RPKI ASPA: Closing the Routing Security Gap

BKNIX Peering Forum / ThaiNOG Day 2026

Sheryl Hermoso (Shane)
Manager – Development
APNIC

Routing Security

RPKI	ROA	ASPA
Globally distributed cryptographic security framework supporting secure internet routing	Resource holders create ROA objects to authorise an AS to originate its prefix	Resource holders create ASPA objects to authorise their provider ASNs to forward route announcement
	Route Origin Validation Routers validate route entries against the RPKI cache	**ASPA Verification** Route entries are verified by routers against the RPKI cache

What is ASPA?

- Autonomous System Provider Authorization (ASPA)
- cryptographically signed object that allows the **resource holder** of an Autonomous System Number (ASN) to **authorize** other ASNs as their **provider networks**.

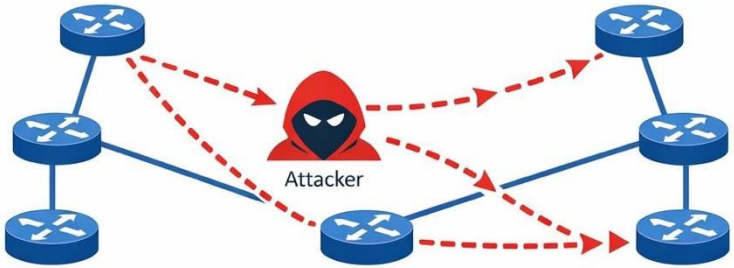
Customer AS (CAS)	45192
Set of Provider ASes (SPA)	1: 4608 2. 4826

- Defined in two documents:
  - draft-ietf-sidrops-aspa-profile
  - draft-ietf-sidrops-aspa-verification

Why is it useful?

- Detect and mitigate **route leaks**
  - In comparison, ROV is about the origin only

- Protect against certain types of **forged-origin/forged-path attacks**
  - Attacker must resort to longer AS paths for route to be accepted



ROA vs ASPA

- ROA verifies the ***origin***
- ROA record requires ASN and prefixes
- *Answers `who is allowed to announce this prefix?`*

- ASPA verifies the ***path***
- ASPA record only needs ASNs
- *Answers `is this route taking a legitimate path through the network?`*

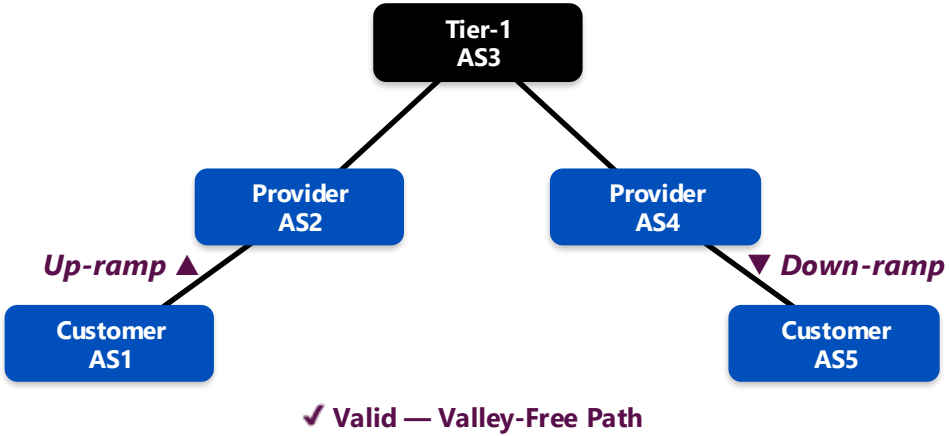
Step #1 Attestation

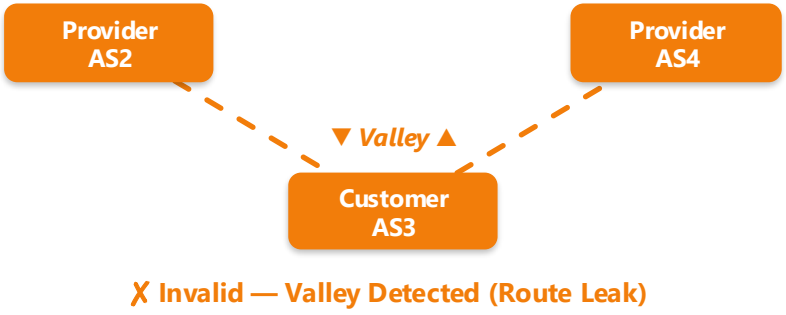
- Customer AS creates a digital signed object
- **“These specific ASNs are my legitimate upstream providers”**

- Why the customer AS?
  - “Bottom-up” security model wherein customer is the “authoritative source” responsible for keeping track of their transit/upstream provider(s).

Step #2 Verification

- BGP router checks the AS Path of each route entry against the ASPA object
- "**Valley Free**" Routing:
  - Expect up-down structure →
    - Customer to Provider (up) and Provider to Customer (down)
  - Rule:
    - Provider to Customer (down) then Customer to Provider (up) creates a "valley" or a dip which indicates a route leak





Validation Outcomes

Outcomes

Provider
ASPA record exists
Hop is confirmed

Not Provider
ASPA record exists
Next AS is not on the list

No Attestation
No ASPA record

States

Valid
Each AS-to-AS Authorization Function yields “provider”

Invalid
At least one AS-to-AS Authorization Function yields “not provider”.

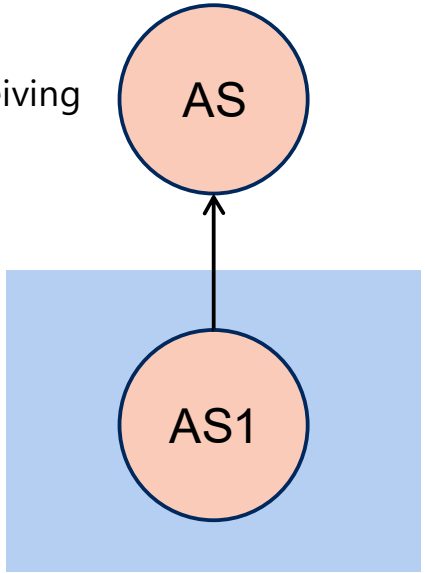
Unknown
At least one AS-to-AS Authorization Function yields “no attestation”, but there is no occurrence of “not provider”.

Upstream validation

1. If AS path has single entry → VALID 
2. If AS path contains hop from provider to customer → INVALID 
3. If AS path contains hop without ASPA → UNKNOWN 
4. Otherwise, all hops are from customer to provider → VALID 

Upstream validation examples (1)

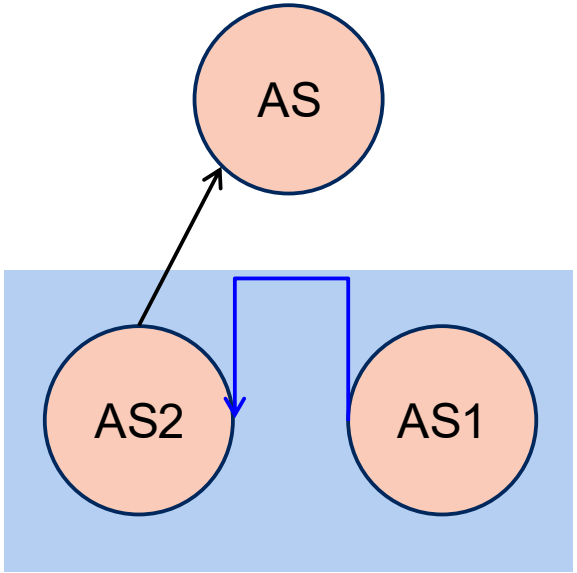
This AS is the upstream, receiving the route



- Single-element AS path
- ASPA state not relevant
- Not possible for it to be a route leak

- Arrows indicate AS path, from origin through peers
- Blue box contains route: only the AS path is relevant to ASPA validation, so the prefix is omitted
- Black arrow: ASPA state between the two ASNs is irrelevant

Upstream validation examples (2)



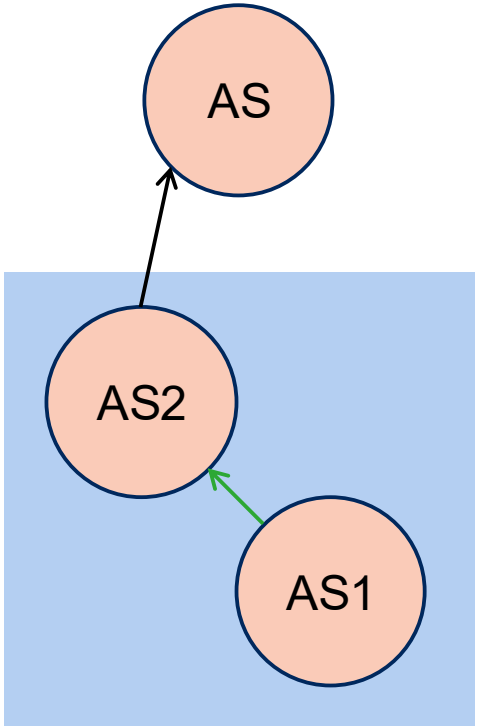
- Blue line: no ASPA for customer-provider pair

- Two-element AS path
- No ASPAs
- Unable to determine validity

Upstream validation examples (3)

AS	Providers
1	2

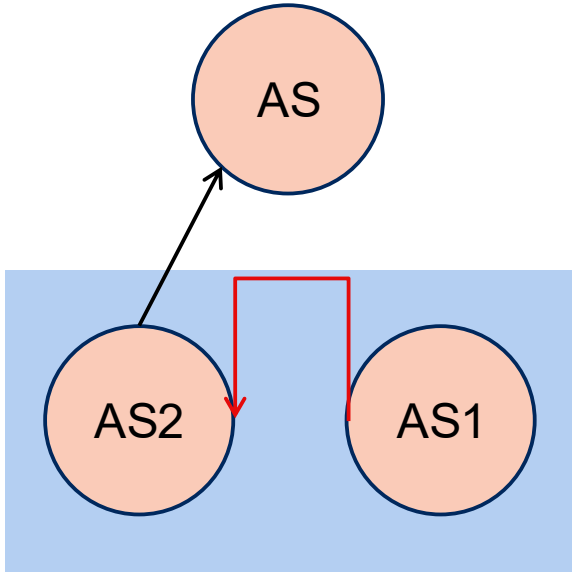
- Within route, higher ASes are providers for lower ASes
- Green line: ASPA exists for customer-provider pair



- Two-element AS path
- ASPA exists for AS1 (origin)
- Able to determine validity

Upstream validation examples (4)

AS	Providers
1	3



- Two-element AS path
- ASPA exists for AS1 (origin), but disclaims AS2 as provider
- Able to determine validity

•Red line: ASPA exists for customer, but does not contain provider ASN

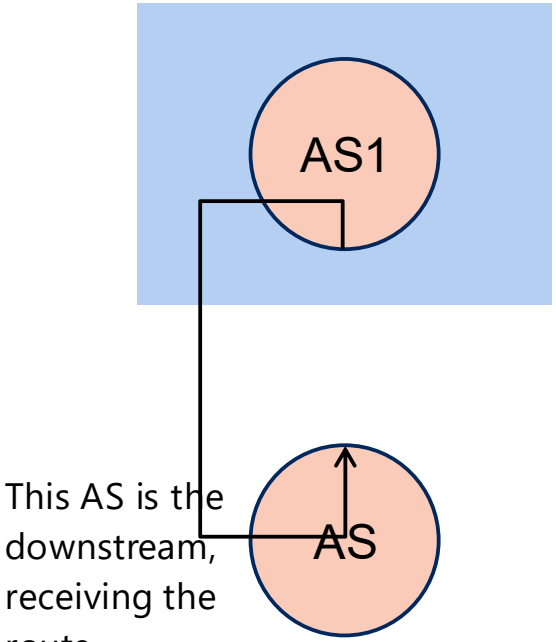
Downstream validation

1. If AS path has:
   - Up-ramp, customer(s) through provider(s)
   - Down-ramp, provider(s) through customer(s)
   - No hops in the middle, or single lateral hop

2. If AS path contains ‘valley’ (hop from provider to customer, then from customer to provider)

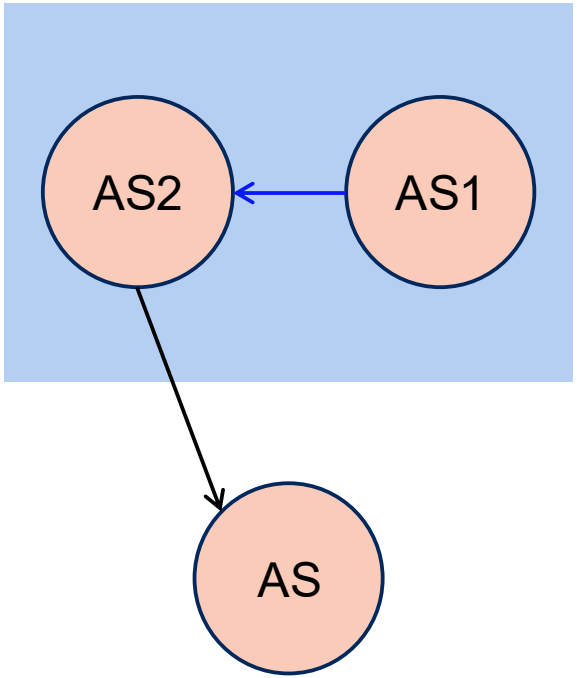
3. Otherwise, unable to determine validity

Downstream validation examples (1)



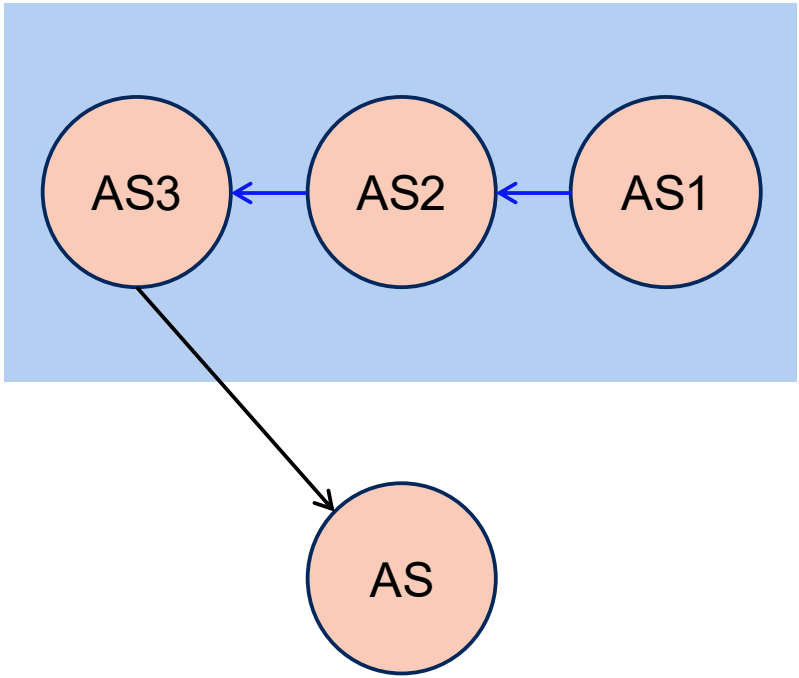
- Single-element AS path
- ASPA state not relevant
- Not possible for it to be a route leak

Downstream validation examples (2)



- Two-element AS path
- No ASPAs
- Not possible for it to be a route leak

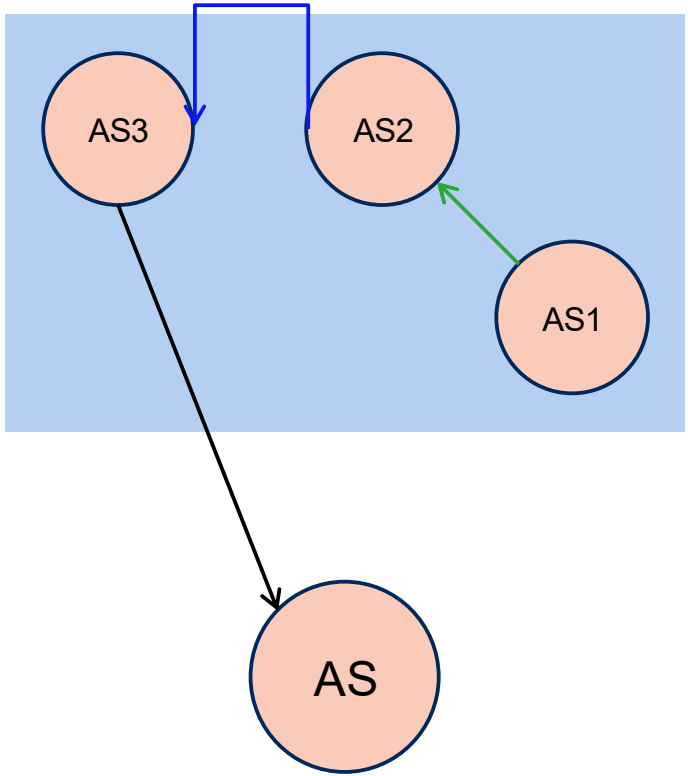
Downstream validation examples (3)



- Three-element AS path
- No ASPAs
- Unable to determine validity

Downstream validation examples (4)

AS	Providers
1	2

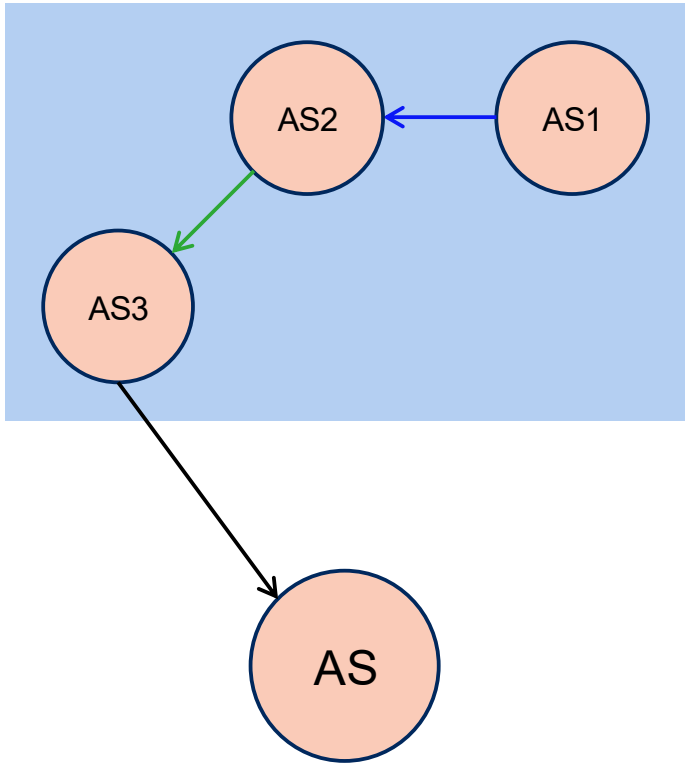


- Three-element AS path
- ASPA exists for AS1 (origin)
- Route leak not possible

Downstream validation examples (5)

Within route, lower ASes are customers of higher ASes

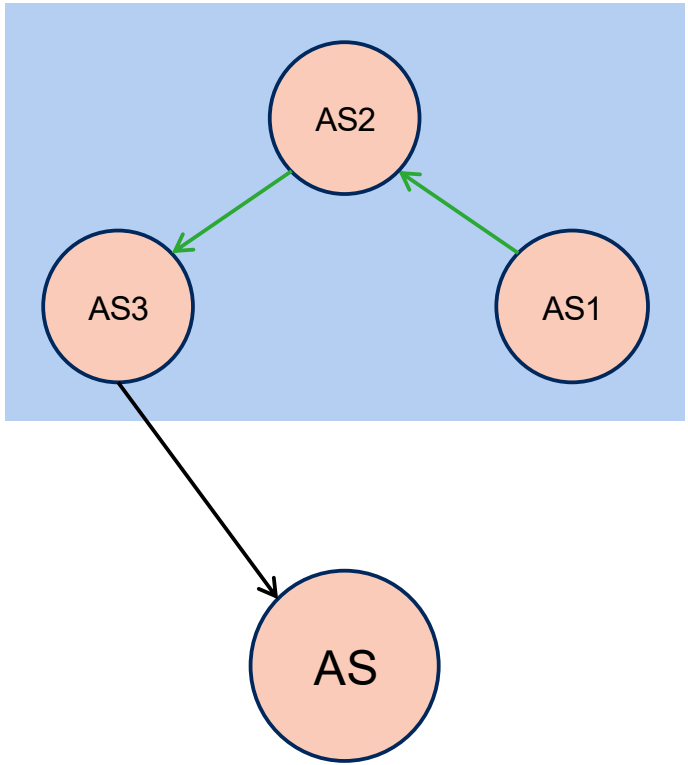
AS	Providers
3	2



- Three-element AS path
- ASPA exists for AS3 (neighbour)
- Route leak not possible

Downstream validation examples (6)

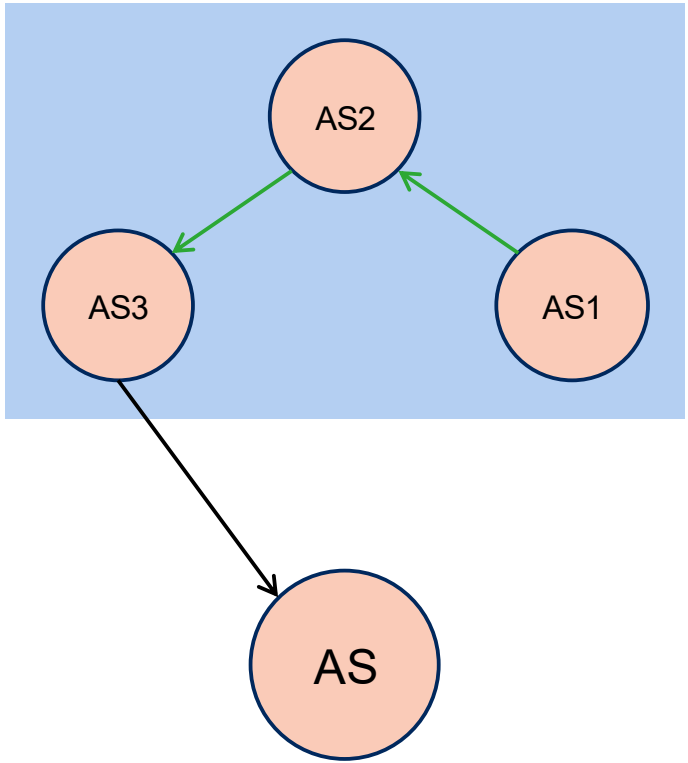
AS	Providers
1	2
3	2



- Three-element AS path
- ASPAs exist for AS1 and AS3
- Route leak not possible

Downstream validation examples (7)

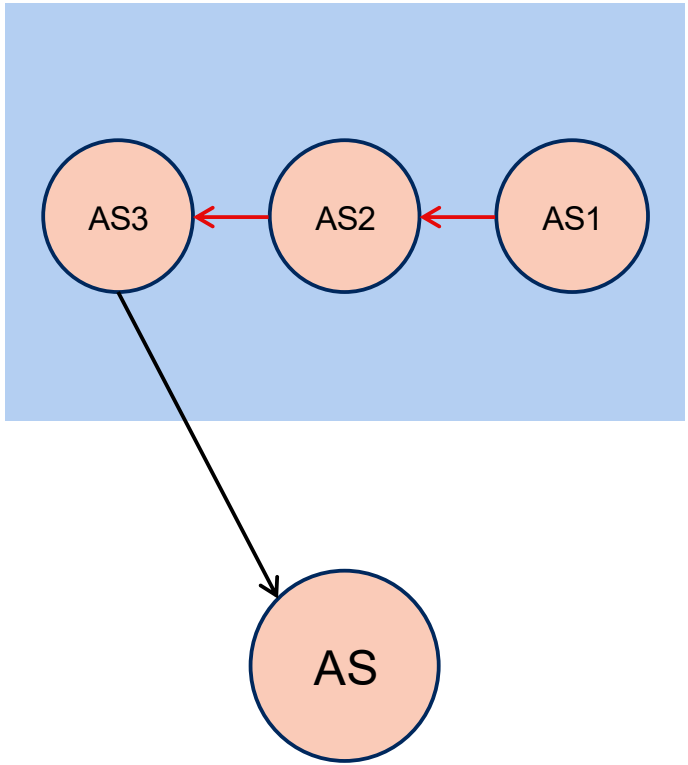
AS	Providers
1	2
2	0
3	2



- Three-element AS path
- AS0 ASPA now exists for AS2, to indicate absence of providers
- Route leak not possible

Downstream validation examples (8)

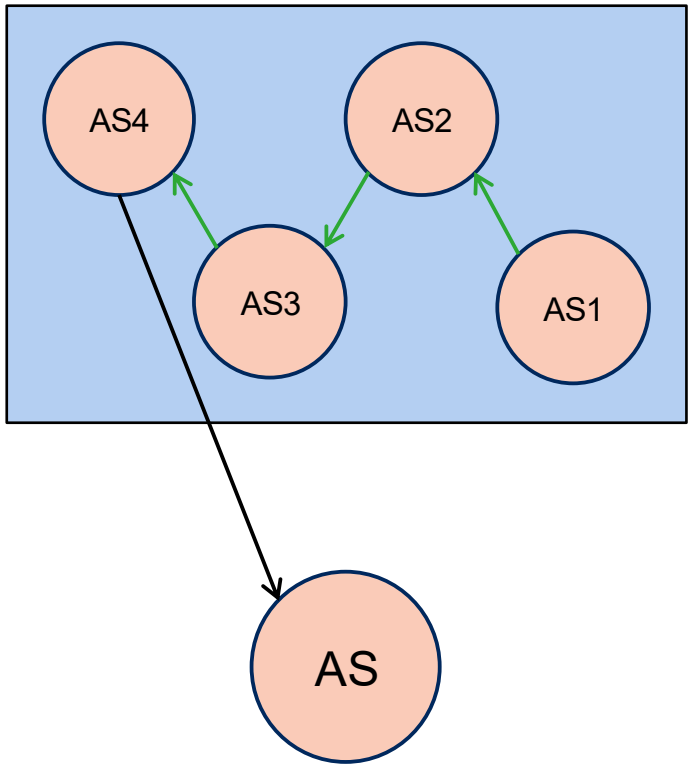
AS	Providers
1	4
2	0
3	5



- Three-element AS path
- Up-ramp and down-ramp ASPAs do not include AS2
- Route leak

Downstream validation examples (9)

AS	Providers
1	2
2	0
3	2, 4
4	0



- Four-element AS path
- Valley from AS2 to AS3 (customer) to AS4 indicates route leak

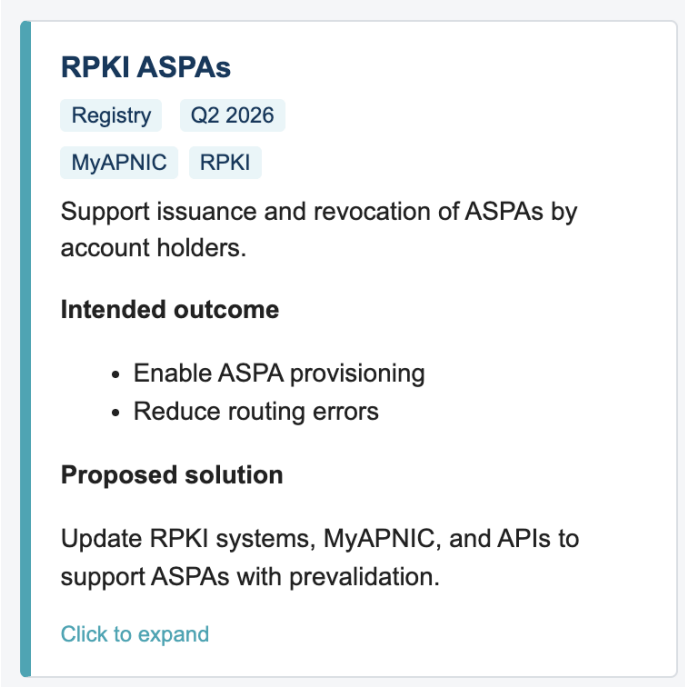
ASPA Support

- **RPKI Software**
  - Krill (Signer/CA)
  - Routinator (Validator/RP)
  - Rpki-client
  - FORT Validator
- **BGP Routing Software**
  - BIRD Internet Routing (v2.16+)
  - OpenBGPD (v7.8+)
  - Cisco IOS-XR (Early Field Trial and Active testing)

FORT

ASPA Implementation @ RIR

- **RIPE NCC** has integrated ASPA into the RIPE RPKI Dashboard since December 2025.
- **ARIN** has deployed ASPA as of January 2026.
- **APNIC** is due to implement in Q2 2026 – see https://roadmap.apnic.net/
- Goal to have ASPA support in all RIRs this year.



Resources

- **RIPE NCC ASPA Documentation**
  https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/aspa/

- **ARIN ASPA Documentation**
  https://www.arin.net/resources/manage/rpki/aspa/

Thank You!