Stream:	Internet Engineering Task Force (IETF)
RFC:	9455
BCP:	238
Category:	Best Current Practice
Published:	August 2023
ISSN:	2070-1721

Authors:	Z. Yan	R. Bush	G. Geng	T. de Kock	J. Yao
	CNNIC	*IIJ Research Lab & Arrcus, Inc.*	*Jinan University*	*RIPE NCC*	*CNNIC*

RFC 9455
Avoiding Route Origin Authorizations (ROAs) Containing Multiple IP Prefixes

Abstract

When using the Resource Public Key Infrastructure (RPKI), address space holders need to issue Route Origin Authorization (ROA) object(s) to authorize one or more Autonomous Systems (ASes) to originate BGP routes to IP address prefix(es). This memo discusses operational problems that may arise from ROAs containing multiple IP prefixes and recommends that each ROA contain a single IP prefix.

Status of This Memo

This memo documents an Internet Best Current Practice.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on BCPs is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9455.

Table of Contents

1. Introduction

In the RPKI, a ROA, which is a digitally signed object, identifies that a single AS has been authorized by the address space holder to originate BGP routes to one or more IP prefixes within the related address space [RFC6482].

Each ROA contains an asID field and an ipAddrBlocks field. The asID field contains a single AS number that is authorized to originate routes to the given IP address prefix(es). The ipAddrBlocks field contains one or more IP address prefixes to which the AS is authorized to originate the routes.

If the address space holder needs to authorize more than one AS to advertise the same set of IP prefixes, multiple ROAs must be issued (one for each AS number [RFC6480]). Prior to this document, there was no guidance recommending the issuance of a separate ROA for each IP prefix or a single ROA containing multiple IP prefixes.

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

An address space holder can issue a separate ROA for each of its routing announcements. Alternatively, for a given asID, it can issue a single ROA for multiple routing announcements, or even for all of its routing announcements. Since a given ROA is either valid or invalid, the routing announcements for which that ROA was issued will "share fate" when it comes to RPKI validation. Currently, no existing RFCs provide recommendations about what kinds of ROAs to issue: one per prefix or one for multiple routing announcements. The problem of fate-sharing was not discussed or addressed.

In the RPKI trust chain, the Certification Authority (CA) certificate issued by a parent CA to a delegatee of some resources may be revoked by the parent at any time, which would result in changes to resources specified in the certificate extensions defined in [RFC3779]. Any ROA object that includes resources that are a) no longer entirely contained in the new CA certificate or b) contained in a new CA certificate that has not yet been discovered by Relying Party (RP) software will be rejected as invalid. Since ROA invalidity affects all routes specified in that ROA, unchanged resources with associated routes via that asID cannot be separated from those affected by the change in CA certificate validity. They will fall under this invalid ROA even though there was no intent to change their validity. Had these resources been in a separate ROA, there would be no change to the issuing CA certificate and therefore no subsequent invalidity.

CAs have to carefully coordinate ROA updates with updates to a resource certificate. This process may be automated if a single entity manages both the parent CA and the CA issuing the ROAs (Scenario D in [RFC8211], Section 3.4). However, in other deployment scenarios, this coordination becomes more complex.

As there is a single expiration time for the entire ROA, expiration will affect all prefixes in the ROA. Thus, changes to the ROA for any of the prefixes must be synchronized with changes to other prefixes, especially when authorization for a prefix is time bounded. Had these prefixes been in separately issued ROAs, the validity interval would be unique to each ROA, and invalidity would only be affected by reissuance of the specific issuing parent CA certificate.

A prefix could be allowed to originate from an AS only for a specific period of time, for example, if the IP prefix was leased out temporarily. If a ROA with multiple IP prefixes was used, this would be more difficult to manage, and potentially be more error-prone. Similarly, more complex routing may require changes in asID or routes for a subset of prefixes. Reissuance of a ROA might result in changes to the validity of previously received BGP routes covered by the ROA's prefixes. There will be no change to the validity of unaffected routes if a) the time-limited resources are in separate ROAs, or b) for more complex routing, each change in asID or a change in routes for a given prefix is reflected in a change to a discrete ROA.

The use of ROA with a single IP prefix can minimize these side effects. It avoids fate-sharing irrespective of the cause, where the parent CA issuing each ROA remains valid and where each ROA itself remains valid.

4. Recommendations

Unless the CA has good reasons to the contrary, an issued ROA **SHOULD** contain a single IP prefix.

5. Security Considerations

Issuing separate ROAs for independent IP prefixes may increase the file-fetch burden on the RP during validation.

6. IANA Considerations

This document has no IANA actions.

7. 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>.

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, DOI 10.17487/RFC3779, June 2004, <https://www.rfc-editor.org/info/rfc3779>.

[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>.

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, DOI 10.17487/RFC6482, February 2012, <https://www.rfc-editor.org/info/rfc6482>.

[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>.

[RFC8211] Kent, S. and D. Ma, "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>.

Acknowledgements

The authors wish to thank the following people for their reviews and contributions to this document: George Michaelson, Tim Bruijnzeels, Job Snijders, Di Ma, Geoff Huston, Tom Harrison, Rob Austein, Stephen Kent, Christopher Morrow, Russ Housley, Ching-Heng Ku, Keyur Patel, Cuiling Zhang, and Kejun Dong. Thanks are also due to Sean Turner for the Security Area Directorate review.

This work was supported by the Beijing Nova Program of Science and Technology under grant Z191100001119113.

Authors' Addresses

Zhiwei Yan
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing
100190
China
Email: yanzhiwei@cnnic.cn

Randy Bush
IIJ Research Lab & Arrcus, Inc.
5147 Crystal Springs
Bainbridge Island, Washington 98110
United States of America
Email: randy@psg.com

Guanggang Geng
Jinan University
No.601, West Huangpu Avenue
Guangzhou
510632
China
Email: gggeng@jnu.edu.cn

Ties de Kock
RIPE NCC
Stationsplein 11
Amsterdam
Netherlands
Email: tdekock@ripe.net

Jiankang Yao
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing
100190
China
Email: yaojk@cnnic.cn