

Lessons from 10 Months of ASPA



TL;DR

	Origin	Path Spoofing	Route Leaks	Deployment
ROA	+	-	-	++
ASPA	-	+/--	+	++/-
BGPsec	-	+	-	-

- ROAs alone protect against mistaken announcements, but not against path issues.
- ROAs and ASPAs protect against mistaken announcements and route leaks. ASPAs do not protect fully against path spoofing, but make it harder.
- ASPA signing is widely available, validation is coming.
- BGPsec (perhaps in future) is complementary and protects against path spoofing, but not *on its own* against leaks.



How ASPA Works



ASPA Object Structure (simplified)

- Like a ROA
- Signed by the holder of one Customer AS
- Authorising one or more Provider ASes

The holder of the Customer AS Number declares which AS Numbers may appear as their Providers in BGP paths



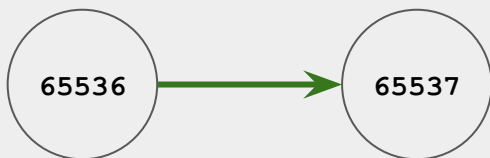
Provider Free Networks

AS0 is used in ASPA objects to indicate that the **customer AS** has no providers.

- AS0 is reserved and cannot be on the path
- So every next AS gets “Not Provider”
- Used by
 - Tier-1/Transit-free Networks
 - Transparent Route Servers
 - Route Collectors
 - Or even... unused ASNs

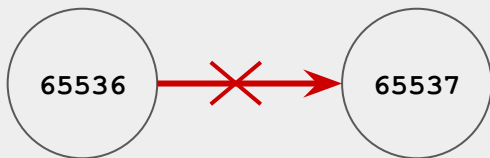


Fundamental Function to Evaluate AS Pairs



Provider

65536 has an ASPA including 65537



Not Provider

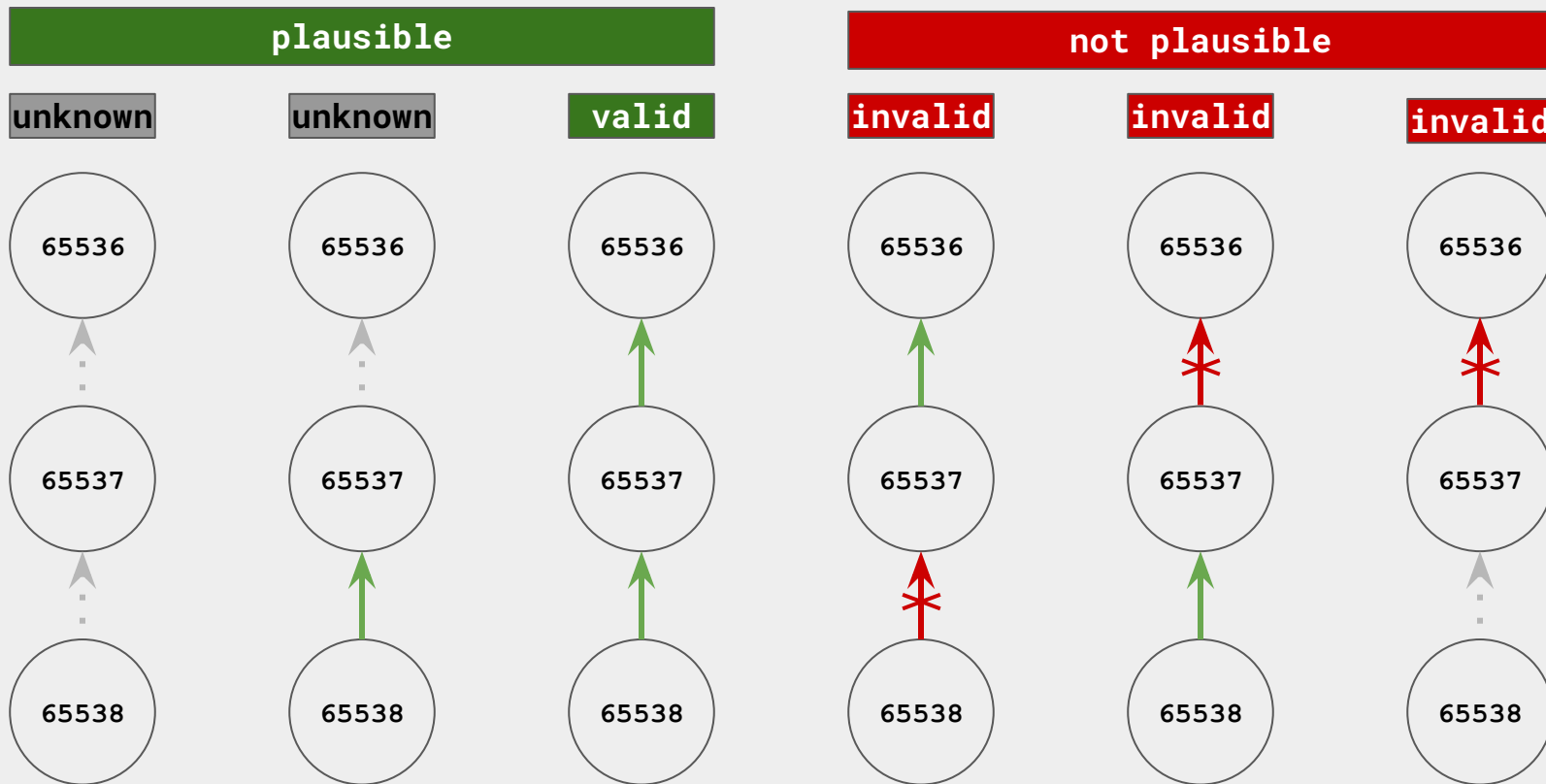
65536 has an ASPA without 65537



No Attestation

65536 has no ASPA

You as Upstream to Customers, Peers or Route Servers





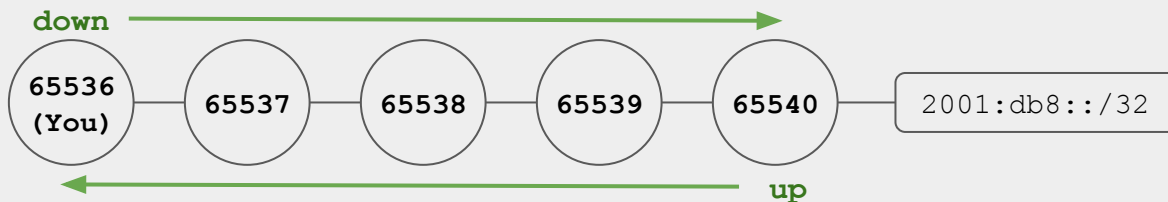
Valley Free Routing

- Find plausible upstream paths from both ends of path:
 - longest **plausible** customer-provider up-ramp **from the origin**
 - longest **plausible** customer-provider down-ramp **from the reverse**
- Okay if...
 - They overlap (e.g. partial deployment)
 - They meet in a single shared provider
 - They meet in a single peering adjacency
- More adjacencies indicate a **valley**
 - E.g. up-lateral-up-down, up-down-up-down
 - Latency/Congestion/Cost/Data security

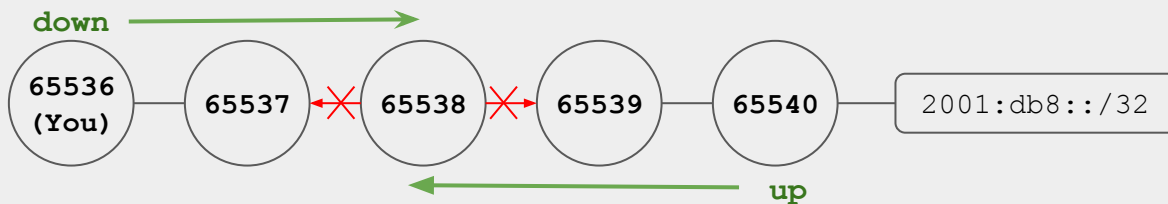
You as Downstream to Providers (Examples)



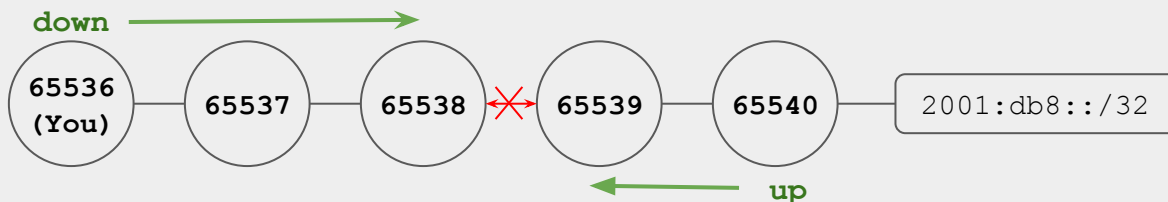
plausible



Little/No ASPAs



65538 is a shared provider (possibly tier-1)

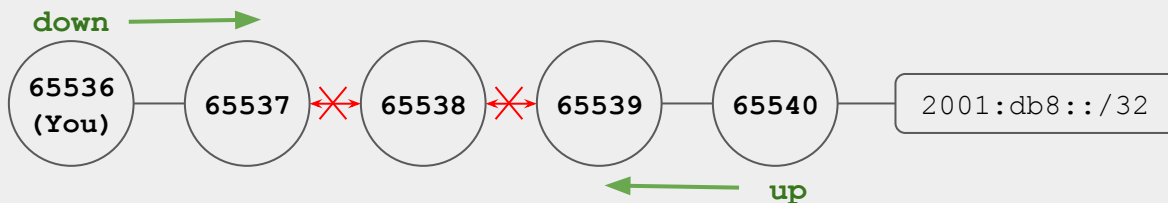


65538 and 65539 are assumed to be peering

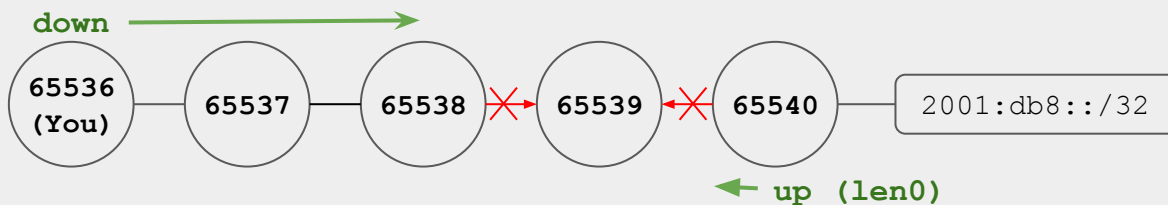
You as Downstream to Providers (Examples)



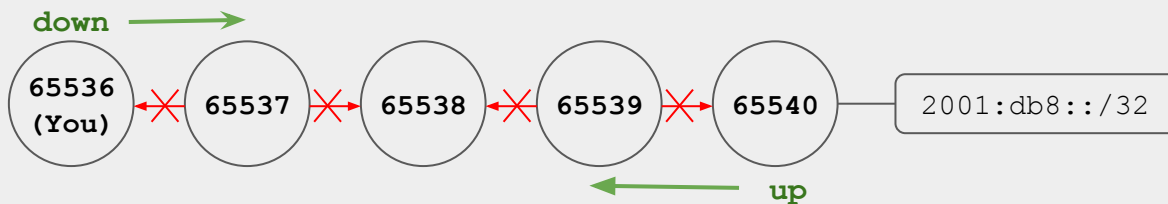
not plausible



65538 leaks to other (possible) peer

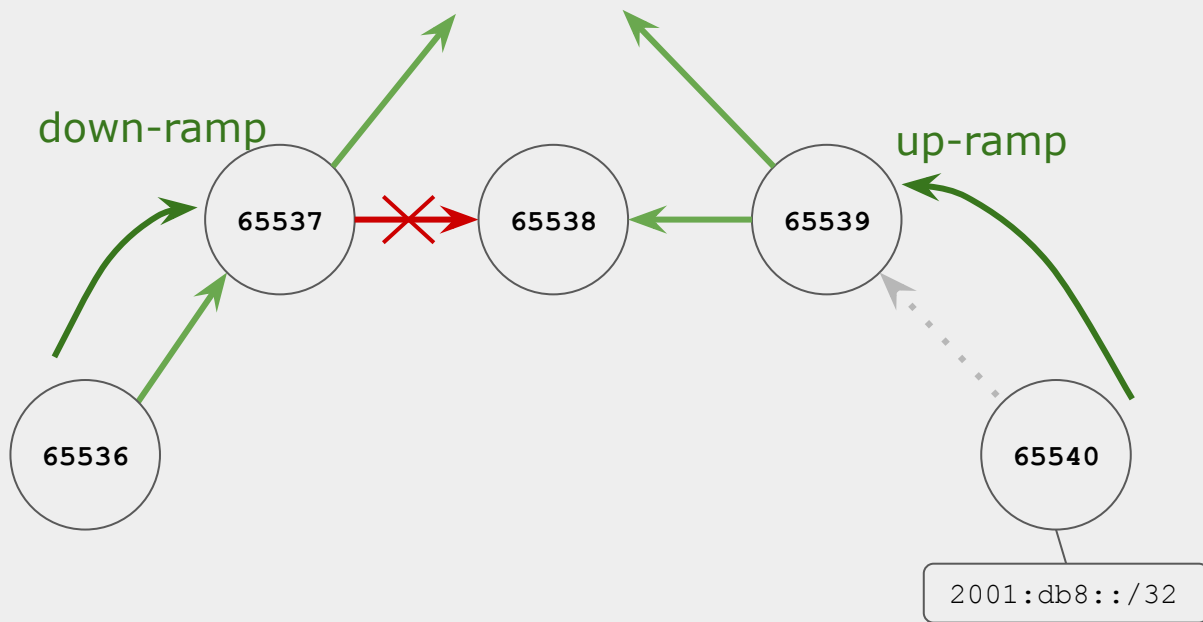


65539 is not provider to 65540 (leak or spoof)



65538 leaks route from provider to another provider

Complex: When a Peer is sometimes Provider



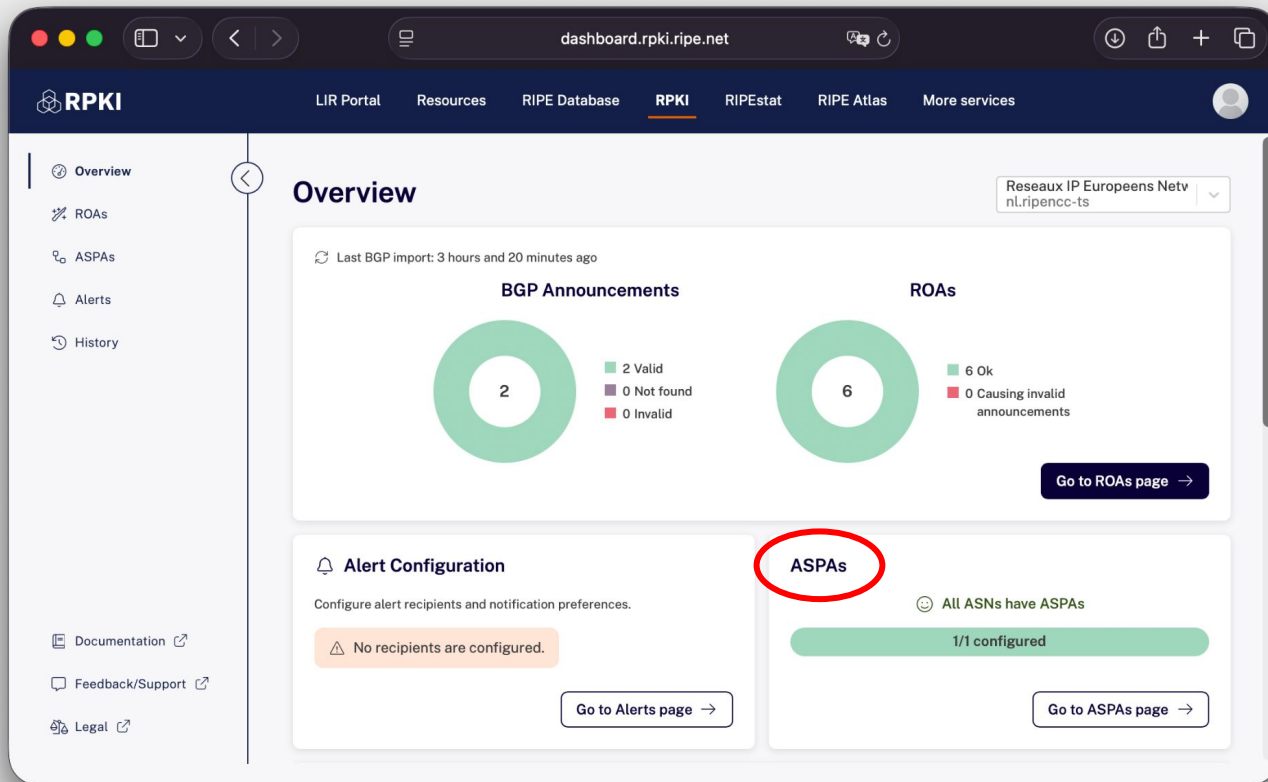
Adding a peer as provider allows them to leak, so **do not do this**, unless they can be a provider.

65539 added 65538 as provider, so the path is accepted. 65538 appears to peer with 65537.

Consider using RFC 9234 “Only-to-Customer” (OTC)



ASPA Signing





dashboard.rpki.ripe.net

RPKI LIR Portal Resources RIPE Database **RPKI** RIPEstat RIPE Atlas More services

Overview
ROAs
ASPAs
Alerts
History

Go to overview →

ASPAs

Reseaux IP Europeens Netw
nl.ripecc-ts

What is ASPA?

ASPA is an emerging standard coming out of the IETF that can help to prevent BGP route leaks, and to a degree improves BGP path security. We recommend to read the documentation below.

[Read the documentation](#)

Watch it explained

We recommend that you watch the presentation given at RIPE 91 before you start.

[Watch the presentation](#)

What providers should I include?

- All your Providers!
- Not your lateral peers
- Unless those peers that can act as your Provider
- Also include non-transparent route servers

Customer ASN	Provider ASNs
AS2121	AS3333, AS56595

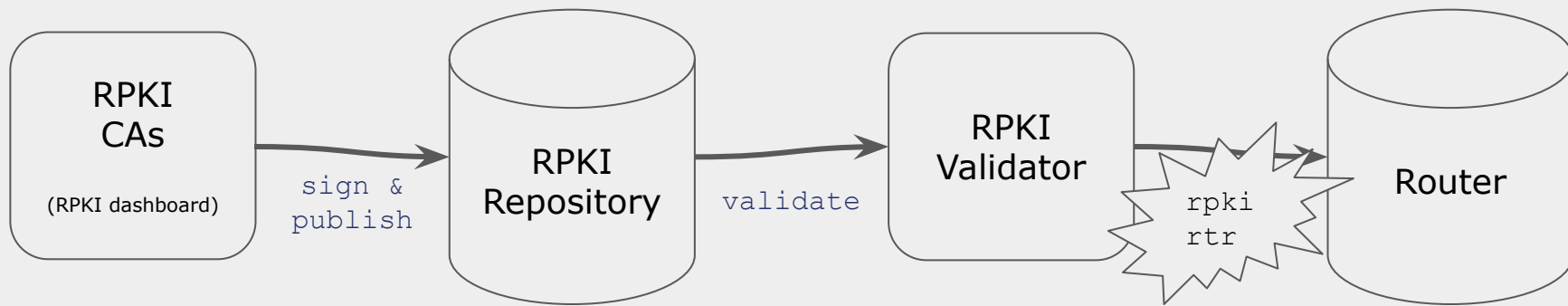
Edit Delete

Documentation
Feedback/Support
Legal



ASPA in the Router

From Signing to Router



- Same deployment model as ROAs
- No crypto in the router (works on modest hardware)
- Allows simple config in routers
- Long standardisation process (yes, even by IETF measures)
 - ◆ object profile, rpki-rtr, path verification
- Consensus finally reached (it seems)



It's a sharp tool

- As with Route Origin Validation: reject invalid
- Fix your ASPAs:
 - Do NOT sign if you don't maintain
 - Assume that people will drop invalid

But it's early days

- Not yet available on many routers, talk to your vendor!
(Supported on: Bird, OpenBGPd, NIST-BGP-SR. Test phase: Cisco IOS-XR)

YYCIX was first (2023)



[nanog](#) mailing list archives 

[By Date](#) [By Thread](#)

List Archive Search 

Calgary Internet Exchange (YYCIX) deploys world's first ASPA-filtering Route Servers

From: Job Snijders <job () sobornost net>
Date: Thu, 2 Feb 2023 18:57:09 +0000

CALGARY, CA-AB, Feb. 2, 2023 – The Calgary Internet Exchange (YYCIX) is thrilled to announce the deployment of the world's first ASPA-filtering Route Servers on a public peering fabric. The YYCIX Route Servers drop ASPA-invalid BGP routes in order to protect multilateral peers.

ASPA (Autonomous System Provider Authorization) is a free RPKI-based technology for detection and mitigation of BGP route leaks. ASPA enables holders of Autonomous System identifiers to securely authorize one or more other Autonomous Systems as their upstream providers, in turn enabling Relaying Parties (ISPs and IXPs) to use this cryptographically

Using:

- rpki-client
- OpenBGPd

(both run on Linux and other systems as well)

Dropping ASPA (and ROV) Invalid in OpenBGPD



```
include "/var/db/rpki-client/openbgpd"

neighbor 5.10.192.4 {
    role customer
    remote-as 51088
}

neighbor 2a02:1668:a2b:1:3::1 {
    role customer
    remote-as 51088
}

# reject ROA invalids
deny quick from ebgp ovs invalid

# reject ASPA invalids
deny quick from ebgp avs invalid
```

<https://man.openbsd.org/bgpd.conf>



Key Configuration of BIRD (3.2.1+)

```
roa4 table roas4;
roa6 table roas6;
aspa table aspas;
attribute enum roa roa_status;
attribute enum aspa aspa_status;
attribute int valid_roa;
attribute int valid_aspa;

protocol rpki rpki_validator {
    roa4 { table roas4; };
    roa6 { table roas6; };
    aspa { table aspas; };
    remote ...;
}

template bgp public_transit_v4 {
    direct;
    local as 2121;
    local role customer;

    ipv4 {
        import filter bgp_in_transit_v4;
        export where proto = "as2121_v4";
        import keep filtered;
        # Needed for automatic RPKI reload
        import table on;
    };
};
```

routinator over rpki-rtr



Key Configuration of BIRD (3.2.1+)

```
filter bgp_in_transit_v4 {  
  (...)  
  roa_status = roa_check(roas4);  
  case roa_status {  
    ROA_INVALID: {  
      valid_roa = 2;  
      reject "Invalid ROA (...);"  
    }  
    ROA_VALID: valid_roa = 1;  
    ROA_UNKNOWN: valid_roa = 0;  
  }  
}
```

```
  aspa_status = aspa_check_downstream(aspas);  
  case aspa_status {  
    ASPA_INVALID: {  
      valid_aspa = 2;  
      reject proto, ": invalid ASPA(...)";  
    }  
    ASPA_VALID: valid_aspa = 1;  
    ASPA_UNKNOWN: valid_aspa = 0;  
  }  
  
  accept;  
}
```

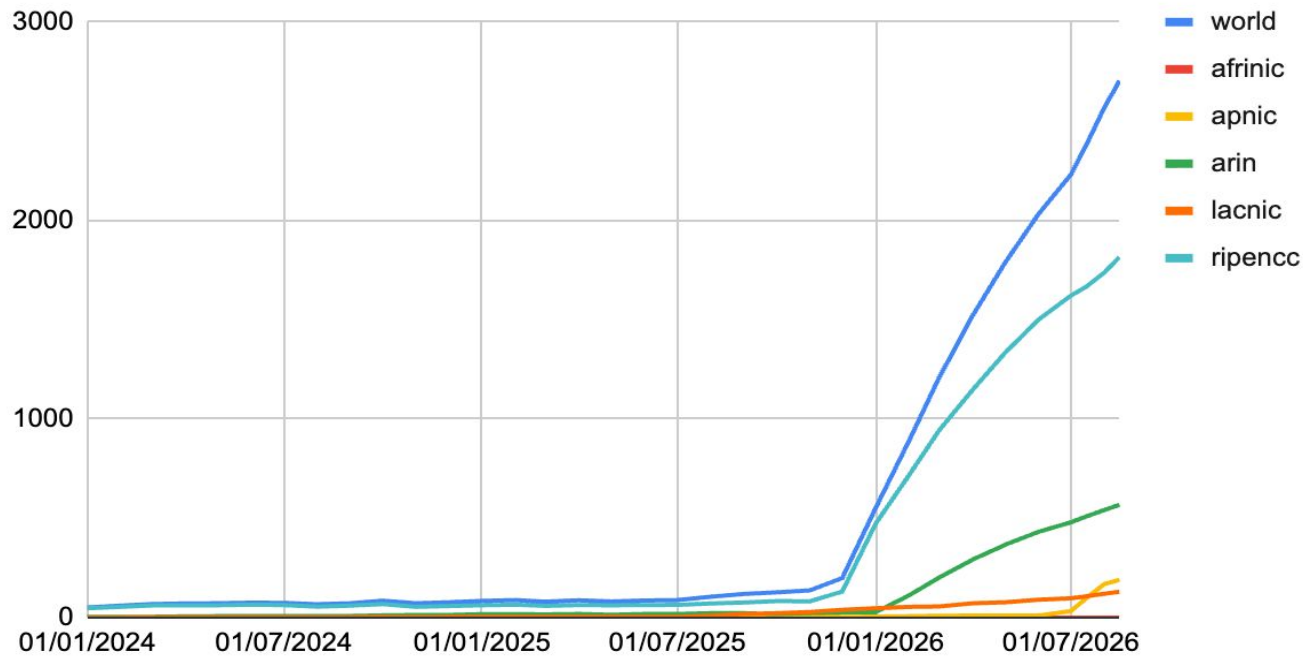


ASPA Uptake

ASPA Signing Uptake



Number of ASPA Objects



July 2025

Krill UI (~.BR)

Nov 2025

RIPE NCC UI

Jan 2026

ARIN UI

June 2026

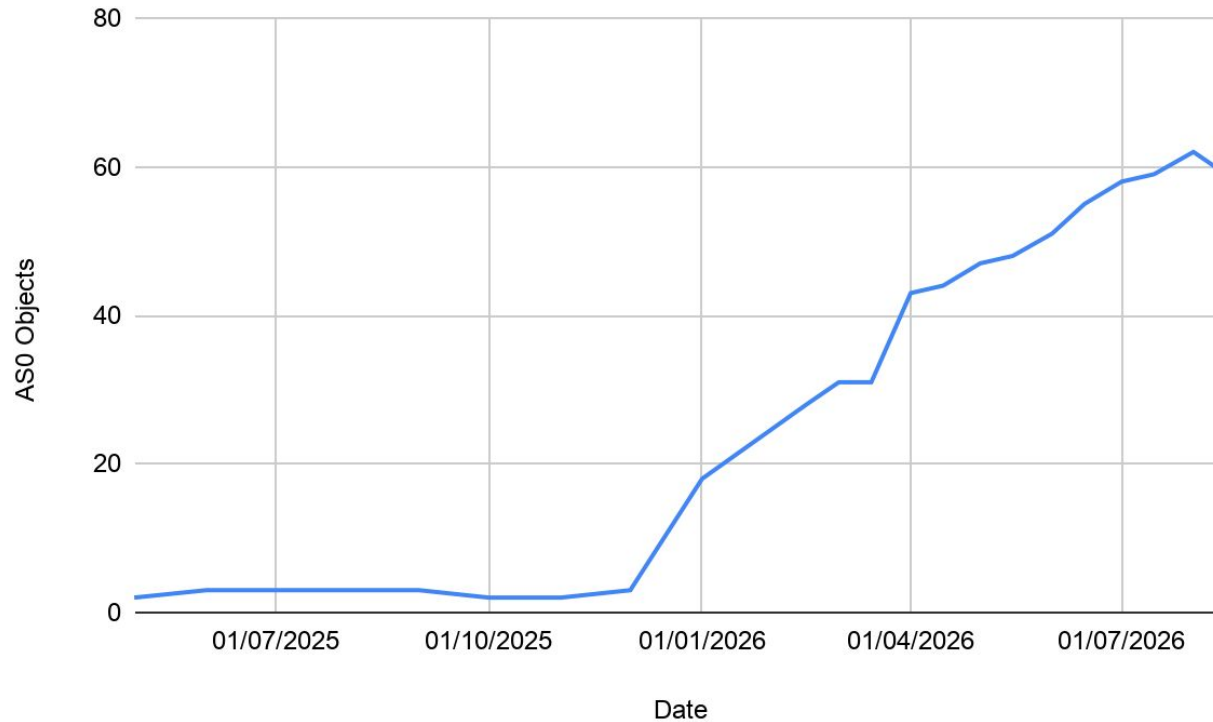
APNIC UI

ASPA Relative Signing Uptake - 15 August 2026



Region	Registered ASNs
World	2.2%
RIPE NCC	4.6%
NL	6.1%
DE	8.8%
BE	6.5%
GB	5.7%
PL	2.0%
CZ	10.9%

ASO Signing Uptake





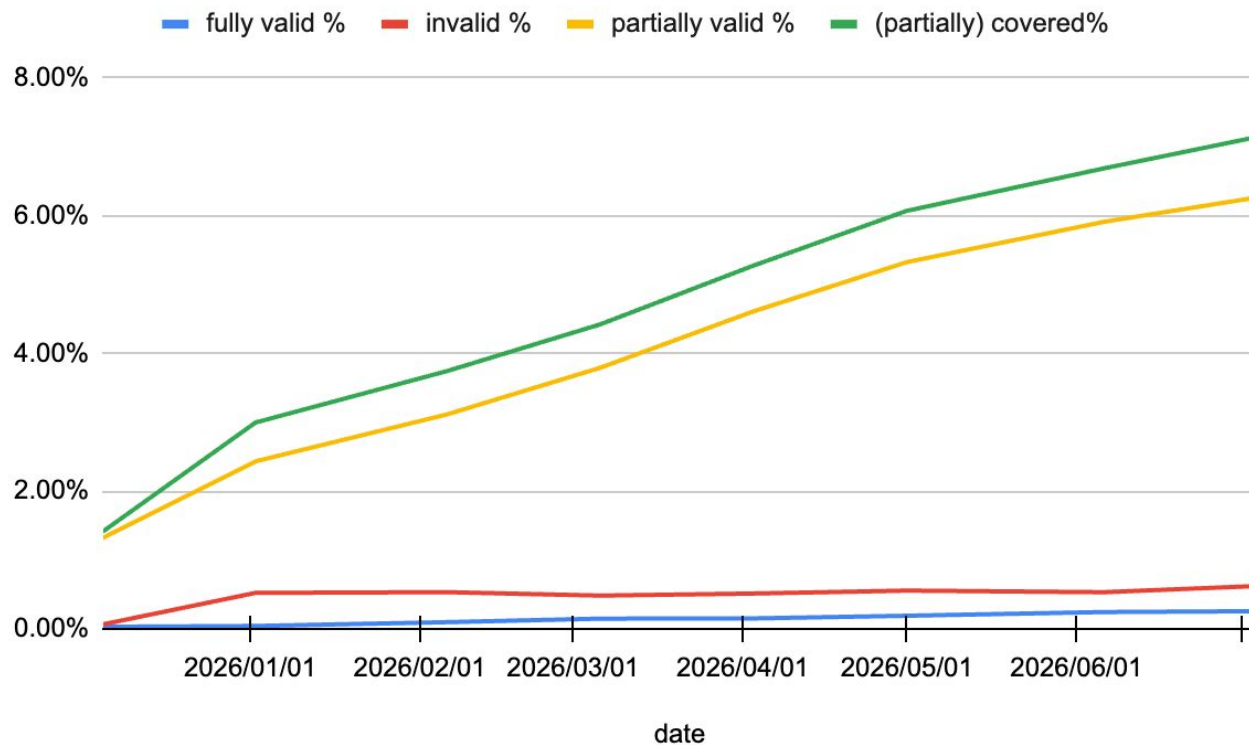
ASPA Path Analysis



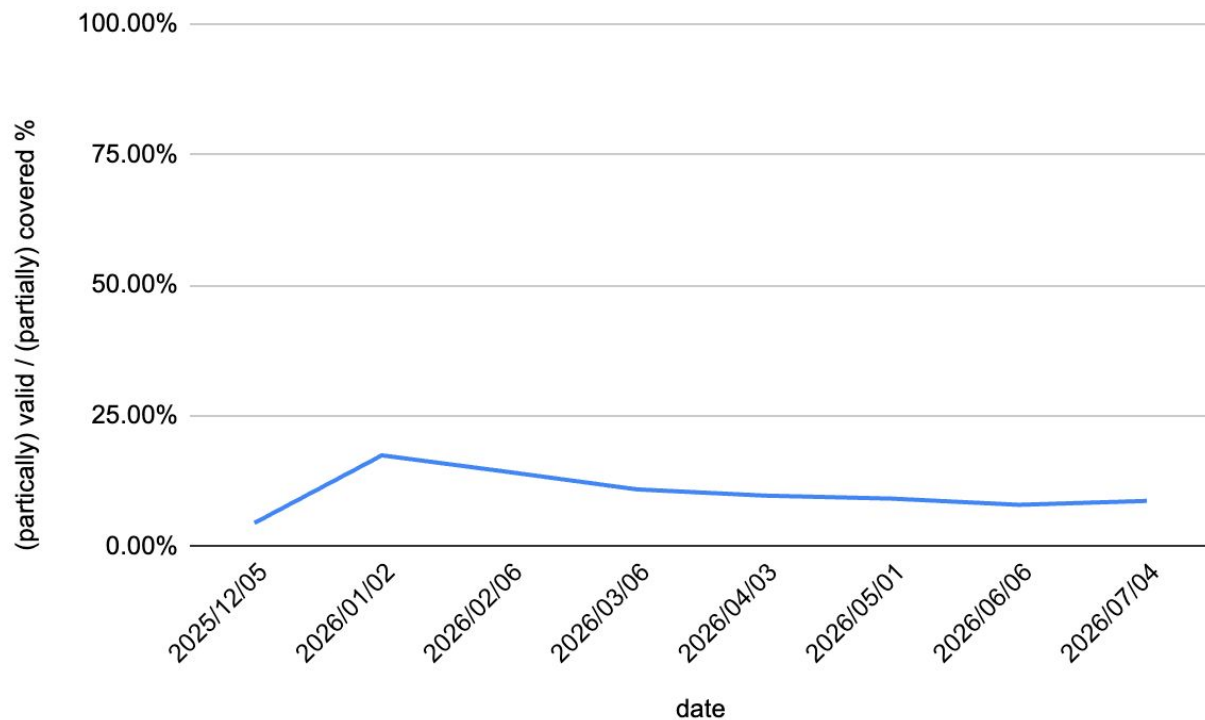
AS0 ASPAs signal Provider Free Networks

- Look at **all** routes seen in RIS
<https://data.ris.ripe.net/derived/prototypes/parquet/v0/bview/>
- Get the **unique** paths leading up to a **provider free** network
- Remove any duplicated ASes in the path (learned this the hard way)
- Then validate these paths, as **customer** paths:
 - invalid
 - fully valid
 - partially valid (at least on ASPA on path)
 - not covered at all

ASPA Path Validity to AS0 Networks



How common are invalids?





Next Steps?



Extend the ASPA UI (Q1 2027?)

- Provide better tooling for users for the RPKI Dashboard
 - Inform who their providers *could* be
 - Inform which peers may *actually act as providers*
- Don't make it a click and save
 - You *should* know who your transits are
 - You *should* check suggestions
- Evaluate ASPA path validity before publication
 - Show effect on routes for customer AS
 - Leverage known other ASPAs
 - Leverage known role for routes collected in RIS
- Show "Left Neighbours"



Dos

- Sign your ASPAs!
 - Maintain your ASPAs
 - Include **all** your transits
- Validate routes
- Reject ASPA **invalid** routes

Don'ts

- Up/down pref (not effective)
- Set communities based on validation state (too much churn)



Questions & Comments



tbruijnzeels@ripe.net