Diverging Branches : How different are RPKI Trees across RIRs?

Deepak Gouda Cecilia Testart

Georgia Institute of Technology

Introduction

Motivation :

- Network operators are increasingly relying on RPKI for route validation
- Each RIR independently implements its RPKI infrastructure
- Individual design decisions impact the entire ecosystem

Objective : Study the different designs of RPKI infrastructure across the five RIRs. How these differences impact the RPKI Certificate repository?

Key finding : Some RPKI repositories are more scalable and computationally efficient than others by design.

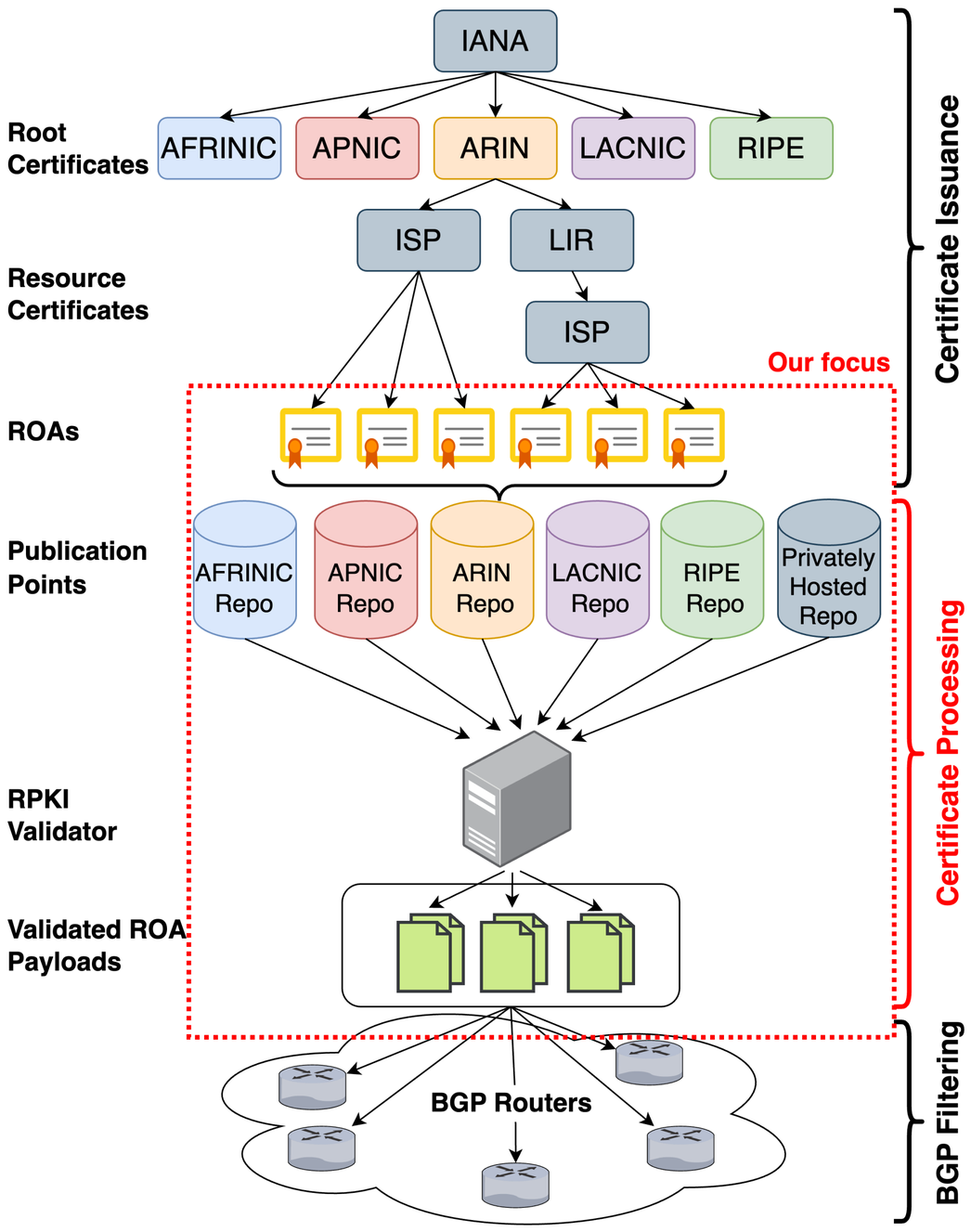

Figure 1. RPKI Certificate issuance & validation mechanism. Diagram similar to Fig 2. [2]

X.509 Resource Certificate

File:	0153231e-bade-4c05-b3fd-55b65671daae.cer
Subject key identifier:	B9:A6:5D:CA:07:55:7E:11:15:64:29:15:E9:88:...
Authority key identifier:	7C:7A:F7:9C:7A:DF:7C:4B:E8:CE:A8:54:6D:F3...
Certificate not before:	Thu 03 Oct 2024 18:54:20 +0000
Certificate not after:	Fri 12 Dec 2025 01:45:22 +0000
Subordinate resources:	AS: 11070
	IP: 107.182.0.0/20
	IP: 140.235.84.0/22

- **Authority Key Identifier (AKI)** : Public key corresponding to the private key of the authority signing the certificate
- **Subject Key Identifier (SKI)** : Public key corresponding to the private key of the current certificate

AKI and SKI values can be chained together to form the RPKI Certificate issuance tree. Trees of each RIR are shown in Fig 2.

Key Metrics

	AFRINIC	APNIC	ARIN	LACNIC	RIPE
Num ROAs	7,678	30,308	145,536	27,674	45,638
Mean ROA size	1,937	1,908	2,118	1,953	1,873
CRL size	6,252	112,478	88,099	28,341	97,199
μ(Num ROAs per RC)	9.84	3.47	31.89	5.19	2.83
μ(Num VRPs per ROA)	1.34	4.37	1.14	1.26	5.72
Num BGP prefixes	19,369	170,155	119,124	113,186	242,236

Table 1. Key metrics of five RPKI repositories; μ refers to mean; *ROA file size is in bytes

Key Factors

- **Length of signature chains** : Longer signature chain ⇒ more computational complexity
- **Number of files in RPKI repository** : More files ⇒ more computational complexity
- **Delegated CAs** : Publication point is unavailable ⇒ RPKI validators face delays in fetching and validating certificates

Observations

- **Signature Chains** - longest in APNIC, LACNIC; shortest in AFRINIC
- **Number of certificate objects** - highest in ARIN, highest mean file size
- **Delegated CAs** - exist only in APNIC, ARIN, RIPE
- **ARIN** - issues new ROAs for almost every prefix-origin pair, leading to large number of ROAs which require more storage and computation
- **RIPE and APNIC** - pack more VRPs into one ROA, effectively reducing the number of files that need to be processed
- **RIPE and APNIC repositories** - more scalable and efficient at the cost of higher number of certificate revocations

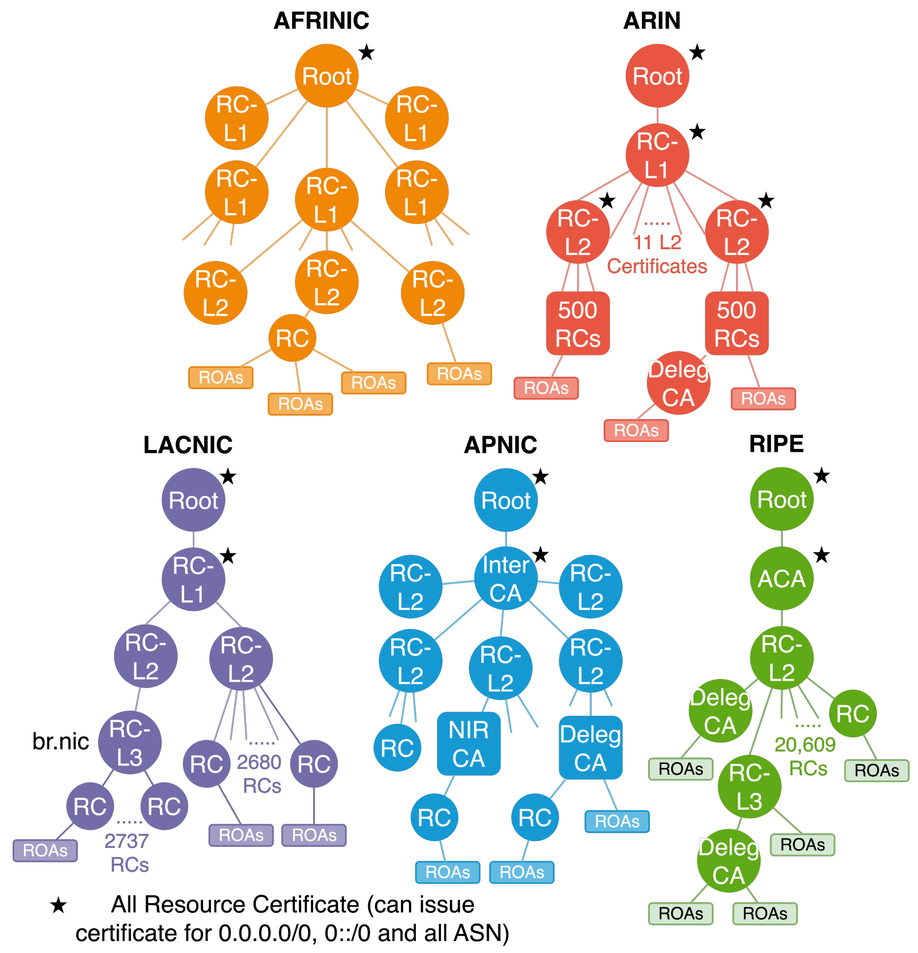

Figure 2. RPKI structure of the five RIRs

References

[1] Kristaps Dzonsons; Claudio Jeker; Job Snijders; Theo de Raadt; Sebastian Benoit; and Theo Buehler. rpki-client, Aug 2024.

[2] Nils Rodday, Ítalo Cunha, Randy Bush, Ethan Katz-Bassett, Gabi Dreo Rodosek, Thomas C. Schmidt, and Matthias Wählisch. The resource public key infrastructure (rpki): A survey on measurements and future prospects. *IEEE Transactions on Network and Service Management*, 21(2):2353–2373, 2024.