SIDROPS
Internet-Draft
Updates: 6487 (if approved)
Intended status: Standards Track
Expires: 4 September 2025

J. Snijders
B. Maddison
Workonline
T. Buehler
OpenBSD
3 March 2025

Relying Party Handling of Resource Public Key Infrastructure (RPKI) Certificate Revocation List (CRL) Number Extensions
draft-ietf-sidrops-rpki-crl-numbers-02

Abstract

This document clarifies how Resource Public Key Infrastructure (RPKI) Relying Parties (RPs) handle Certificate Revocation List (CRL) Number extensions. This document updates RFC 6487.

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 4 September 2025.

Table of Contents

1. Introduction

Section 5.2.3 of [RFC5280] describes the value of the Certificate Revocation List (CRL) Number extension as a monotonically increasing sequence number, which "allows users to easily determine when a particular CRL supersedes another CRL~~.~~". In other words, in Public Key Infrastructures (PKIs) in which it is possible for Relying Parties (RPs) to encounter multiple usable CRLs, the CRL Number extension is a means for ~~the~~ an RP to determine which ~~CRL(s)~~CRLs to rely upon.

In the Resource Public Key Infrastructure (RPKI), a well-formed Manifest FileList contains exactly one entry for its associated CRL, together with a collision-resistant message digest of that ~~CRLs~~ CRL's contents (see Section 2.2 of [RFC6481] and Section 2 of [RFC9286]). Additionally, the target of the CRL Distribution Points extension in an RPKI Resource Certificate is the same CRL object listed on the issuing Certification Authorities (CAs) current manifest (see Section 4.8.6 of [RFC6487]). Together, these properties guarantee that RPKI RPs will always be able to unambiguously identify exactly one current CRL for each RPKI CA. Thus, in the RPKI, the ordering functionality provided by CRL Numbers is fully subsumed by monotonically increasing Manifest Numbers (Section 4.2.1 of [RFC9286]), thereby obviating the need for RPKI RPs to process CRL Number extensions at all.

Therefore, although the CRL Number extension is mandatory in RPKI CRLs for compliance with the X.509 v2 CRL Profile (Section 5 of [RFC5280]), any use of this extension by RPKI RPs merely adds complexity and fragility to RPKI Resource Certificate path validation. This document mandates that RPKI RPs MUST ignore the CRL Number extension.

This document updates [RFC6487] with clarifications for RP implementers. Refer to Section 2 for more details.

Commenté [MB1]: Redundant with the changes below. Please avoid use of normative language here but point to Section 2

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.

1.2. Related Work

It is assumed that the reader is familiar with the terms and concepts described in "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" [RFC5280] and "A Profile for Resource Certificate Repository Structure" [RFC6481].

1.3. Changes from RFC 6487

This section summarizes the significant changes between [RFC6487] and this document.

* Clarifications for handling of CRL Numbers for RPs.

* ~~Incorporated~~ Integration of RFC 6487 Errata 3205.

2. Updates to RFC 6487

This section updates Section 5 of [RFC6487~~].~~] as follow:

* ~~In Section 5, this paragraph is changed~~First change:~~.~~

OLD

| Where two or more CRLs are issued by the same CA, the CRL with
| the highest value of the "CRL Number" field supersedes all
| other CRLs issued by this CA.

NEW

| When issuing a new CRL, the CA SHOULD use a monotonically
| increasing sequence number in the "CRL Number" extension to aid
| debugging efforts. It is RECOMMENDED that the "CRL Number"
| matches the "manifestNumber" of the manifest that will include
| this CRL (see Section 4.2.1 of [RFC9286]).

* ~~In Section 5, this paragraph is changed.~~Second change:

OLD

| An RPKI CA MUST include the two extensions, Authority Key
| Identifier and CRL Number, in every CRL that it issues. RPs
| MUST be prepared to process CRLs with these extensions. No
| other CRL extensions are allowed.

NEW

| An RPKI CA MUST include exactly two extensions in every CRL
| that it issues: an Authority Key Identifier (AKI) and a CRL
| Number. No other CRL extensions are allowed.
|
| - RPs MUST process the AKI extension.
|
| - RPs MUST ignore the CRL Number extension except for checking
| that it is marked as non-critical and contains a non-
| negative integer less than or equal to 2^159-1.

Commenté [MB2]: For consistency with the previous item

Commenté [MB3]: Given that both changes are in Section 5

Commenté [MB4]: We need to check if this is conflicting with «Each CA MUST issue a version 2 CRL that is consistent with [RFC5280]. » +
«The CRL number is a non-critical CRL extension that conveys a monotonically increasing sequence number for a given CRL scope and CRL issuer.»

May be consider to amend that sentence as well.

3. Security Considerations

The Security Considerations of [RFC3779], [RFC5280], and [RFC6487] apply to Resource Certificates and CRLs.

This document clarifies that, in the RPKI, there is exactly one CRL appropriate and relevant for determining the revocation status of a given resource certificate. It is the unique CRL object that is simultaneously:

* the target of the certificate's CRL Distribution Points extension, and

* listed in the issuing CA's current Manifest FileList and has matching hash (see Section 4.2.1 of [RFC9286]).

This is a more stringent requirement than is generally used in other X.509 PKIs. It is therefore important for RPs to use an implementation of the X.509 path validation algorithm that allows specifying the CRL objects to use for each of the intermediate CAs and the leaf.

Commenté [MB5]: Any ops/deployment implications of this updates?

Anything we can insist on from Section 9 of 6487: «It would not be appropriate to introduce a new extension, or authorize use of an extant, standard extension, for a security-relevant purpose on a piecemeal basis. »

4. IANA Considerations

This document has no IANA actions.

5. References

5.1. 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>.

[RFC6481] Huston, G., Loomans, R., and G. Michaelson, "A Profile for Resource Certificate Repository Structure", RFC 6481, DOI 10.17487/RFC6481, February 2012, <https://www.rfc-editor.org/info/rfc6481>.

[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>.

[RFC9286] Austein, R., Huston, G., Kent, S., and M. Lepinski, "Manifests for the Resource Public Key Infrastructure (RPKI)", RFC 9286, DOI 10.17487/RFC9286, June 2022, <https://www.rfc-editor.org/info/rfc9286>.

5.2. Informative References

[FORT] Leiva, A., "FORT validator", <https://fortproject.net/en/validator>.

[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>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[routinator] NLnetLabs, "Routinator", <https://github.com/NLnetLabs/routinator>.

[rpki-client] Jeker, C., Snijders, J., Dzonsons, K., and T. Buehler, "rpki-client", June 2024, <https://www.rpki-client.org/>.

Appendix A. Implementation status - RFC EDITOR: REMOVE BEFORE PUBLICATION

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in RFC 7942. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to RFC 7942, "this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit".

* OpenBSD [rpki-client]

* [FORT]

* [routinator]

Acknowledgements

The authors wish to thank Tom Harrison whose observations prompted this ~~internet-draft proposal~~document, ~~and~~ Alberto Leiva, and Tim Bruijnzeels for valuable feedback.

Authors' Addresses

Job Snijders
Amsterdam
The Netherlands

Email: job@sobornost.net

Ben Maddison
Workonline
Cape Town
South Africa
Email: benm@workonline.africa

Theo Buehler
OpenBSD
Switzerland
Email: tb@openbsd.org