SIDR Operations
Internet-Draft
Intended status: Best Current Practice
Expires: 8 October 2026

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

April 2026

Best Current Practice for ROA Issuance Restrictions in RPKI
draft-zhang-sidrops-rpki-roa-bcp-02

Abstract

This document specifies best current practices for Resource Public Key Infrastructure (RPKI) operators regarding Route Origin Authorizations (ROAs). It RECOMMENDS that a parent Certification Authority (CA) void issuing ROAs for Internet number resources delegated to a child CA. RPKI certification authorities(CA software) and relying party software are expected to support these practices by appropiate warning.

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 3 October 2026.

Copyright Notice

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. Upon delegation, the child CA typically gains effective operational 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) that RECOMMENDS restrictions on ROA issuance by parent CAs for delegated resources, while providing flexible operational guidance to support legitimate BGP practices such as announcing covering prefixes alongside more-specific customer announcements.

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. Problem Statement

When a parent CA delegates resources to a child CA, authority over those resources is generally expected transferred. However, parent CAs sometimes issue ROAs for those delegated resources. This can lead 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. Note that this BCP primarily mitigates misconfigurations rather than providing complete protection against a fully malicious parent CA, which retains other powers (e.g., certificate revocation or resource modification)

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.

3. Best Current Practice

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

* Parent CAs SHOULD 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 SHOULD warn or reject ROAs issued for resources that have been delegated to a child CA (i.e., resources no longer within the issuer’s effective authority due to delegation).

* 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.

* Operational Guidance for Covering Prefixes and Customer Delegations:

  When an ISP holds a covering prefix (e.g., a /16) and delegates a more-specific prefix (e.g., a /24) to a customer:

  - If the delegation occurs within the same administrative domain or the ISP wishes to retain operational control, the shared CA model is RECOMMENDED. The ISP and customer operate under a common CA certificate. This allows the ISP to issue ROAs for both the covering prefix and the more-specific delegation, supporting common BGP practices such as announcing an aggregate alongside customer more-specifics. In such cases, creating a separate child CA is NOT RECOMMENDED and is often discouraged.

  - If the customer requires full control (independent ROA management and announcement from a different origin AS), the parent/child CA model MAY be used. The child CA issues the ROA for the more-specific prefix, while the parent MAY retain a ROA for the covering prefix if needed for its own announcements. RP software SHOULD flag such overlapping ROAs for operator review but MUST NOT automatically invalidate them.

* 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.

4. IANA Considerations

This memo includes no request to IANA.

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.

This BCP primarily addresses misconfigurations and unintended authority overlaps. It does not prevent all possible actions by a malicious or compromised parent CA, which could still revoke child certificates, shrink resource sets, or re-delegate resources.

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. Special Considerations

In operational environments, organizations may delegate resources internally to subsidiaries or to external customers while needing to announce covering prefixes themselves.

When the more-specific prefix belongs to a different legal entity requiring independent control of its BGP announcements, the parent/child CA model may be necessary. This document does not invalidate such configurations, nor does it impact the validity of BGP announcements containing both covering prefixes and more-specifics. The focus is strictly on minimizing cryptographic authority conflicts to prevent validation ambiguity.

Resources MAY appear on multiple CA certificates for legitimate purposes such as key rollovers and make-before-break transfers.

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/rfc/rfc2119>.

[RFC9582] Snijders, J., Maddison, B., Lepinski, M., Kong, D., and S. Kent, "A Profile for Route Origin Authorizations (ROAs)", BCP 14, RFC 9582, DOI 10.17487/RFC9582, May 2024, <https://www.rfc-editor.org/rfc/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/rfc/rfc8174>.

7.2. 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/rfc/rfc6480>.

[RFC6811] Bush, B., "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2013, <https://www.rfc-editor.org/rfc/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/rfc/rfc8211>.

Authors' Addresses

Heng Zhang
CNNIC
Email: zhangheng@cnnic.cn

Hui Zou
CNIC
Email: zouhui@cnic.cn

Likun Zhang
CNNIC
Email: zhanglikun@cnnic.cn

Xue Yang
CNNIC
Email: yangx@cnnic.cn

Di Ma
ZDNS
Email: madi@zdns.cn

Yanbiao Li
CNIC
Email: lybmath@cnic.cn