Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: 7 March 2026

L. Poulopoulos
S. Boudjema
H. Siddique
Verisign

3 September 2025

Route Origin Authorization (ROA) Governance for Anycasted Services with Unique Origin ASNs
draft-pbs-sidrops-roaanycast-00

Abstract

This document describes a set of best practices for the management of Route Origin Authorizations (ROAs) used to certify globally anycasted services with unique origin autonomous system numbers (ASNs) per node. It identifies key risk areas related to anycast-based ROA publication and how to mitigate technical risk for RPKI operations.

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 7 March 2026.

Table of Contents

1. Introduction 2
1.1. Conventions Used in This Document 3
2. Single-prefix Minimal ROAs 4
3. Sequential-Use EE Certificate 4
4. Single Signing Time 4
5. Synchronous Operations 4
6. IANA Considerations 5
7. Security Considerations 5
8. References 5
8.1. Normative References 5
8.2. Informative References 6
Authors' Addresses 6

1. Introduction

Anycasting, the origination of a prefix from multiple nodes, is an internet design pattern for improving the performance, stability and resiliency of global networks and is commonly implemented by DNS, CDN and DDoS protection service operators. This approach can result in lower latency and can simplify fail-over. An anycast node can be easily taken offline via withdrawl of its BGP route, causing traffic to automatically shift to other available nodes.

Anycast services originating from unique origin ASNs per node [RFC6382], originate a single prefix from multiple distinct ASNs. The approach allows for more precise monitoring and troubleshooting of routing anomalies or hijacks. The primary benefit is enhanced observability of anycasted services, especially when a large number of nodes are in operation.

This design (distinct origin ASNs) calls for specific considerations when publishing Route Origin Authorizations (ROA). Certifying origins of a Multiple Origin Autonomous System (MOAS) prefix implies the existence of a set of ROAs to certify all origins of the prefix. Given the exclusive nature of route origin validation (ROV), partial ROA coverage of MOAS prefixes MUST be avoided, as it would result in "INVALID" prefix/origin pairs for non-covered origins. In this instance, absence of coverage is preferable over partial coverage as it would make all prefix/origin pairs resolve to RPKI "UNKNOWN".

This document presents a set of recommendations meant to avoid partial ROA coverage of MOAS prefixes, by ensuring shared fate among the set of ROAs covering them.

1.1. Conventions Used in This Document

Anycast: the practice of making a particular service address available in multiple, discrete, autonomous nodes, such that datagrams sent are routed to one of several available nodes [RFC4786].

Multi-origin Autonomous System: a particular setup of Anycast routing, where each node originating the same service is identified by a unique Autonomous System Number (ASN) [RFC6382].

The terms "MOAS Service" and "MOAS Prefix" are used throughout this document as a convenience shorthand for the more verbose "Globally Anycasted Service with Unique Origin Autonomous System Numbers per Node".

The terms "covering", "covered", when used to describe the effect of a ROA on a prefix/origin pair, are to be interpreted in the intuitive sense of "certified by". They are not to be interpreted in the more restrictive sense employed by other writings, where "covering" only applies to the prefix of a prefix/origin pair [RFC6811] [RFC6483].

They key words "VALID", "INVALID" and "UNKNOWN", are to be interpreted as RPKI validity states as described in [RFC6483] when, and only when, they appear in all capitals, as shown here. 巽 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. Single-prefix Minimal ROAs

Separate ROAs SHOULD be published for each prefix/origin-AS pair of the MOAS prefix. This entails that these ROAs should contain a single prefix and the maximal length should be equal to the prefix length, i.e., be minimal ROAs [RFC9319].

Doing so, ensures that routes of a MOAS prefix do not share fate with unrelated resources.

3. Sequential-Use EE Certificate

A set of ROAs covering origins of a MOAS prefix SHOULD be signed using the same End-Entity (EE) certificate (a.k.a. "sequential use" EE certificate [RFC6487]).

This guarantees a common validity period among all origins of the prefix, avoiding partial expiry or partial revocation within the ROA set.

Moreover, using a single EE certificate for all ROAs covering a MOAS prefix avoids unnecessary CRL bloating.

4. Single Signing Time

A set of ROAs covering origins of a MOAS prefix SHOULD present the same CMS signing time attribute.

This practice may also have positive consequences if the publication point uses the CMS signing time as a reference to override filesystem timestamps [RFC9589] [I-D.ietf-sidrops-publication-server-bcp].

5. Synchronous Operations

Signing, publication and withdrawal of ROAs covering origins of a MOAS prefix SHOULD be synchronous to ensure shared fate among them and avoid partial coverage.

In the context of the RPKI publication protocol [RFC8181], clients SHOULD request publication or withdrawal of all ROAs related to the MOAS prefix as part of a single publication query message, preferably avoiding operations on resources unrelated to the MOAS prefix. Reciprocally, publication servers SHOULD honor atomicity of transactions requested as part of a single query message.

When creating ROAs as the consequence of the addition of new origin node to a MOAS service, ROAs covering existing nodes of the prefix SHOULD be renewed at the same time to preserve common signing and validity times among all origins of the prefix.

More broadly, any modification to a ROA covering a MOAS prefix SHOULD be accompanied by changes to all ROAs covering the same MOAS prefix to preserve uniform validity attributes across the set. Consequently, these changes SHOULD be published within a single RPKI Repository Delta Protocol (RRDP) serial increment, to ensure synchronicity on the relying party end [RFC8182].

6. IANA Considerations

This document makes no requests of IANA.

7. Security Considerations

This section will be added later based on community review and feedback

8. References

8.1. 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>.

[RFC4786] Abley, J. and K. Lindqvist, "Operation of Anycast Services", BCP 126, RFC 4786, DOI 10.17487/RFC4786, December 2006, <https://www.rfc-editor.org/info/rfc4786>.

[RFC6382] McPherson, D., Donnelly, R., and F. Scalzo, "Unique Origin Autonomous System Numbers (ASNs) per Node for Globally Anycasted Services", BCP 169, RFC 6382, DOI 10.17487/RFC6382, October 2011, <https://www.rfc-editor.org/info/rfc6382>.

[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>.

[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>.

[RFC8181] Weiler, S., Sonalker, A., and R. Austein, "A Publication Protocol for the Resource Public Key Infrastructure (RPKI)", RFC 8181, DOI 10.17487/RFC8181, July 2017, <https://www.rfc-editor.org/info/rfc8181>.

[RFC8182] Bruijnzeels, T., Muravskiy, O., Weber, B., and R. Austein, "The RPKI Repository Delta Protocol (RRDP)", RFC 8182, DOI 10.17487/RFC8182, July 2017, <https://www.rfc-editor.org/info/rfc8182>.

[RFC9319] Gilad, Y., Goldberg, S., Sriram, K., Snijders, J., and B. Maddison, "The Use of maxLength in the Resource Public Key Infrastructure (RPKI)", BCP 185, RFC 9319, DOI 10.17487/RFC9319, October 2022, <https://www.rfc-editor.org/info/rfc9319>.

[RFC9589] Snijders, J. and T. Harrison, "On the Use of the Cryptographic Message Syntax (CMS) Signing-Time Attribute in Resource Public Key Infrastructure (RPKI) Signed Objects", RFC 9589, DOI 10.17487/RFC9589, May 2024, <https://www.rfc-editor.org/info/rfc9589>.

8.2. Informative References

[I-D.ietf-sidrops-publication-server-bcp] Bruijnzeels, T., de Kock, T., Hill, F., Harrison, T., and J. Snijders, "RPKI Publication Server Best Current Practices", Work in Progress, Internet-Draft, draft-ietf-sidrops-publication-server-bcp-03, 24 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-publication-server-bcp-03>.

[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 2013, <https://www.rfc-editor.org/info/rfc6811>.

Authors' Addresses

L. Poulopoulos
Verisign
Route du Petit Moncor 1E
CH-1752 Villars sur Glane
Switzerland
Email: lpoulopoulos@verisign.com
URI: https://www.verisign.com/

S. Boudjema
Verisign
Route du Petit Moncor 1E
CH-1752 Villars sur Glane
Switzerland
Email: sboudjema@verisign.com
URI: https://www.verisign.com/

H. Siddique
Verisign
12061 Bluemont Way
Reston, VA 20190
United States
Email: hsiddique@verisign.com
URI: https://www.verisign.com/