Confirming BGP AS_PATH Based on Route Path Authorizations (RPA)

draft-guo-sidrops-rpa-profile-00
draft-xu-sidrops-rpa-verification-00

Shenglin Jiang, Yangfei Guo

IETF 124 SIDROPS

Nov. 2025

Why Route Path Authorization (RPA) Is Needed

Even with **RPKI-ROV** and **ASPA** improving BGP security, several gaps remain:

- **Complex relationships:** ASPA handles only customer-to-provider links, missing internal, peer, and lateral cases.
- **Ingress/Egress control:** No way to define which routes an AS can announce.
- **Partial deployment risk:** Limited ASPA adoption leaves validation blind spots.
- **Privacy concerns:** ASPA may expose sensitive business relationship information.

RPA complements ASPA by defining explicit **routing intentions** and controlling **route acceptance and announcement** at both ingress and egress.

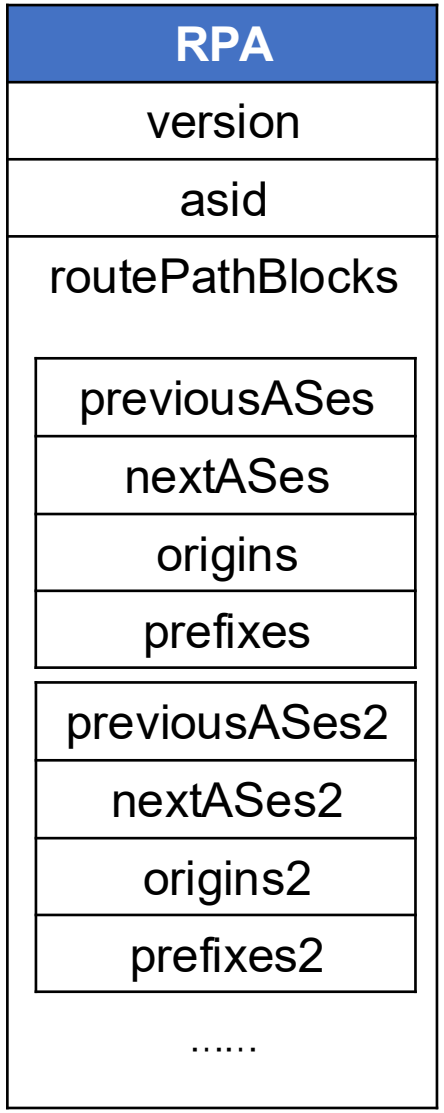
Aspect	ASPA	RPA
Direction	Upstream validation	Ingress/Egress control
Coverage	Customer→Provider	All AS relations

RPA signed object

Route Path Authorizations (RPA)

Customer/Peer/Provider → Set of Advertisable Paths (including ingress/egress)

- version: 0
- asid: local AS number, issuer's AS number
- routePathBlocks: routing path intent description (**only at ingress, only at egress, or at both ingress and egress**)
  - previousASes: upstream Ases, default is None for any
  - nextASes: downstream ASes, default is None for any
  - origins: optional field, origin ASes, references to ROA/SPL/..., default is None for any
  - prefixes: optional field, default is None for any

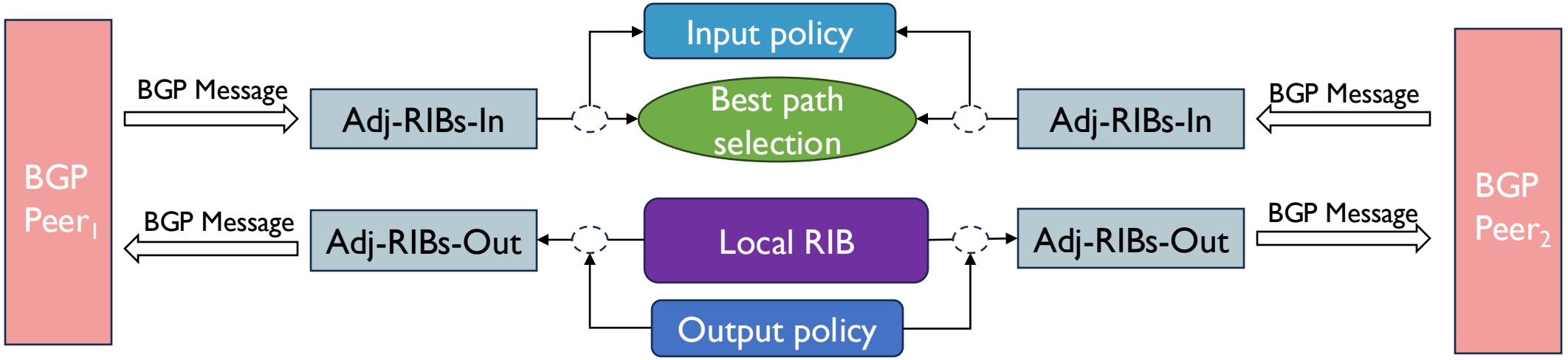


RPA Verification Process

The workflow enables combined relationship and path-intent verification for higher AS-PATH integrity.

Neighbor sends BGP update with AS_PATH.

1. Router checks ASPA data to verify customer-provider direction.
2. Router checks RPA records to validate ingress/egress path intent.
3. If validation pass, route accepted; otherwise, flagged or rejected.



Confirming AS_PATH under partial registration

Step 1 Per-AS:

RPA_A object	
PreviousASes	
NextASes	B,E
Origins	
Prefixes	

VALID ✅

RPA_B object	
PreviousASes	A
NextASes	C
Origins	
Prefixes	

VALID ✅

RPA_D object	
PreviousASes	C
NextASes	
Origin	
Prefix	

VALID ✅

Step 2 AS_PATH:

VALID ✅

RPA and ASPA: Parallel and Complementary Verification

- **Parallel operation:**
  RPA works **alongside ASPA**, not as a replacement. While ASPA validates "who is my provider," RPA validates **"which paths I authorize for exchange"** — covering both **ingress** and **egress** directions.
- **Enhanced relationship coverage:**
  RPA extends verification to **provider→customer**, **peer→peer**, and **lateral** links that ASPA cannot fully represent.
- **Fine-grained policy control:**
  Operators can express and verify specific routing intents — e.g., *accept from A but not from B*, or *announce only via C* — providing granular protection against leaks and forged path segments.
- **Improved resilience under partial deployment:**
  Even if ASPA adoption is incomplete, RPA's bidirectional authorization helps identify **fake links** or **unintended path propagation**.

Thank you!

Many many thanks to those who give us suggestions and comments:
Jakob Heitz, Job Snijders, Jeffrey Haas, Ruediger Volk, Randy Bush, Sriram Kotikalapudi, Christopher Morrow, Nan Geng, Maria Matejka and so on.

IETF 124 SIDROPS

Nov. 2025