GROW
Internet-Draft
Intended status: Informational
Expires: 22 April 2026

S. Wang
M. Xu
Y. Wang
J. Zhang
Beijing Zhongguancun Laboratory

19 October 2025

Requirements for Monitoring RPKI-Related Processes on Routers Using BMP
draft-wang-grow-bmp-rpki-mon-reqs-02

Abstract

This document outlines requirements for extending the BGP Monitoring Protocol (BMP) to provide comprehensive monitoring of RPKI-related processes on routers on routers, including RPKI data acquisition, RPKI-related policy configuration, route validation, and the impact of validation on routing decisions. The proposed extensions aim to standardize router-side monitoring on RPKI within BMP, addressing scalability and interoperability limitations in existing implementations.

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 22 April 2026.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights

and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

The Resource Public Key Infrastructure (RPKI) enhances BGP security by enabling cryptographic validation of route origins [RFC6483] [RFC6811] and AS paths [I-D.ietf-sidrops-aspa-verification]. Despite growing adoption of RPKI, standard implementations of the BGP Monitoring Protocol (BMP) [RFC7854] do not natively support monitoring of RPKI-related data. This limitation hampers visibility into RPKI validation processes and their impact on network operations.

While existing proposals aim to extend BMP for specific aspects of RPKI monitoring, such as reporting invalid routes [I-D.ietf-grow-bmp-path-marking-tlv] [I-D.ietf-grow-bmp-rel] or providing validation statistics [I-D.ietf-grow-bmp-bgp-rib-stats], a comprehensive and end-to-end monitoring framework for RPKI lifecycle on the router is still lacking. This document defines requirements and extensions for BMP to monitor four key stages:

* Acquisition of RPKI data;

* Configuration of RPKI policies;

* Validation of routes using RPKI;

* Impact of RPKI validation on routing decisions.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Requirements Overview

The BMP extension for RPKI monitoring SHOULD:

* Monitor extensible RPKI data transport from various sources to routers, including through RPKI-to-Router Protocol (RTR) [RFC8210], BGP [RFC4271], or static configurations;

* Enable real-time monitoring of the route validation process on the router [RFC6811];

* Facilitate the correlation between RPKI validation states and BGP routing decisions;

* Scale efficiently across diverse validation types.

Consequently, this document identifies four key stages in the RPKI lifecycle on routers which necessitate detailed monitoring and reporting:

3.1. RPKI Data Acquisition

To ensure accurate and timely acquisition of RPKI data, network administrators require BMP to provide real-time, consistent monitoring on the health and status of all RPKI data sources. These sources include connections to RPKI caches, local static configurations, and i/eBGP peers. This enables rapid detection and response to faults or outages in data provisioning. Accordingly, BMP SHOULD report the connection parameters, synchronization states, and error metrics for each source.

3.2. RPKI Policy Configuration

Routing policies on the router may change dynamically, therefore real-time monitoring is necessary to ensure correct implementation and prompt misconfiguration detection of RPKI-based policies. To achieve this, BMP SHOULD report global RPKI enforcement status, RPKI-related validation rules and policies for each peer.

3.3. Route Validation with RPKI

Routers from different vendors implement RPKI-based route validation— including origin validation and path validation —with varying approaches. To facilitate accurate troubleshooting against validation outcomes, BMP SHOULD report the RPKI validation state as well as the related rules that contribute to the state.

3.4. Impact of RPKI Validation on Routing

A router may implement numerous routing policies, resulting in complex routing behavior that obscures the influence of RPKI validation on decision-making. To provide visibility into this impact, BMP should report both intended outcomes and unintended side effects that are caused by the RPKI validation process.

4. RPKI Data Acquisition

BMP SHOULD enumerate all sources of RPKI data on the monitored router. These sources include the RPKI-to-Router (RTR) protocol with RPKI cache servers, static configurations, iBGP sessions with the other router within the same AS, and eBGP sessions with the other ASes (mostly upstream providers). For each source, BMP SHOULD report the following relevant information:

For RTR sources:

* The RPKI cache’s designation as primary or backup, including its priority in the selection order;
* The version of the RTR protocol in use (e.g., version 0 [RFC6810], version 1 [RFC8210], or custom versions);
* The type of TCP connection established (e.g., plain TCP, TLS, SSH);
* The IP address and port number of the cache;
* The total number of RPKI records received, including ROAs and ASPAs;

* The current status of the connection (e.g., active or idle);
* The timestamp of the most recent synchronization;
* Errors and timeouts encountered;
* Any other relevant information.

For iBGP sources:

* The IP address of the iBGP peer providing the RPKI data;
* The status of the iBGP session;
* The total number of RPKI records received, including ROAs and ASPAs;
* The current status of the connection (e.g., active or idle);
* The timestamp of the most recent synchronization;
* Errors and timeouts encountered;
* Any other relevant information.

For eBGP sources:

* The IP address and AS number of the eBGP peer providing the RPKI data;
* The AS relationship between the eBGP peer and current AS;
* The status of the eBGP session;
* The total number of RPKI records received, including ROAs and ASPAs;
* The current status of the connection (e.g., active or idle);
* The timestamp of the most recent synchronization;
* Errors and timeouts encountered;
* Any other relevant information.

For static configuration sources:

* The number of statically configured RPKI records (ROAs and ASPAs);

* The timestamp of the last modification to the static configuration;

* Read/write errors of static configuration;

* Any other relevant information.

To convey this information, a new BMP message type RPKI_SOURCE (Type = TBD1) SHOULD be defined. This message SHALL use the standard BMP common header followed by Type-Length-Value (TLV) elements per [I-D.ietf-grow-bmp-tlv]. TLVs SHALL be grouped per RPKI data source. Each group SHALL use a Group TLV to index Stateless parsing TLVs containing the above fields. A dedicated TLV within each group SHOULD specify the source type to ensure consistency and scalability.

5. RPKI Policy Configuration

BMP SHOULD report the RPKI-related policy configuration, which may be applied globally (uniformly applied across all peers) or on a per-peer basis (For example, only applied to the provider). The reported information SHOULD include:

* The enablement status of RPKI validation;

* The enabled set of validation rules derived from RPKI data, such as VRPs or ASPA entries;

* If enabled, the configured actions for routes with Invalid or Not-Found states.

To convey this information, a new BMP message type RPKI_POLICY (Type = TBD2) SHOULD be defined. For global policy configurations, this message SHALL comprise the BMP common header followed by TLVs that specify the validation rules and the actions associated with each non-valid state (i.e., Invalid and Not-Found), such as filtering, priority reduction, tagging, etc. For per-peer policy configurations, the message SHALL include an additional per-peer header, followed by TLVs that detail the RPKI rules and policies specific to each peer.

Note that since the size of the total validation rule set could be really large, BMP could only convey the route features of enabled validation rules. These features could be logical combination (AND/OR) of a series of conditions (the origin ASes should be within a certain set, the origin ASes should be a certain role such as the customer, the rule source should only be static or iBGP, etc). The network administrator could combine the features and per-route specific information in the next section to obtain the total validation rules.

6. Route Validation with RPKI

BMP SHOULD be extended to report both statistical summaries of validation results on a per-peer basis and detailed validation information for each route. For each peer, BMP messages SHOULD include counts of received routes categorized by their RPKI validation states. To improve clarity and emphasize RPKI-specific data, it is RECOMMENDED that a dedicated RPKI Statistics Message RPKI_STAT(Type = TBD3) be introduced by enhancing the original Statistics Report Message.This message specifically report the following RPKI-related statistics:

* The number of routes in each validation state: Valid, Invalid, and Not-Found;

* Optional statistics, such as the number of routes filtered as a result of RPKI validation.

This separation enhances readability and could easily extend to support any future RPKI-related objects.

For any individual route, since it may go through multiple types of validations, and may hit multiple validation rules, BMP SHOULD report not only the overall validation state, but also every validation rule which is hit. Therefore, for per-route validation report, it is RECOMMENDED that a dedicated Validation Report Message RPKI_VALIDATION (Type = TBD4) be defined, by enhancing the original Route Monitoring Message with additional TLVs. These TLVs should describe:

* The overall validation state, including Valid, Invalid or Unknown;

* The types of validations the route goes through;

* The information of all relevant validation rules, including the rule content (ROA entry for origin validation, ASPA entry for path validation, AS group set for region validation, etc), the data source, the expiration date, and the specific validation state for each rule.

Note that if the overall validation state is Valid, the specific validation state for every relevant validation rule should be valid; if the overall validation state is Unknown, there shouldn’t be any relevant validation rule; if the overall validation state is Invalid, there should be at least one relevant validation rule whose specific validation state is Invalid.

7. Impact of RPKI Validation on Routing

BMP SHOULD report the consequences of RPKI validation on route selection, with a particular focus on routes whose selection status is altered by RPKI validation:

* Routes that are demoted due to RPKI validation (i.e., routes that would have been selected as the best path without RPKI but are not selected when RPKI is enabled);

* Routes that are promoted due to RPKI validation (i.e., routes that would not have been selected as the best path without RPKI but are selected when RPKI is enabled).

For each route affected by RPKI validation, the BMP extension SHOULD report:

* The validation information, as detailed in the Route Validation stage;

* The actions applied to the route following validation, such as degradation of preference, attribute tagging, or exclusion from the selection process.

Furthermore, the BMP message SHOULD include information about the alternate best route:

* For routes demoted due to RPKI, the message SHOULD report the new best route selected with RPKI enabled;

* For routes promoted due to RPKI, the message SHOULD report the best route that would have been selected without RPKI.

This facilitates a direct comparison of routing decisions with and without RPKI, thereby enhancing the understanding of RPKI's influence on BGP path selection.

To enable per-route reporting of RPKI's impact on BGP routing, it is RECOMMENDED that a dedicated Validation Impact Message RPKI_IMPACT (Type = TBD5) be defined, by enhancing the original Route Monitoring Message with additional TLVs, to capture changes in route handling due to RPKI validation and policies. When a route is affected— such as being dropped, deprioritized, or superseded by another route-due to RPKI validation, such message could be triggered to report the incident. This message SHOULD include:

* The prefix and attributes of the affected route;

* The RPKI validation state of the affected route;

* Details of all the relevant RPKI validation rules of the affected route;

* The policy action enforced on the affected route (e.g., drop, reduce priority, tag);

* Information of the alternate best route, including its prefix, attributes, and RPKI validation state.

8. Security Considerations

8.1. Transmission Security

To ensure the integrity and authenticity of the transmitted monitoring data on RPKI, BMP MUST support the following requirements:

* Protocol safety: BMP MUST employ either TCP Authentication Option (TCP-AO) [RFC5925] or Transport Layer Security (TLS) to encrypt the monitoring sessions.

* data integrity: BMP should enforce mechanism like end-to-end signatures to ensure the integrity of critical data such as ROA validation result fields and AS_PATH change records, and validate the integrity of the received data prior to extracting the content of the data to prevent the propagation of tampered or corrupted information. The signing/verification keys could be dynamically derived from the RPKI certificate authority chain or managed through other secure mechanisms, and form a cross-verification mechanism with the source AS validation results of BGP UPDATE messages (where applicable) to prevent malicious rollback or tampering of the related monitoring data during transmission.

8.2. Operational Security

To ensure the extended BMP aligns with router's original configuration, BMP MUST support the followign requirements:

* Protocol transparency: The monitoring data collection must strictly adhere to the "zero-intrusion" principle. For operations involving the RTR protocol [RFC8210], only read-only interfaces are permitted to retrieve certificate synchronization status, and any modification to the router's local RPKI cache tree structure is prohibited. The polling frequency of monitoring probes should be restricted, and appropriate memory access layer protections must be implemented to prevent cache reconstruction triggered by monitoring data extraction. Additionally, the acquisition of collected ROA validation records should not interfere with real-time traffic processing.

* Forward compatibility: When the router does not enable the monitoring function recommended by this standard, or when the monitoring function fails, its native RPKI validation process [RFC6811] and BGP decision logic must maintain full functional consistency to prevent unintended routing policy changes caused by the monitoring mechanism.

9. IANA Considerations

This document requires IANA to assign values for new BMP message types (TBD1-TBD5) and their associated TLVs. The registration procedures for these assignments SHALL follow the policy outlined in [RFC7854].

10. References

10.1. 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>.

[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>.

[RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", RFC 5925, DOI 10.17487/RFC5925, June 2010, <https://www.rfc-editor.org/info/rfc5925>.

[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-23, 22 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-23>.

[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>.

[RFC6483] Huston, G. and G. Michaelson, "Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)", RFC 6483, DOI 10.17487/RFC6483, February 2012, <https://www.rfc-editor.org/info/rfc6483>.

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2012, <https://www.rfc-editor.org/info/rfc6811>.

[RFC6810] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol", RFC 6810, DOI 10.17487/RFC6810, January 2013, <https://www.rfc-editor.org/info/rfc6810>.

[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>.

[I-D.ietf-grow-bmp-tlv]
Lucente, P. and Y. Gu, "BMP v4: TLV Support for BGP Monitoring Protocol (BMP) Route Monitoring and Peer Down Messages", Work in Progress, Internet-Draft, draft-ietf-grow-bmp-tlv-19, 10 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-grow-bmp-tlv-19>.

10.2. Informative References

[I-D.ietf-grow-bmp-path-marking-tlv]
Cardona, C., Lucente, P., Francois, P., Gu, Y., and T. Graf, "BMP Extension for Path Status TLV", Work in

Progress, Internet-Draft, draft-ietf-grow-bmp-path-marking-tlv-04, 25 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-grow-bmp-path-marking-tlv-04>.

[I-D.ietf-grow-bmp-rel]
Lucente, P. and C. Cardona, "Logging of routing events in BGP Monitoring Protocol (BMP)", Work in Progress, Internet-Draft, draft-ietf-grow-bmp-rel-04, 3 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-grow-bmp-rel-04>.

[I-D.ietf-grow-bmp-bgp-rib-stats]
Srivastava, M., Liu, Y., Lin, C., and J. Li, "Advanced BGP Monitoring Protocol (BMP) Statistics Types", Work in Progress, Internet-Draft, draft-ietf-grow-bmp-bgp-rib-stats-11, 17 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-grow-bmp-bgp-rib-stats-11>.

Authors' Addresses

Shuhe Wang
Beijing Zhongguancun Laboratory
Building 8, CourtYard 1, Zhongguancun East Road, Haidian District
Beijing
China
Email: wangsh@mail.zgclab.edu.cn

Mingwei Xu
Beijing Zhongguancun Laboratory
Building 8, CourtYard 1, Zhongguancun East Road, Haidian District
Beijing
China
Email: xmw@cernet.edu.cn

Yangyang Wang
Beijing Zhongguancun Laboratory
Building 8, CourtYard 1, Zhongguancun East Road, Haidian District
Beijing
China
Email: wyy@cernet.edu.cn

Jia Zhang
Beijing Zhongguancun Laboratory
Building 8, CourtYard 1, Zhongguancun East Road, Haidian District
Beijing
China
Email: zhangj@mail.zgclab.edu.cn