Building a Routing Security Culture

RPKI and ROAs for Network Operators and Enterprise Networks in Nigeria

Ololade Iyowu | Equinix
Nigerian Peering & Interconnection Forum 2026

Why RPKI: BGP trusts by default

- Any network can announce any prefix, and neighbors generally accept it
- Mistakes and malicious hijacks reroute, slow down, or blackhole traffic
- Example: in 2008 a routing mistake by one ISP took YouTube offline for much of the world for a short time
- Nigerian banks, ISPs, and services depend on routes being correct

It happened here: early 2026

A real incident involving a customer in Nigeria



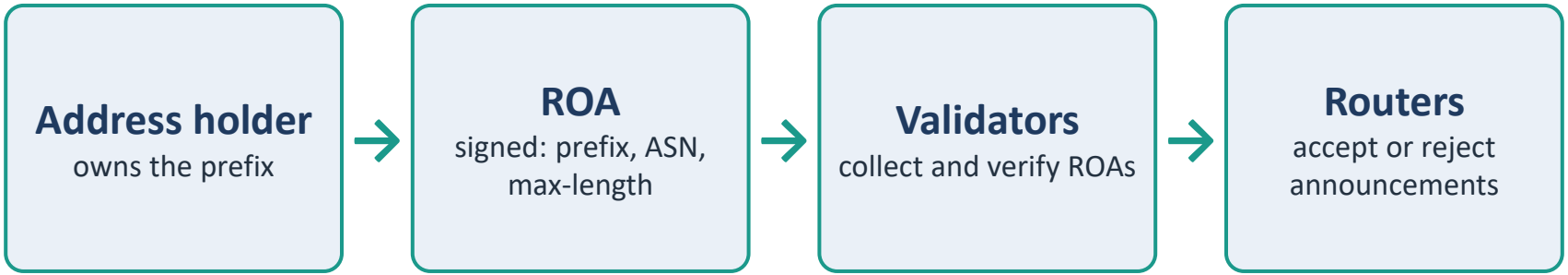
Result: the Nigerian customer lost access to Microsoft services for a few hours.

The cause was a routing announcement, not a fault in Microsoft's service. The most specific route wins, and nothing checked who was allowed to announce it.

What would have helped: a ROA with a matching max-length. A more specific announcement from another network is then invalid, and networks that validate can reject it.

What is RPKI?

- RPKI (Resource Public Key Infrastructure) is run through the Regional Internet Registries
- A ROA (Route Origin Authorization) is the signed record that says who may originate your prefix
- ROV (Route Origin Validation) is when a network checks each route against the ROAs and drops the invalid ones



How a router checks a route: three results

Valid

A ROA matches: right AS number, and the prefix is no longer than the max-length.

What happens: Accepted

Example: AS64496 announces 192.0.2.0/24 and the ROA says exactly that.

Invalid

A ROA covers the prefix, but the announcement does not match it.

What happens: Dropped by networks that validate (ROV)

Example: Another AS announces it, or a longer prefix than the max-length.

Not found

No ROA covers the prefix, so the router cannot tell either way. Some tools may also call this 'unknown'.

What happens: Usually accepted, with no protection

Example: The owner never created a ROA. This is the biggest gap in Nigeria.

What does RPKI helps with?

ROAs: who may originate a prefix

- Stop accidental origin hijacks
- Make many malicious hijacks easier to reject
- Prove you hold your prefixes

ASPA: who may be in the path

- Path validation is done by ASPA (Autonomous System Provider Authorization)
- A network publishes a signed list of its allowed upstream providers
- Helps catch route leaks and unauthorized paths

How they relate: ASPA is built on RPKI. It uses the same certificates, registry portals and validators, so ROAs come first and ASPA adds path checks on top. ASPA adoption is still early.

Neither encrypts traffic, and neither protects you from networks that do not sign or validate.

RPKI adoption in Nigeria: where we stand

56%
of prefixes have a valid ROA
Cloudflare Radar

44%
of prefixes have no ROA ('not found')
Cloudflare Radar

2
RPKI-invalid prefixes visible (0.06%)
Cloudflare Radar, MANRS

38–43%
of IPv6 prefixes covered by ROAs
Cloudflare Radar 38%; Internet Society Pulse 43%*

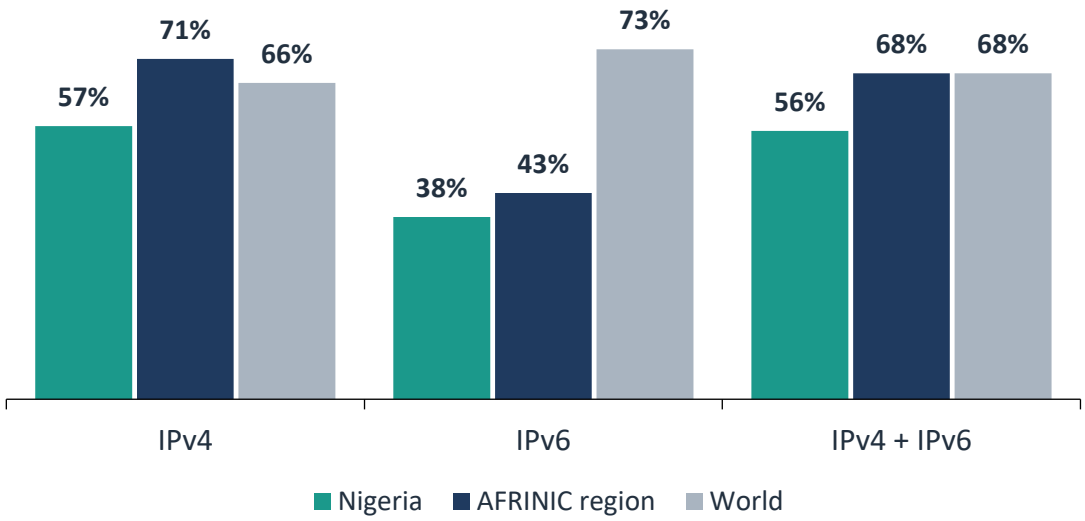
3–5%
of networks validate routes (ROV)
MANRS Observatory 3%; Internet Society Pulse 5%

Few invalid routes, many prefixes with no ROA, very little validation.

Sources: Cloudflare Radar, RPKI in Nigeria (13 Oct 2026): Announced prefixes from ASes registered in Nigeria; 3,301 IPv4 and 165 IPv6 prefixes.
38% is calculated from Cloudflare's counts (63 of 165 IPv6 prefixes).
MANRS Observatory (Oct 2026) and Internet Society Pulse, Nigeria (2026) measure the share of networks that validate; their methods differ, so the two ROV figures are shown separately.

Nigeria vs the AFRINIC region and the world

Share of routed prefixes covered by a valid ROA, 13 October 2026



What this shows

Nigeria is behind both the AFRINIC region and the world on IPv4 and overall.

IPv6 coverage is lower than IPv4 in Nigeria (38%) and across the AFRINIC region (43%), while worldwide it is higher (73%).

Route validation (ROV) is a separate measure and is much lower: 3% of Nigerian networks per MANRS, 5% per Internet Society Pulse.

Sources (13 Oct 2026): Nigeria: Cloudflare Radar, shares calculated from its prefix counts. AFRINIC region and world: Hurricane Electric RPKI & ASPA report, rounded to whole numbers. The AFRINIC region also covers Indian Ocean countries.
The two sources use different methods, so treat the comparison is seen as indicative.
ROV: MANRS Observatory and Internet Society Pulse (Nigeria only).

Large transit providers already filter invalid routes

Large backbones reject RPKI-invalid routes, and more are joining

Some tier 1 networks and large transit providers reported as rejecting RPKI-invalid routes

GTT	Arelion (Telia)	Telstra
NTT	Lumen	Orange
PCCW	AT&T	Sparkle (Feb 2026)

What it means for Nigerian networks

An invalid route can be dropped by the largest backbones, so it may not reach parts of the internet.

Kentik's analysis found that invalid routes rarely reach more than half the vantage points that valid routes do.

A wrong ROA now has a real cost, and no ROA means no protection.

Get your ROAs created and correct before your upstreams enforce.

Sources: Kentik blog posts on RPKI ROV (named providers, propagation analysis); Cloudflare, "Is BGP safe yet?" (Sparkle, Feb 2026); AT&T announcement on NANOG (2019). Provider policies change. This list is not exhaustive, check each provider's current policy

Reasons to deploy RPKI

- Protect your own prefixes and your customers from hijacks
- Protect your reputation and service availability
- Make your routes verifiable to every network that validates
- Meet growing expectations from upstreams, peers, and exchanges
- Low cost, small effort, no new hardware to start

Implementing: what to prepare

- List your prefixes and the ASN that originates each one
- Confirm access to your RIR portal and the right account
- Decide max-length to match what you actually announce
- Check live announcements first, so you do not invalidate real routes
- Use a public validator or looking glass to check the result

Registering a ROA, step by step

1. Log in to your RIR portal and enable RPKI
2. Create a ROA: prefix, origin ASN, max-length
3. Publish and allow time to propagate
4. Verify with a public validator
5. Monitor and review on a schedule

Portal steps 1–2: Get set up

Example: AFRINIC portal

STEP 1

Request a BPKI certificate

Go to my.afrinic.net and sign in. Navigate to “My Account > BPKI” for the requirements to approve BPKI.

If you are an administrative contact, send details to service-support@afrinic.net.

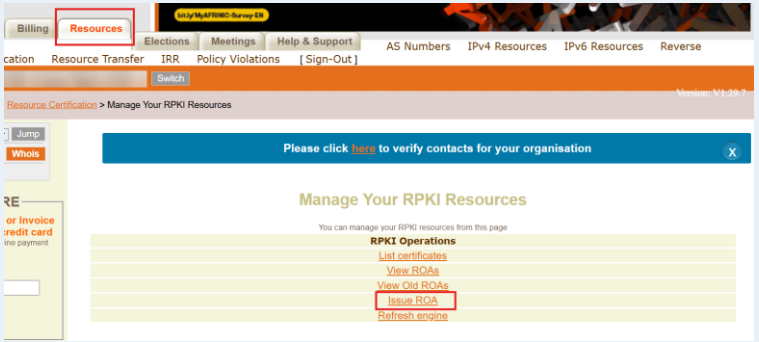
Skip this step if you already have a BPKI certificate.



STEP 2

Navigate to Resource Certification

From the main menu: Resources → Resource Certification → Issue ROAs.

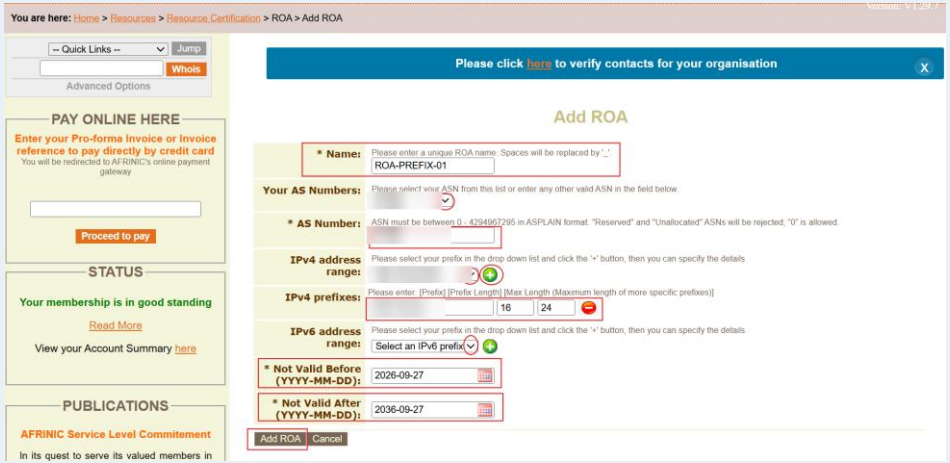


Portal step 3: Fill in the ROA form

Example: AFRINIC portal

STEP 3

Fill in the ROA form



ROA name

Any label unique to you. For your own reference, not used in routing.

Origin ASN

The ASN you hold or are authorized to sign for.

Prefix (IPv4/IPv6)

Must match what the registry has registered to you.

Max length

Keep equal to the prefix length unless you truly announce smaller sub-prefixes.

Validity dates

Set an end date and add a calendar reminder to renew.

Portal steps 4–5: Add the ROA and verify it

Example: AFRINIC portal

STEP 4

Add the ROA

Once the ASN, prefix, max length and validity dates are filled in, click “Add ROA.”

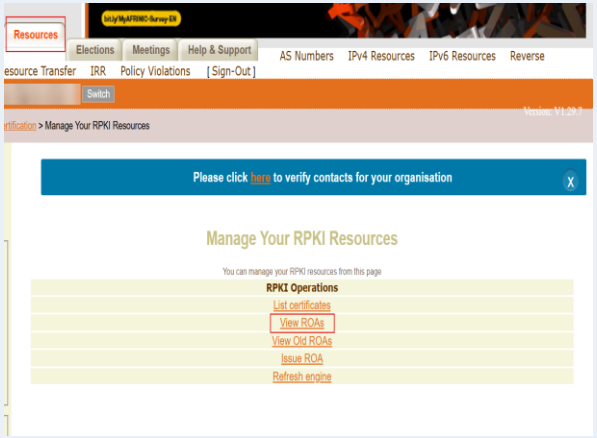
Repeat the form for each additional prefix or ASN combination. One ROA covers one prefix (plus its max length) per origin ASN.

STEP 5

Verify it was created

Open “View ROAs” and confirm the entry shows the correct prefix, ASN and max length, with a status other than “Revoked.”

Propagation can take a little while. Cross-check with a public RPKI validator once it is published.



Mistakes to avoid, and what comes next

- Max-length too loose or too tight for what you announce
- Missing prefixes announced by upstream or customer ASNs
- Stale ROAs after renumbering
- Next step: validate routes you receive (route origin validation) and drop invalids

Why networks and operators should act now

- Only about 3 to 5% of Nigerian networks validate routes today, so there is time to sign correctly before enforcement spreads
- Validation is spreading and over time, unsigned prefixes get less protection
- Every signed prefix makes the Nigerian ecosystem harder to hijack
- Operators can ask customers and downstream networks to sign too
- Signing today is cheap, recovering from a hijack is not

Why enterprises should act now

- Banks, fintechs, and other enterprises with their own ASN originate their own routes
- A hijack of your prefixes can interrupt payments, apps, and customer trust
- Signing your ROAs is something you control directly
- Ask your ISPs whether they sign and validate

What do you need to do?

- Check whether your prefixes have valid ROAs
- Create ROAs for prefixes that do not have ROAs
- Ask your peers, providers, and customers about theirs
- Plan route origin validation
- Share what you learn with the community

Resources: check, register, learn and deploy

Check your ROA status (search your ASN or prefix)

AFRINIC Routinator: routinator.afrinic.net

Cloudflare RPKI portal: rpki.cloudflare.com

Hurricane Electric: bgp.he.net

RIPEstat: stat.ripe.net (RPKI validation)

MANRS Observatory: observatory.manrs.org

Register your ROA

MyAFRINIC: my.afrinic.net

Path: Resources > Resource Certification > Issue ROAs

Access: registered admin-c or tech-c contact

Learn about RPKI

RPKI documentation: rpki.readthedocs.io

Cloudflare: isbgpsafeyet.com

MANRS: manrs.org

Deploy RPKI (validate routes)

Routinator (NLnet Labs): routinator.docs.nlnetlabs.nl

rpki-client: rpki-client.org

Routers: validator feeds routers via RPKI-RTR

NIST monitor: rpki-monitor.antd.nist.gov

Questions and answers

Start with one thing this month: check whether your prefixes have a valid ROA.

Ololade Iyowu | Equinix

Nigerian Peering & Interconnection Forum 2026