idr
Internet-Draft
Intended status: Standards Track
Expires: 9 August 2026

M. Huang
Zhongguancun Laboratory
N. Geng
Huawei Technologies
D. Li
Tsinghua University
S. Yue
China Mobile

5 February 2026

# RPKI-based BGP Origin Attestation
# draft-huang-idr-bgp-origin-attestation-00

## Abstract

The Resource Public Key Infrastructure (RPKI) provides a framework for Route Origin Validation (ROV), but its deployment faces two critical challenges: 1) high false positive rates for "invalid" states and the operational burden these create; 2) incremental deployment has been hindered by limited immediate value when ROA coverage is incomplete and ROV deployment remains sparse.

This document proposes a paradigm shift from reactive ROV validation to proactive origin attestation. We introduce two complementary mechanisms: 1) "Pre-validation before propagation" where routers validate self-originated routes against local RPKI Verified ROA Payload (VRP) cache before advertisement, holding invalid routes for operator intervention; and 2) A BGP extension that carries cryptographically signed origin attestation in BGP UPDATE messages.

Unlike traditional ROV which only validates against outband RPKI-based ROAs, this approach enables originating ASes to actively attest to the legitimacy of their routes. This provides immediate security benefits even with partial deployment: each deploying AS gains stronger protection for its own prefixes, and downstream ASes receive clearer signals to distinguish legitimate routes from potential hijacks. The mechanisms dramatically reduce false positives while creating a deployable path toward comprehensive route origin security.

## Status of This Memo

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

This Internet-Draft will expire on 9 August 2026.

## Copyright Notice



## Table of Contents

# 1. Introduction

## 1.1. Motivation and Paradigm Shift

The Resource Public Key Infrastructure (RPKI) [RFC6480] and Route Origin Validation (ROV) [RFC6811] represent significant advancements in inter-domain routing security. However, after more than a decade of development, actionable deployment (where invalid routes are dropped rather than merely monitored) remains limited among network operators.

The fundamental challenge is not the lack of security benefits, but the operational cost of deployment. Current ROV implementations suffer from persistent false positive "invalid" states, primarily due to registration and propagation mismatches between RPKI management plane and router control plane [Right_the_Ship] [Demystifying_RPKI-Invalid_Prefixes]. For the downstream ASes point of view, these false positives create urgent operational burdens that outweigh the security benefits. Meanwhile, most operators-- especially incubent operators have very strict announcing prefixes management process, they have a stronger motivation and direct capability to protect the prefixes they announce, which is not well leveraged in the current mechanism that relies on offline ROA signing and validation by downstream ASes.

This document proposes a paradigm shift in how we approach route origin security. Instead of focusing solely on validating routes against out-of-band RPKI-based ROA records (a reactive model), we introduce a proactive model where originating ASes proactively cross-verify their locally originated routes against their local RPKI cache data, and ensuring consistency before actively attesting to the legitimacy of their routes through cryptographic signatures.

This shift addresses the core deployment challenges:

1. It enables actionable 'drop' policies by drastically reducing false positives. This is achieved through a layered approach at the origin. First, enforcing consistency between the RPKI management plane and the router control plane eliminates false positives caused by configuration errors. Second, and crucially, the 'validate-before-advertise' principle, combined with the ability for the origin AS to attest its announced prefixes and

validation result, directly tackles the problem of transient false positives caused by RPKI data synchronization delays across different ASes. While perfect global synchronization is impractical, this mechanism allows downstream ASes to distinguish between a true hijack and a mere synchronization lag, dramatically reducing both the frequency and operational difficulty of handling invalid states.

2. It provides immediate, "selfish" security benefits to break the deployment deadlock. Each originating AS that deploys these mechanisms gains stronger protection against hijacking for its own announced prefixes from day one, independent of widespread adoption. This creates a clear and compelling value proposition for first movers, solving the classic coordination problem where no single party has sufficient incentive to deploy alone.

3. It creates a powerful virtuous cycle by shifting operational responsibility toward the origin. The core innovation is moving the burden of verification and troubleshooting to the originating AS. By performing self-validation and attesting its routes, an AS ensures the "cleanliness" of its announcements. For every downstream AS, this translates to a significant reduction in emergency operational alerts and manual investigation. As more ASes deploy, the aggregate operational burden across the ecosystem decreases while routing confidence increases for everyone. This cooperative model establishes a strong, self-reinforcing incentive loop.

### 1.2. Key Innovations

This specification introduces two complementary innovations:

1. *Pre-validation before propagation*: Routers validate their own originated routes against local RPKI cache before advertisement. Routes that would be "invalid" are held for operator intervention, preventing false positives or route misconfiguration from entering the global routing table.

2. *BGP Origin Attestation Extension*: A new optional transitive BGP path attribute that carries cryptographically signed origin attestation. This allows originating ASes to actively declare the validity of their routes, providing downstream ASes with stronger signals for validation decisions.

Together, these mechanisms transform RPKI from a purely reactive validation system into a proactive attestation framework that provides deployable security benefits at every stage of adoption.

### 1.3. Terminology

Pre-validation: The process of validating self-originated routes against local RPKI cache before advertisement to BGP neighbors.

Origin Attestation (OA): The act of an originating AS cryptographically signing its route advertisement to declare its legitimacy.

BGP Origin Attestation Extension (BGP-OA): The BGP path attribute defined in this document that carries origin attestation information.

Originating Router (OR): A router that supports pre-validation and the generation of the BGP-OA extension for locally originated prefixes.

Downstream Router (DSR): A router that supports verification and processing of the received BGP-OA extension.

Enablement Status of Origin Attestation (OA-Status): The operational state of the Origin Attestation function on a router. It includes two steady states (Disabled, Enabled) and two transient states (Enabling, Disabling), as defined in Section 4.1.

Origin Route Cache (OR-Cache): A cache maintained by an OR containing its originated routes and their corresponding pre-validation results when OA-Status is Enabled.

Attested Origin Prefix List (AOPL): A list maintained by a DSR containing prefixes attested by all ORs of an AS, along with their corresponding origin router ID and attested validation state.

### 1.4. 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. Problem Statement and Deployment Challenges

1.The False Positive Problem

According to RPKI monitoring data, there are thousands of global IPv4 routes that are validated as invalid based on ROA records, with less than 1% are true positives caused by router control plane errors. The main scenarios leading to false positive judgments include:

* Timing mismatches between ROA publication and route advertisement. Research [RPKI_Time-of-Flight] indicates that the average delay in ROA publication is about 10 minutes with a widely dispersed distribution, the maximum delay can exceed 100 minutes.

* Configuration errors or untimely updates in the RPKI management plane. For example, incorrect ASN or Maxlength settings in ROA records, as well as stale ROA records after service migration.

2.Operational Barriers to Actionable ROV

For operators considering enabling ROV with drop actions for invalid routes, false positives represent an unacceptable operational burden. Each event requires immediate investigation, disrupts change control procedures, and its handling cost can exceed the perceived security benefits. As a result, the number of operators who have effectively deployed and are operating ROV remains small, and most of these deployments are primarily in monitoring mode, which delays response to actual hijacks.

3.The Incremental Deployment Dilemma

The security benefits of traditional ROV depend on both widespread ROA coverage and widespread actionable ROV deployment. Inadequate ROV deployment becomes a bottleneck restricting the incentive for comprehensive ROA coverage, creating a circular dependency that hinders overall progress.

4.Asymmetric Security Benefits

The current RPKI model creates an imbalance between the private costs (operational burden, complexity, risk of self-inflicted outages) borne by an operator and the public benefits (improved global routing security). This imbalance has been a significant barrier to widespread adoption of actionable ROV.

## 3. Solution Overview: RPKI-based BGP Origin Attestation

### 3.1. Architecture Principles

The proposed solution is built on four core principles:

1. *Cross-plane consistency as a security primitive*: Requiring consistency between the RPKI management plane (ROAs) and the router control plane (route configuration) before route advertisement dramatically reduces error rates. This proactive check prevents both hijacking-prone misconfigurations and false-positive-causing ROA errors at the source.

2. *Proactive declaration over reactive validation*: Originating ASes actively declare route legitimacy through attestations, rather than relying solely on downstream validation against potentially stale or incomplete ROA data. This leverages the origin AS's strong willingness and capability to protect its routes.

3. *Actionable ROV on Downstream ASes*: Downstream ASes must be empowered to identify real hijacks with high accuracy and minimal operational overhead. Enhanced source-level information (attestations) is key to breaking the bottleneck in effective downstream ROV deployment.

4. *Incremental deployability*: The system MUST provide tangible security benefits at every stage of deployment, not just at full adoption. Early benefits should accrue primarily to the deploying origin AS to create a self-reinforcing incentive loop.

### 3.2. Security Paradigm Shift

This proposal enables the paradigm shift for route origin security - from passive validation to active attestation:

--Traditional ROV (reactive): BGP UPDATE -> Query local RPKI cache -> Determine validity -> Act

--Proposed Model (proactive): Prepare route -> Self-validate -> Attest legitimacy -> Advertise with attestation -> Downstream verification

### 3.3. Value of the Solution

This solution provides the following benefits:

1. Leveraging the willingness and capability of the origin: By performing cross-validation between the RPKI management plane and the origin AS control plane, errors can be detected and corrected at the source to the greatest extent, preventing hijacking misjudgments caused by RPKI ROA misconfigurations or prefix hijacks resulting from router control plane misconfigurations.

2. "Validate before announce" mechanism at the origining AS: This can significantly reduce both the scale and duration of transient false positives experienced by downstream ASes due to RPKI data propagation delays.

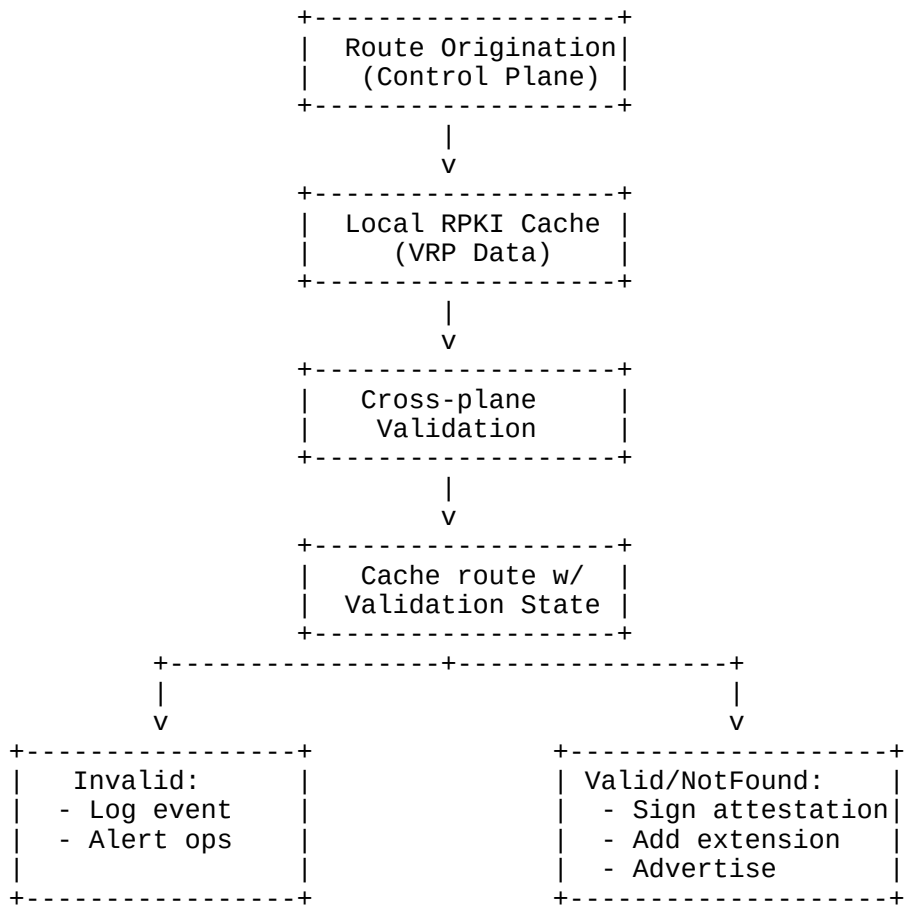
3. Route origin legitimacy attestation in the router control plane: Provides real-time and completeness guarantees that the RPKI ROA plane cannot offer, clearing obstacles for downstream ASes to promptly identify and handle transient false positives and prefix hijacks related to the origin AS.

4. Initiates a positive feedback loop: Origin deployment -> error correction -> attestation delivery -> enables effective downstream ROV -> encourages further origin deployment.

## 4. Protocol Specification

### 4.1. Conceptual Model: Pre-validation Before Propagation

The pre-validation mechanism operates at the boundary between route origination and advertisement:



An OR’s implementations of pre-validation MUST:

1. Perform ROV validation on all self-originated routes before advertisement to any BGP neighbor.

2. Maintain a cache (OR-Cache) of originated routes and their validation results.

3. Provide configurable logging and alerting for invalid routes.

4. Revalidate cached routes when the local RPKI cache is updated. If the validation result changes for a cached route, update the cache and take appropriate action (e.g., adertertise route with BGP-OA, log an alert).

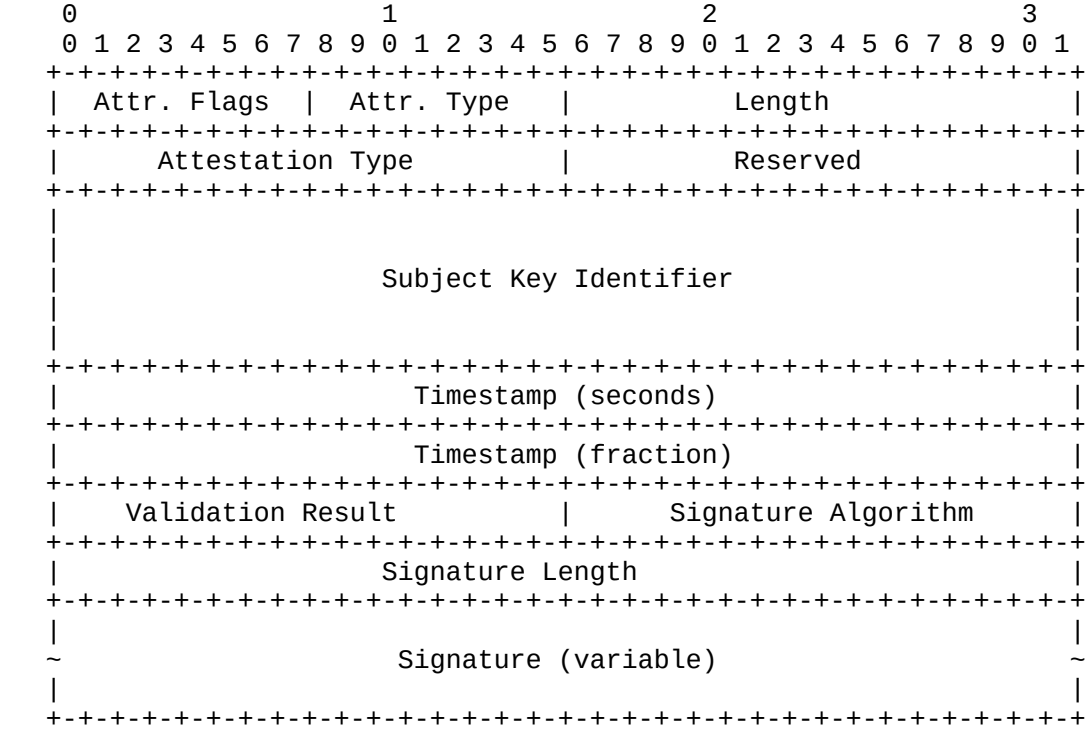
A DSR’s implementation of ingress origin validation, building upon traditional RPKI-based ROV, MUST:

1. Perform route origin validation and policy enforcement based on different combination of the local ROV result and the pre-validation result attested by the origin.

2. Support incremental deployment scenarios, allowing partial BGP-OA deployment within the origin AS.

### 4.2. BGP Origin Attestation Extension

The Origin Attestation is carried in a new optional transitive BGP path attribute. The value part of the attribute has the following format:




Where:

* Attr. Flags: Set to 0xC0 (Optional, Transitive, Extended-Length bit).

* Attr. Type: TBD by IANA

* Length: Total attribute length in octets

* Attestation Type: A 16-bit field indicating attestation properties (see detailed definition below)

* Subject Key Identifier (SKI): A 20-octet identifier that contains the value in the Subject Key Identifier extension of the RPKI router certificate [RFC6487].

* Timestamp: 64-bit NTP timestamp [RFC5905] of attestation creation

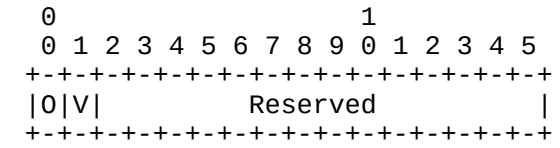
* Validation Result: The ROV validation result from the originator's perspective at the time of signing. 1 = Valid 2 = NotFound (no matching ROA found) 3 = Not-applicable (pre-validation was not performed, e.g., during OA disabling procedure)

* Signature Algorithm: Algorithm identifier used for signature (see IANA registry)

* Signature Length: Length of the signature field in octets

* Signature: Digital signature as specified below

The Attestation Type field is defined as:




* O-bit (bit 0): Origin Attestation Enabled. 1 indicates the OR's OA-Status is Enabled. 0 indicates it is Disabled.

* V-bit (bit 1): Strict Validation Filter. 1 indicates the OR only advertises routes with a pre-validation result of Valid. 0 indicates it advertises routes with results of either Valid or NotFound. The 'valid-only' strict mode would require operators to mandate that ROAs be signed for all originated routes. The subsequent processing flow for this mode has not been included in the description.

* Reserved (bits 3-15): MUST be set to zero on transmission and ignored on reception.

The signature covers the following elements in order:

1. The AS number of the originating AS (as it appears in the AS_PATH attribute).

2. The NLRI (prefix and length) being advertised in this BGP UPDATE.

3. The SKI (from the attribute)

4. Timestamp (from the attribute)

5. The Validation Result (from the attribute)

6. The Attestation Type (from the attribute)

The signature MUST be created using the originating router's private key. The corresponding public key and its binding to the (ASN, SKI) pair MUST be distributed through RPKI router certificates, following the key distribution model defined for BGPSec in [RFC8209].

Downstream routers verifying the signature MUST:

1. Retrieve the router certificate based on (ASN, SKI) pair, to get the appropriate router ID and public key.

2. Verify the signature covers all required elements as listed above.

3. Check that the Timestamp is recent (within a configured validity window, e.g., 24 hours) to prevent replay attacks.

4. If any check fails, the BGP-OA attribute MUST be considered invalid, and the route SHOULD be treated as if the attestation is not present (following local policy for un-attested routes).

# 5. Originating Router Procedures

## 5.1. OA-Status Management

The state machine of OA-Status is defined as follows:

* Disabled (initial state): The Origin Attestation function is not active. BGP UPDATEs do not contain the BGP-OA attribute.

* Enabling (transient): Entered from Disabled upon receiving an "Enable OA" command. The OR performs necessary setup (e.g., ensures RPKI-RTR [RFC8210] session is up, VRP and router keys are cached). It MUST NOT advertise routes with the BGP-OA attribute in this state.

* Enabled (steady state): Entered from Enabling once all prerequisites are met (local RPKI data ready, SKI and signing keys available). In this state, the OR MUST perform pre-validation and include a valid BGP-OA attribute (with O-bit=1) in UPDATEs for originated routes that pass local policy.

* Disabling (transient): Entered from Enabled upon receiving a "Disable OA" command. The OR continues to include the BGP-OA attribute in UPDATEs but sets the O-bit=0. This state MUST be maintained for a minimum period (e.g., 30 minutes) or until all relevant BGP sessions have been re-established, to ensure downstream ASes receive the disabled-state notification.

* Transition from Disabling to Disabled occurs after the minimum notification period. In Disabled state, BGP-OA attributes are no longer included.

### 5.2. Originating a Route

When originating a route, an OR with OA-Status=Enabled MUST:

1. Perform pre-validation against the local RPKI VRP cache.

2. Cache the route and its validation result (Valid, NotFound, Invalid) in the OR-Cache.

3. If the result is "invalid": a. MUST NOT advertise the route. b. MUST log a detailed error and SHOULD alert the operator.

4. If the result is Valid or NotFound (and local policy permits advertisement): a. Create a BGP-OA attribute as per Section 4.2. b. Include the attribute in the BGP UPDATE message. c. Advertise the route to neighbors

Initial Propagation: Upon first entering the Enabled state, the OR MUST reannounce all the routes with the BGP-OA extension.

Disabling Procedure: When transitioning to the Disabling state, the OR SHOULD send BGP UPDATE messages for its attested routes that include the BGP-OA attribute with the O-bit set to 0. This serves as an explicit notification to downstream ASes about the impending deactivation of OA functionality. To ensure robust cleanup and minimize the risk of the notification being lost due to transient network issues, the following steps are RECOMMENDED:

1. Sustained Notification: The OR SHOULD remain in the Disabling state for a minimum period (e.g., 30 minutes). During this period, it SHOULD periodically (e.g., every 5 minutes) re-advertise affected routes with the BGP-OA attribute (O-bit=0, Validation Result set to Not-applicable). This increases the likelihood that downstream ASes receive the state change notification.

2. Final Cleanup: After the minimum notification period, the OR transitions to the Disabled state. At this point, for each affected route that is still valid and should be advertised, the OR SHOULD send a BGP UPDATE message without the BGP-OA attribute. Optionally, for a more definitive cleanup, the OR MAY first send a WITHDRAW for the route and then (if the prefix remains valid) immediately follow it with an UPDATE without the BGP-OA attribute.

This two-phase approach (explicit notification via O-bit=0 followed by cleanup) ensures that downstream ASes are both informed of the state change and that the final routing state is consistent with the OA functionality being disabled.

### 5.3. Handling ROA Cache Updates

When the local VRP cache is updated and the OA-status is "Enabled", the OR MUST: a. Revalidate affected routes in the OR-Cache. b. If a route’s validation result changes from Invalid to Valid/NotFound: i. Generate a new BGP-OA attribute. ii. Advertise the route with the new attestation. c. If a route’s validation result changes from Valid/NotFound to Invalid: i. Update the OR-Cache. ii. Log a detailed error and SHOULD alert the operator.

## 6. Downstream Router Procedures

A DSR MUST have a functional RPKI-RTR session and current VRP/router key cache before processing BGP-OA attributes.

Case A: UPDATE Contains a BGP-OA Attribute

1.Perform Standard ROV: Validate the route using the local RPKI VRP cache. Let Local_ROV_Result be {Valid, NotFound, Invalid}.

2.Verify OA Signature: Extract the (ASN, SKI) from the path and attribute. Retrieve the corresponding public key and router ID from the local RPKI router key cache, verify the signature. If verification fails, discard the BGP-OA attribute and process the route as an un-attested route (go to Case B).

3.Process OA-Status:

* If O-bit=1 (Enabled): Record/update the OA-Status for this (ASN, Router ID) as active. Add/update the prefix in the AOPL for this AS, associated with the router ID and the Attested_Validation_Result from the attribute.

* If O-bit=0 (Disabled): Update the OA-Status for this (ASN, Router ID) as inactive. Remove the router’s entries from the AOPL for this AS. If a prefix has no attesting routers left, remove it from the list. Process the route as an un-attested route (go to Case B).

4.Compare Results (if O-bit=1 and signature valid):

* If Local_ROV_Result and Attested_Validation_Result are the same (Valid/Valid or NotFound/NotFound): Mark the route as Strongly Validated. Propagate the UPDATE with the BGP-OA attribute intact.

* If Local_ROV_Result is Invalid but Attested_Validation_Result is Valid: Check the Timestamp for freshness. If recent, this indicates a likely RPKI cache synchronization delay (transient false positive). The DSR MAY decide to accept/propagate the route while monitoring the situation, or apply a local policy (e.g., lower LOCAL_PREF). It SHOULD schedule a re-check after its next RPKI cache sync.

* If Local_ROV_Result is Valid but Attested_Validation_Result is NotFound or vice versa: This is a minor discrepancy. The DSR SHOULD log it but can treat the route as validated. The more secure result (Valid) MAY be given preference.

Case B: UPDATE Does NOT Contain a BGP-OA Attribute

1.Perform standard ROV, yielding Local_ROV_Result.

2.Check the Attested Origin Prefix List for the origin AS.

* If the prefix is in the list (attested by other routers from the same AS), the DSR has collective attestation knowledge. It MAY use the attested state(s) from the list to inform its decision, similar to step A.4 above, to mitigate false positives.

* If the prefix is not in the list, process based on Local_ROV_Result and local policy only.

## 7. Security Considerations

Trust Model: The security of Origin Attestation relies fundamentally on the RPKI trust anchor hierarchy and the correct binding of router keys to AS resources via RPKI certificates [RFC8209]. Compromise of an origin AS’s RPKI signing key or router private key allows for forged attestations.

Replay Attacks: The mandatory Timestamp field and its verification limit the window for replay attacks. Operators should configure an appropriate validity period (e.g., 24 hours).

Partial Deployment Security: An AS with only partial BGP-OA deployment on its ASBRs is less protected against hijacks via its non-deploying ASBRs. Downstream ASes using collective attestation knowledge (Section 6.1.B) should be aware of this reduced security guarantee for prefixes not fully attested.

Key Management: Secure key generation, storage, and timely rollover procedures as specified for BGPSec [RFC8209] are equally critical for OA.

Algorithm Agility: The Signature Algorithm field provides agility. If a cryptographic weakness is found in the default algorithm, a new algorithm ID can be assigned. Transition mechanisms should be defined in a future update.

## 8. Operation and Management Consideration

Incremental Deployment: It is RECOMMENDED that an AS enables BGP-OA on all its external-facing ASBRs (especially those facing providers) for comprehensive protection. The protocol is designed to function with partial deployment, but coverage gaps remain vulnerable.

Minimizing Oscillation: Operators should avoid frequent enable/ disable toggles. Implementations SHOULD enforce a minimum time between state changes. The use of the transient Disabling state with sustained notification helps ensure downstream cleanup without needing a full Route Refresh.

Troubleshooting: The primary point for diagnosing and resolving attestation or validation issues should be the originating AS, as it has full visibility into its RPKI data and route configuration. ORs MUST provide comprehensive logging for pre-validation failures.

Interaction with BGP Path Selection: The validation state derived from BGP-OA processing MAY influence BGP path selection. It is RECOMMENDED that this influence be implemented as a tie-breaking rule after standard criteria like LOCAL_PREF and AS_PATH length, similar to the VALID > NOT-VALID rule for BGPSec [RFC8205]. For example, a path with a Strongly Validated state (attested and locally Valid) could be preferred over a path with only local Valid or NotFound validation.

## 9. IANA Considerations

This document requests IANA to:

* Assign a new BGP path attribute type code from the "BGP Path Attributes" registry for the Origin Attestation attribute. Suggested value: TBD1.

* Create a new registry titled "BGP Origin Attestation Parameters" under the "Border Gateway Protocol (BGP) Parameters" group. This registry shall include the following sub-registries:

* Attestation Type Flags: Registry for bits in the Attestation Type field. Initial contents: bit 0 (O-bit), bit 1 (V-bit), bit 2 (R-bit). Registration policy: Standards Action or IESG Approval.

* Validation Result Codes: Registry for the 2-byte Validation Result field. Initial values: 1 (Valid), 2 (NotFound), 3 (Not-applicable). Registration policy: Standards Action or IESG Approval.

* Signature Algorithms: Registry for the 2-byte Signature Algorithm field. This registry MAY initially reuse values defined for BGPSec's Algorithm Suite ID in the "BGPSec Algorithm Suite IDs" registry [RFC8208]. Registration policy: Specification Required.

# 10. References

## 10.1. Normative References

[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>.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, DOI 10.17487/RFC6487, February 2012, <https://www.rfc-editor.org/info/rfc6487>.

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2013, <https://www.rfc-editor.org/info/rfc6811>.

[RFC8205] Lepinski, M., Ed. and K. Sriram, Ed., "BGPsec Protocol Specification", RFC 8205, DOI 10.17487/RFC8205, September 2017, <https://www.rfc-editor.org/info/rfc8205>.

[RFC8208] Turner, S. and O. Borchert, "BGPsec Algorithms, Key Formats, and Signature Formats", RFC 8208, DOI 10.17487/RFC8208, September 2017, <https://www.rfc-editor.org/info/rfc8208>.

[RFC8209] Reynolds, M., Turner, S., and S. Kent, "A Profile for BGPsec Router Certificates, Certificate Revocation Lists, and Certification Requests", RFC 8209, DOI 10.17487/RFC8209, September 2017, <https://www.rfc-editor.org/info/rfc8209>.

[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>.

### 10.2. Informative References

[RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, DOI 10.17487/RFC5905, June 2010, <https://www.rfc-editor.org/info/rfc5905>.

[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>.

[RPKI_Time-of-Flight] "RPKI Time-of-Flight", March 2023, <https://dl.acm.org/doi/10.1007/978-3-031-28486-1_18>.

[Right_the_Ship] "Assessing the Legitimacy of Invalid Routes in RPKI", November 2025, <https://dl.acm.org/doi/10.1145/3719027.3744853>.

[Demystifying_RPKI-Invalid_Prefixes] "Demystifying RPKI-Invalid Prefixes - Hidden Causes and Security Risks", February 2026, <https://weitongli.com/publications/papers/li-2026-demystifying.pdf>.

## Authors' Addresses

Mingqing Huang
Zhongguancun Laboratory
Beijing
China
Email: huangmq@zgclab.edu.cn

Nan Geng
Huawei Technologies
Beijing
China
Email: gengnan@huawei.com

Dan Li
Tsinghua University
Beijing
China
Email: tolidan@tsinghua.edu.cn

Shengnan Yue
China Mobile
Beijing
China
Email: yueshengnan@chinamobile.com