Network Working Group
Internet-Draft
Intended status: Informational
Expires: 19 March 2026

T. Bruijnzeels
RIPE NCC
M. Hoffmann
K. van Hove
NLnet Labs

15 September 2025

Change Publication Server used by an RPKI CA
draft-timbru-sidrops-change-pubserver-01

Abstract

This document outlines how an RPKI CA can migrate from one RFC 8181 Publication Server to another. The process is similar to the RPKI CA Key Rollover process defined in RFC 6489, except that in this case a new location is used for the new key.

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 19 March 2026.

Table of Contents

1. Requirements notation

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. Introduction

There are a number of reasons why a CA may wish to migrate from its current Publication Server to a new one.

One reason may be that an organization is running their own Publication Server, but wishes to migrate to a server operated by their parent (e.g., a Regional Internet Registry), possibly because their parent did not offer this service when they first set up their CA, but now they do.

Another reason may be that the current Publication Server used by a CA is falling behind in terms of their availability on either the publication protocol [RFC8181], or the public rsync or RRDP [RFC8182] repository compared to other options.

If the current Publication Server has become unavailable and there is no sign that it will become available again, then that may constitute an even more urgent reason to migrate to a new server.

This document describes a modified RPKI Key Rollover [RFC6489] process that can be used to change the Publication Server used by an RPKI CA.

3. Migration Process

This section assumes familiarity with RPKI Key Rollovers [RFC6489].

The migration process is similar to the process described in section 2 of [RFC6489] with some notable differences that we will describe below.

This document uses the three CA states CURRENT, NEW and OLD as described in section 2 of [RFC6489].

3.1. Upload new Repository Response

Before initiating the Publication Server migration the relationship between the publishing CA and the new server MUST be estiblished and verified.

First, a Publisher Request XML file MUST be retrieved from the CA. The CA MAY re-use the same XML and BPKI TA certificate that was used for the setup of the current Publication Server for this purpose.

Then, the Publication Server MAY generate a Repository Response XML file for this CA. If the Publication Server refuses to execute this step, then the migration MUST be cancelled.

When the CA receives the Respository Response XML file it MUST verify that it can communicate with the new server by sending it an [RFC8181] list query. If the query is successful, the new server is accepted and the CA proceeds to the next step. If the query is unsuccessful then the migration process MUST be cancelled.

3.2. Create new Key

The second step in the process is to generate a key pair for the NEW CA, and then request a new certificate for it from its parent as described in steps 1 and 2 in section 2 of [RFC6489].

3.3. Use the new Key

The NEW CA MUST reissue all signed certificates and RPKI signed objects as described in section 4 of [RFC6489] and publish them at its (new) Publication Server.

This is necessary because if the NEW CA were to delay re-issuance and publication until it is promoted to become the CURRENT CA and the then OLD CA is revoked immediately as described in steps 3-6 in section 2 of [RFC6489], then this would lead to a situation where no certificates and RPKI signed objects could be found by RP software due to timing issues in fetching both repositories. This issue does not apply to the normal [RFC6489] Key Rollover process as all the updates would be published at the same Publication Server in that case as a single atomic delta.

3.4. Staging Period

During the staging period the CA MUST maintain signed content under both its current and new key, and MUST ensure that these are in sync.

A staging period of 24 hours SHOULD be used to avoid any race conditions where RP software was not yet able to get the content from the NEW CA repository before revoking the CURRENT CA as per the next step in this process.

However, if there is any operational issue with the Publication Server and/or its repository used by the CURRENT CA then this staging period SHOULD be skipped.

After the staging period has passed, or has been skipped, the CURRENT CA becomes the OLD CA and NEW CA becomes the CURRENT CA.

3.5. Revoke OLD CA

The final step in the process is that the OLD CA MUST be revoked by sending an [RFC6492] revocation request for its key. Furthermore, all content for the OLD CA SHOULD be removed from the (old) Publication Server used by it. Note that this may be impossible in cases where a non-functioning Publication Server prompted this migration.

The private key for the OLD CA MUST be destroyed.

4. Relying Party Considerations

4.1. Authority Information Access

It should be noted that the Authority Information Access (AIA) URIs for delegated CA certificates will change when the NEW CA key and repository are used.

Relying Parties MAY warn when AIA URIs in the RPKI signed objects (Manifest, ROAs, etc) and possible certificates (delegated CA or BGPSec Router Certificates) published do not match the location of the signing CA certificate in the new publication point, but they MUST accept them as long as they are otherwise valid.

5. Implementation Status

This section is to be removed if and before this document becomes an RFC.

Version -00 of this document is implemented by [krill] release 0.9.2 and later.

6. IANA Considerations

OID needs to be requested.

7. Security Considerations

TBD

8. Acknowledgements

TBD

9. 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>.

[RFC6489] Huston, G., Michaelson, G., and S. Kent, "Certification Authority (CA) Key Rollover in the Resource Public Key Infrastructure (RPKI)", BCP 174, RFC 6489, DOI 10.17487/RFC6489, February 2012, <https://www.rfc-editor.org/info/rfc6489>.

[RFC6492] Huston, G., Loomans, R., Ellacott, B., and R. Austein, "A Protocol for Provisioning Resource Certificates", RFC 6492, DOI 10.17487/RFC6492, February 2012, <https://www.rfc-editor.org/info/rfc6492>.

[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>.

10. Informative References

[krill] NLnet Labs, "krill", <https://github.com/NLnetLabs/krill>.

Authors' Addresses

Tim Bruijnzeels
RIPE NCC
Email: tbruijnzeels@ripe.net
URI: https://www.ripe.net/

Martin Hoffmann
NLnet Labs
Email: martin@nlnetlabs.nl
URI: https://www.nlnetlabs.nl/

Koen van Hove
NLnet Labs
Email: koen@nlnetlabs.nl
URI: https://www.nlnetlabs.nl/