Workgroup:	SIDR Operations Working Group
Internet-Draft:	draft-xxx-sidrops-xxx-00
Published:	19 September 2025
Intended Status:	Standards Track
Expires:	23 March 2026
Author:	xxx. xxx
	xxx

RPKI-based Validation with Prioritized Resource Data

Abstract

Based on RPKI ROAs, Route Origin Validation (ROV) is a practical solution to address prefix origin hijacking. During ROV operations, the data used may come from local sources other than ROAs. These data sources can vary in terms of credibility, and ROV operations may require different response actions for invalid or unknown routes. This document describe an enhancement of ROV with multi-level priority, and outlines the use cases, framework, and requirements for ROV operations that involve multi-level priority.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 23 March 2026.

Copyright Notice

Table of Contents

1. Introduction

Route Origin Validation (ROV), which is built on RPKI Route Origin Authorizations (ROAs), stands as a practical and effective approach to combat prefix origin hijacking. In ROV operations, the validating data utilized is not limited to ROAs alone; it may also include various types of local data from other sources. These additional data sources can exhibit varying levels of credibility, with some being highly reliable due to their authoritative origins and others being less

trustworthy due to potential inconsistencies or lack of verification. Correspondingly, ROV operations need to be flexible enough to take different actions when dealing with invalid routes and unknown routes. This document introduces an enhancement of ROV with multi-level priority, and elaborates the gap analysis, framework, and specify the key requirements for implementing ROV with multi-level priority in current RPKI infrastructure.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Suggested Reading

It is assumed that the reader understands BGP[RFC4271] and RPKI[RFC6480].

3. Gap analysis

ROV (Route Origin Validation) based on RPKI (Resource Public Key Infrastructure) relies on ROA (Route Origin Authorization) data. It is known that ROA data has the following deployment issues: it does not fully cover all routes in the routing table; there exist ROA data with artificial registration errors; and network operators can filter specific validation data from VRP (Validated ROA Payload) data locally as needed, or supplement it with additional data (e.g., data inferred through machine learning). SLURM (Simplified Local Internet Number Resource Management) technology can be used to modify the data locally.

Due to such mixed data sources, the credibility of the data varies to different degrees and is no longer uniform. Similarly, network operators expect to perform different operations on validation results based on their credibility. This approach offers benefits such as the following use case: an ISP (Internet Service Provider) uses data derived from its own experience to supplement RPKI ROAs, but the credibility of this supplementary data is lower than that of RPKI ROAs. When a route is verified as "invalid" by RPKI ROAs, the router can discard the route; if a route is verified as "invalid" by supplementary data with medium credibility, the router can be configured to trigger an alert.

However, current RPKI technology does not support such operations. Regardless of the source of the validation data, the same type of validation result triggers the same operation. This fails to meet the need for customized processing of different scenarios in network operations. This document describes a RPKI validation mechanism with multi-level priority to make RPKI-based validation processing more flexible.

4. Requirements for Multi-Priority RPKI ROV

This section outlines the requirements for extending the RPKI architecture to support the processing and propagation of RPKI data with multiple priority levels. These requirements are necessary to enable differentiated handling of routing validation results based on their perceived trustworthiness, such as those derived from authoritative sources (e.g., RPKI ROAs) versus inferred or supplemental sources (e.g., AI-generated data).

4.1. Priority Setting

RPKI Relying Party (RP) software MUST support the assignment of a priority level to each validated RPKI object. The priority SHOULD be configurable based on the data source (e.g., RPKI-signed, locally imported, or AI-inferred). The priority value MUST be represented in a standardized format to ensure interoperability.

4.2. Multi-Priority Data Merge

When multiple representations of the same prefix-origin pair or customer-provider list exist with different priorities, RP software MUST be capable of merging them according to a consistent policy. The merge policy SHOULD prefer high-priority data and MAY allow low-priority data to be used only when high-priority data is absent.

4.3. SLURM Support for Priority Marking

The SLURM mechanism [RFC8416] MUST be extended to allow local exceptions and additions to include a priority attribute. This enables network operators to override or supplement RPKI data with local policies that reflect differentiated trust levels.

4.4. RTR Support for Priority Marking

The RPKI-to-Router (RTR) protocol [RFC8210] MUST be extended to convey the assurance level (priority) of the validation data it delivers. This enables routers to apply appropriate local policy based on the trustworthiness of the origin. To provide flexibility in deployment, two implementation models SHALL be supported:

1. One single local cache server transmits data of multiple assurance levels. The protocol MUST be extended to include a new field within its Protocol Data Units (PDUs) to explicitly carry the assurance level for each payload data item (e.g., a ROA or an ASPA). This model allows a router to maintain a single, simple transport session with one cache server while receiving a mixed-priority data set.

2. A router establishes transport sessions with multiple local cache servers, where each server is designated to provide data for a specific assurance level (e.g., a primary server provides high-priority RPKI-validated data, and a secondary server provides low-priority supplemental data). The protocol itself remains unchanged, as the priority is derived from the configuration of the router-to-server association.

Network operators SHOULD choose which implementation to deploy based on their specific operational preferences and infrastructure.

4.5. ROV/ASPA Validation with Priority Awareness

ROV and ASPA validation processes MUST be enhanced to support a multi-priority data model. The validation procedure MUST operate as a two-stage process to maximize the utility of available data while respecting the inherent trust level of each source.

1. Primary Validation with High-Priority Data: The validator MUST first perform validation using only the high-priority data available for a route. The outcome of this primary validation MUST be considered determinative and final if the state is either Valid or Invalid.

2. Secondary Validation with Low-Priority Data: If and only if the outcome of the primary validation is Unknown, the validator MAY perform a secondary validation using low-priority data. The outcome of this secondary validation (Valid, Invalid, or Unknown) MUST then be adopted as the final validation state for the route.

Annotation of Validation Outcome: The validation process MUST annotate the resulting validation state (Valid, Invalid) with an indication of the assurance level, which identifies the priority tier of the data that was used to reach that conclusion. For example, an "Invalid" result derived from a local override (high-priority) MUST be distinguishable from an "Invalid" result derived from inferred data (low-priority).

This annotated validation state MUST then be used to inform subsequent routing policy actions. Implementations SHOULD provide flexible policy mechanisms that allow network operators to define actions (e.g., reject, depreference, warn, accept) based on both the validation state (e.g., Invalid) and its associated assurance level (e.g., High or Low).

4.6. Router Handling of Priority-Based Invalid Routes

BGP speakers SHOULD support configurable policies to handle invalid routes based on the priority of the validation data. For example, routes invalidated by high-priority data MAY be deprioritized or discarded, while those invalidated by low-priority data MAY be retained with a warning.

4.7. BMP Support for Priority in Validation Reports

The BGP Monitoring Protocol (BMP) [RFC7854] SHOULD be extended to include priority information in reports of ROV/ASPA validation results. This enables network operators to monitor and analyze routing decisions based on data trust levels.

5. Security Considerations

This document defines a framework for handling RPKI data with multiple levels of priority (assurance), which introduces new considerations beyond those of the base RPKI system [RFC6480].

Amplification of RPKI Repository Failures: If a high-priority source (e.g., a primary RTR cache) becomes stale or unavailable, the system may fall back to low-priority data. This could lead to a mass re-evaluation of routes from a 'Unknown' state to a 'Valid' or 'Invalid' state based on less trustworthy information, potentially causing widespread routing churn. Implementations should include mechanisms to detect such scenarios and allow operators to define appropriate fallback behaviors.

6. IANA Considerations

This document has no IANA actions

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/info/rfc6480>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC8893] Bush, R., Volk, R., and J. Heitz, "Resource Public Key Infrastructure (RPKI) Origin Validation for BGP Export", RFC 8893, DOI 10.17487/RFC8893, September 2020, <https://www.rfc-editor.org/info/rfc8893>.

[RFC9234] Azimov, A., Bogomazov, E., Bush, R., Patel, K., and K. Sriram, "Route Leak Prevention and Detection Using Roles in UPDATE and OPEN Messages", RFC 9234, DOI 10.17487/RFC9234, May 2022, <https://www.rfc-editor.org/info/rfc9234>.

[RFC7854] Scudder, J., Ed., Fernando, R., and S. Stuart, "BGP Monitoring Protocol (BMP)", RFC 7854, DOI 10.17487/RFC7854, June 2016, <https://www.rfc-editor.org/info/rfc7854>.

[RFC8210] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1", RFC 8210, DOI 10.17487/RFC8210, September 2017, <https://www.rfc-editor.org/info/rfc8210>.

[RFC8416] Ma, D., Mandelberg, D., and T. Bruijnzeels, "Simplified Local Internet Number Resource Management with the RPKI (SLURM)", RFC 8416, DOI 10.17487/RFC8416, August 2018, <https://www.rfc-editor.org/info/rfc8416>.

7.2. Informative References

[I-D.ietf-sidrops-aspa-profile] Azimov, A., Uskov, E., Bush, R., Snijders, J., Housley, R., and B. Maddison, "A Profile for Autonomous System Provider Authorization", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-profile-19, 6 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-profile-19>.

[I-D.ietf-sidrops-aspa-verification] Azimov, A., Bogomazov, E., Bush, R., Patel, K., Snijders, J., and K. Sriram, "BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-verification-22, 23 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-22>.

Acknowledgements

The authors thank Nan Geng, Sriram Kotikalapudi and Randy Bush for their valuable suggestions and comments.

Author's Address

xxx
xxx
xxx
Email: xxx