; draft-zhang-rpki-roa-bcp-00
Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: 11 April 2026

H. Zhang
CNNIC
H. Zou
CNIC
L. Zhang
X. Yang
CNNIC
D. Ma
ZDNS
Y. Li
CNIC

8 October 2025

Best Current Practice for ROA Issuance Restrictions in RPKI
<https://datatracker.ietf.org/draft/draft-zhang-rpki-roa-bcp/>

Abstract

This document specifies best current practices for Resource Public Key Infrastructure (RPKI) operators regarding Route Origin Authorizations (ROAs). It mandates that a parent Certification Authority (CA) MUST NOT issue ROAs for Internet number resources delegated to a child CA. RPKI certification authorities(CA software) and relying party software are required to enforce this restriction by rejecting or flagging invalid ROAs issued outside of resource allocations.

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 11 April 2026.

Table of Contents

1. Introduction

The Resource Public Key Infrastructure (RPKI) [RFC6480] provides a framework to secure the Internet routing by associating IP address blocks with public key certificates. Route Origin Authorizations(ROAs) [RFC9582] allow the holder of an IP prefix to authorize an Autonomous System (AS) to originate routes for that prefix.

In the RPKI hierarchy, IP resources are delegated from a parent Certification Authority (CA) to a child CA, transferring exclusive authority over those resources. However, some RPKI implementations permit parent CAs to issue ROAs for delegated resources, leading to conflicts and undermining the RPKI trust model.

This document establishes a Best Current Practice (BCP) to specify that only the entity holding the resource certificate with effective authority for a prefix may issue ROAs for that prefix. Effective authority is transferred to the child CA upon delegation, and the parent CA MUST NOT issue ROAs for those resources.

2. Terminology

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.

3. Problem Statement

When a parent CA delegates resources to a child CA, authority over those resources is exclusively transferred. According to the RPKI architecture [RFC6480], the parent CA relinquishes operational control and MUST NOT issue ROAs for delegated resources. However, in practice, some RPKI systems permit this leading to the following issues:

- Competing ROAs [RFC8211]: Multiple ROAs may exist for the same IP prefix, issued by both parent and child CAs.
- Validation ambiguity: Relying party (RP) software cannot prioritize between competing ROAs, including all valid ROAs in validated ROA payloads(VRPs). This may lead to routing decisions that conflict with the delegation model(e.g., a parent CA’s ROA for 192.0.2.0/24 authorizing AS1, and a child CA’s ROA for the same prefix authorizing AS2).
- Security risk: A malicious or compromised parent CA could issue ROAs to hijack routes or disrupt legitimate routing.

These issues directly affect the security and stability of the Internet routing system, as RPKI data is used to validate route origins and influence routing decisions.

4. Best Current Practice

To ensure consistency, security in the RPKI ecosystem, the following practices are RECOMMENDED:

- Parent CAs MUST NOT issue ROAs for resources delegated to a child CA. If legacy ROAs exist, the parent CA SHOULD revoke them in coordination with the child CA to minimize disruption.
- RPKI CA software MUST reject ROAs issued for resources outside the issuer’s certified resources, defined as those resources in the CA’s active certificate, excluding delegated portions.
- Relying party (RP) software SHOULD flag ROAs issued by a parent CA for resources delegated to a child CA, issuing warnings during validation. The detection rule is:verify if a parent CA’s ROA prefix overlaps with resources delegated to a child CA.
- It is RECOMMENDED that only leaf CAs(CAs that have not delegated resources further) issue ROAs. Restricting ROA issuance to leaf CAs clarifies authority, prevents overlapping or competing ROAs between parent and child CAs, and reduces risks of misconfiguration or misuse that could lead to routing incidents. If a non-leaf CA issues a ROA, RP software triggers an warning during validation. This recommendation is consistent with the above restriction on parent CAs and extends the principle by specifying that only CAs without further delegation (leaf CAs) should perform ROA issuance.
- In cases where a parent CA, such as a Regional Internet Registry (RIR), operates its own network and needs to issue ROAs for the resources it directly holds (i.e., resources not delegated to child CAs), it is RECOMMENDED that the parent CA create a dedicated subordinate CA for those resources. ROAs should then be issued from this subordinate CA, maintaining clear separation between allocation and operational roles.
- Operators of RPKI CAs SHOULD implement monitoring to detect ROA misconfigurations, with automated alerts for unauthorized issuance.
- Regional Internet Registries (RIRs) and other certification authorities are encouraged to update their RPKI documentation and user interfaces to clearly communicate these restrictions to end users.

5. Security Considerations

Failure to enforce ROA issuance restrictions can lead to serious security consequences, including:

- Route hijacking: An compromised parent CA could issue ROAs to redirect traffic.
- Routing blackhole: If a parent CA issues an ROA for a delegated prefix (e.g., 192.0.2.0/24 authorizing AS1) and the child CA, holding the same prefix, does not issue an ROA but announces via AS2, the route may be marked "Invalid" per [RFC6811], causing traffic to be dropped and resulting in a routing blackhole.
- Erosion of trust: Ambibuities in ROA authority reduce confidence in RPKI.

Strict enforcement at both the CA and relying party levels is essential to maintaining the integrity of the global routing system. This document reinforces the principle of least authority within the RPKI hierarchy.

6. Iana Considerations

This document has no IANA actions.

7. Special Considerations

In some operational environments, organizations may delegate resources internally to subsidiaries or business units. In such cases, the parent organization may still need to issue ROAs that cover subsidiary resources. The recommended practice is to avoid using the parent/child CA model for this purpose. Instead, the parent and subsidiary should share a common CA certificate within the same administrative domain, and implement internal controls to ensure that ROAs are issued according to IP allocation rules. This prevents conflicts and ensures compliance with the principle of least authority within the global RPKI framework.

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>.

[RFC9582] Snijders, J., Maddison, B., Lepinski, M., D. Kong, and S. Kent, "A Profile for Route Origin Authorizations (ROAs)", RFC 9582, DOI 10.17487/RFC9582, May 2024, https://www.rfc-editor.org/info/rfc9582

[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>.

8.2. Informative 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>.

[RFC6811] Bush, R., "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2013, <https://www.rfc-editor.org/info/rfc6811>.

[RFC8211] Kent, S. and A. Chi, "Adverse Actions by a Certification Authority (CA) or Repository Manager in the Resource Public Key Infrastructure (RPKI)", RFC 8211, DOI 10.17487/RFC8211, September 2017, <https://www.rfc-editor.org/info/rfc8211>.

Authors’ Addresses
Heng Zhang
CNNIC
Building 4, No.9 Beijing Auto Museum West Road
Beijing
100070
China
Email:zhangheng@cnnic.cn

Hui Zou
CNIC
CAS Informatization Plaza No.2 Dong Sheng Nan Lu
Beijing
100083
China
Email:zouhui@cnic.cn

Likun Zhang
CNNIC
Building 4, No.9 Beijing Auto Museum West Road
Beijing
100070
China
Email:zhanglikun@cnnic.cn

Xue Yang
CNNIC
Building 4, No.9 Beijing Auto Museum West Road
Beijing
100070
China
Email:yangx@cnnic.cn

Di Ma
ZDNS
21/F, Building B, Greenland Center, Building 7, Wangjingdongyuan Zone 4
Beijing
100102
China
madi@zdns.cn

Yanbiao Li
CNIC
CAS Informatization Plaza No.2 Dong Sheng Nan Lu
Beijing
100083
China
Email:lybmath@cnic.cn