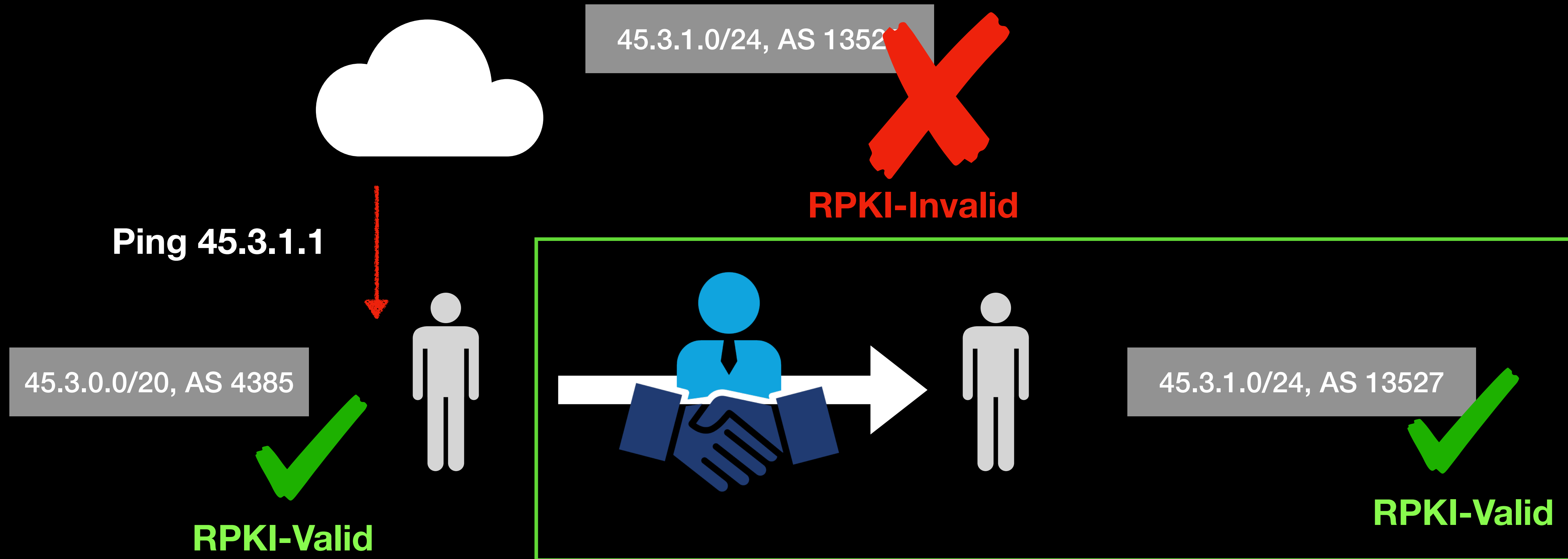
# Evade ROA Monitoring



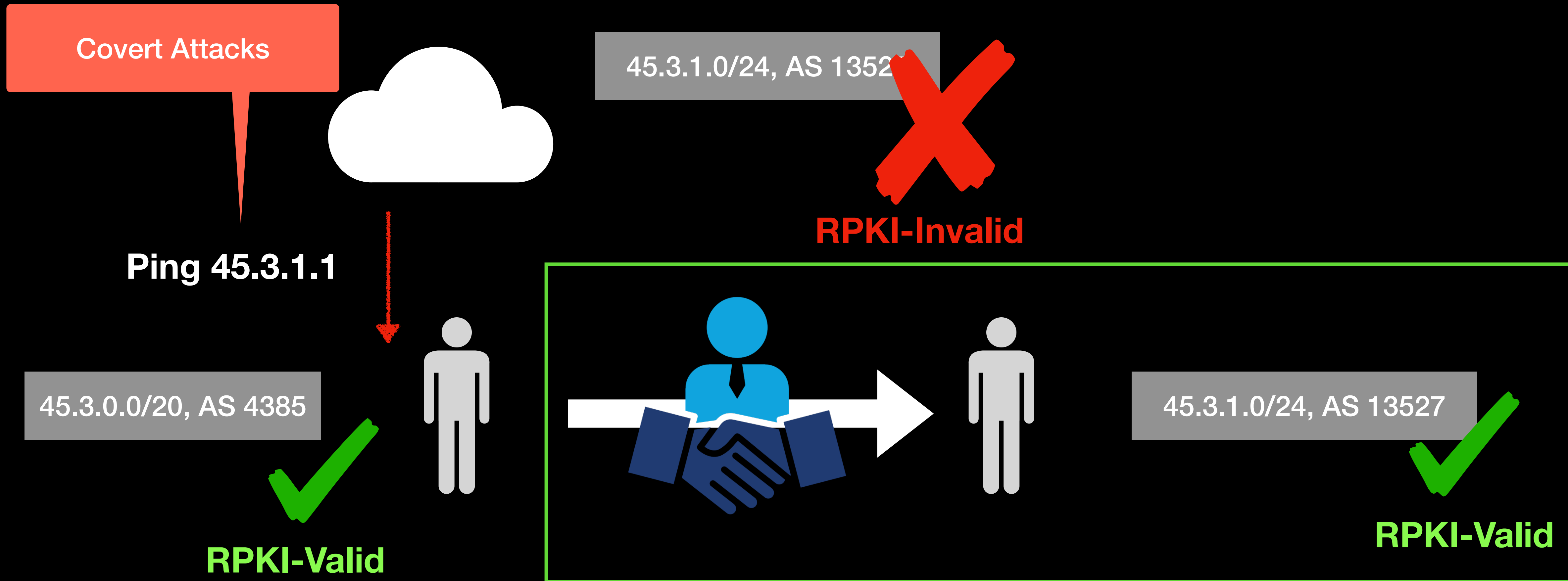
# Evade ROA Monitoring



# Evade ROA Monitoring



# Evade ROA Monitoring

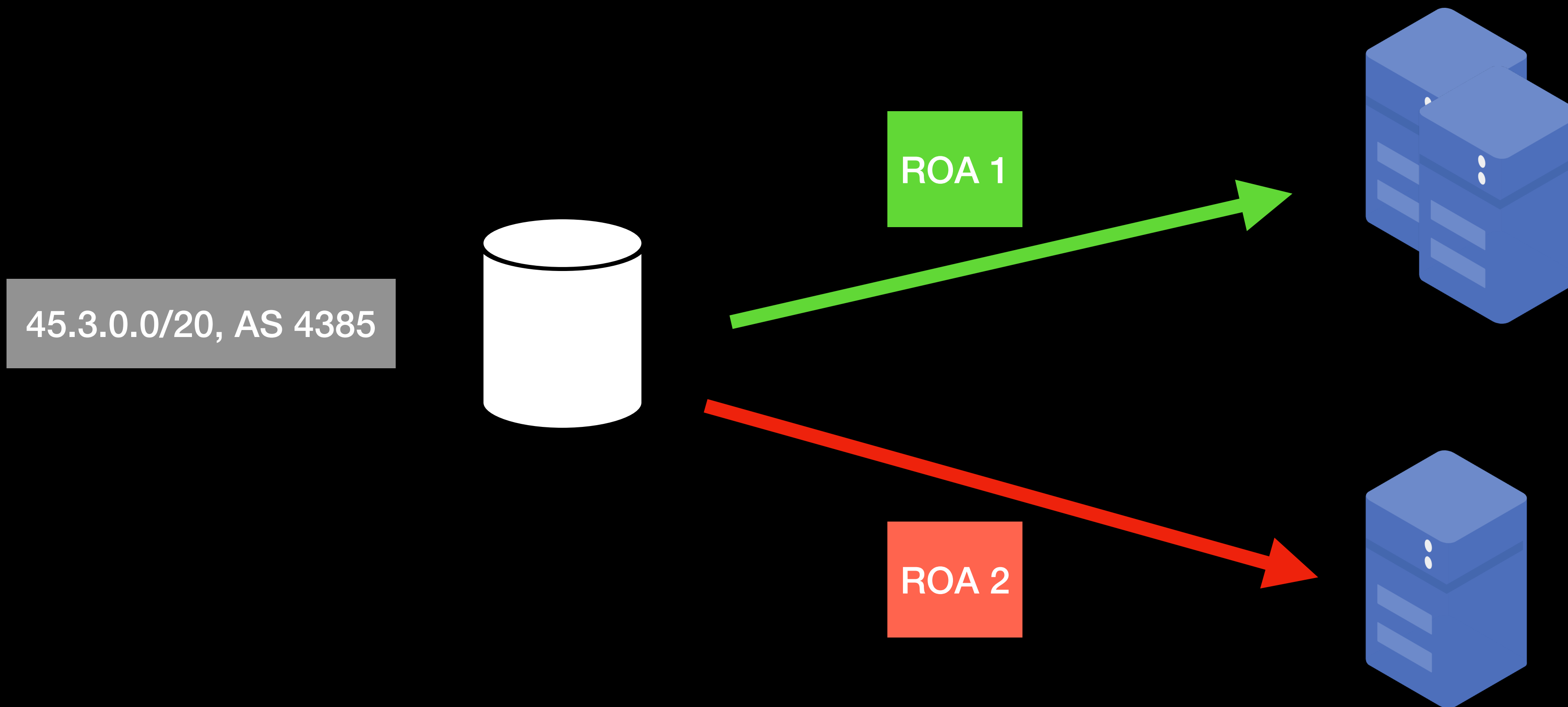


# Identify the Validators

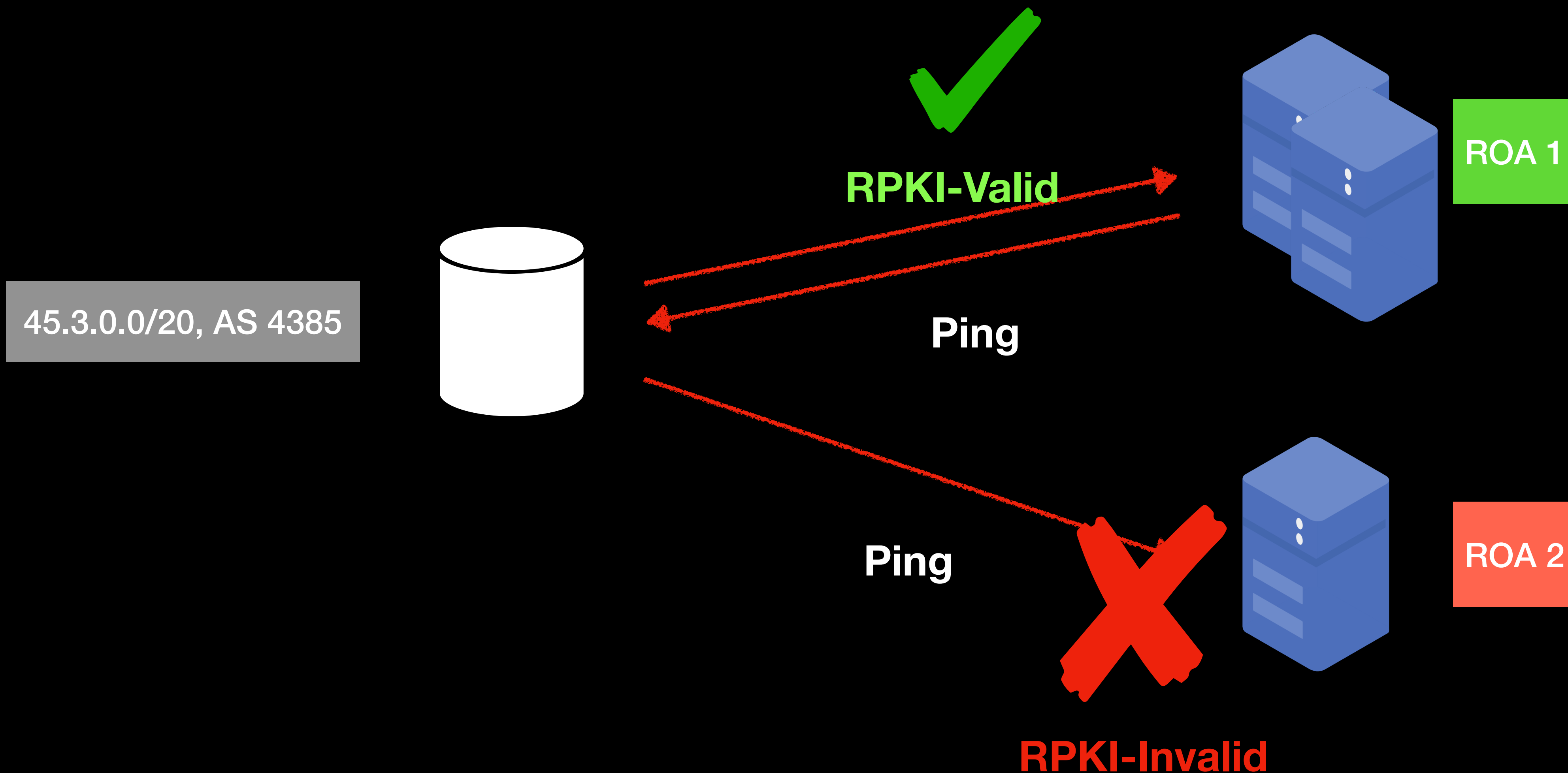
To evade ROA monitoring, the attackers need to locate the validators (RPs) brokers and lessees use.

- Most network operators host their validators inside their networks.
- Validators can be mapped by data-plane ping, fingerprint with RRDP serial numbers.

# Mapping the Validators



# Mapping the Validators



# Real-world Testing

- We set up our own publication points, hijack our prefixes using AWS/Vultr/Peering Testbed networks.
- We simulate the covert hijack, giving lease-compliant ROAs to brokers and public RPs.
- Average hijack success rate for covert hijack is **80.7%**.
- Successfully obtain a TLS certs from Let's Encrypt ACME **without hijacking any other networks.**

# Vulnerable Prefixes

To be vulnerable, the prefix need to be:

- Under leased
- Lessor still obtain control over ROA (specific RIRs allow ROA access delegation, but are raw in deployment)

34,618 out of 44,591 leased prefixes (76.6%) remain at risk, 1,392 (4.0%) prefixes are RPKI-invalid right now!

# Mitigations

- Short-term: Monitoring ROA from different vantage points, check consistent using tools like RTRmon
- Anomaly validators against fingerprint: Erik protocol [2] (draft in sidrops)
- Introduce partial delegations for ROA access in RIRs, allow lessor to give ROA access to lessee and brokers for only the prefixes under leasing.

[2] The Erik Synchronization Protocol for use with the Resource Public Key Infrastructure (RPKI)

**Thanks!**