Internet Engineering Task Force (IETF)
Request for Comments: 9829
Updates: 6487
Category: Standards Track
ISSN: 2070-1721

J. Snijders

B. Maddison
Workonline

T. Buehler
OpenBSD

July 2025

Handling of Resource Public Key Infrastructure (RPKI) Certificate Revocation List (CRL) Number Extensions

Abstract

This document revises how the Resource Public Key Infrastructure (RPKI) handles Certificate Revocation List (CRL) Number extensions. This document updates RFC 6487.

Status of This Memo

This is an Internet Standards Track document.

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 Internet Standards 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/rfc9829.

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 an RP to determine which 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 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 ignore the CRL Number extension.

This document updates [RFC6487]. Refer to Section 3 for more details.

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

The reader is assumed to be familiar with the terms and concepts described in "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" [RFC5280], "A Profile for Resource Certificate Repository Structure" [RFC6481], and "Manifests for the Resource Public Key Infrastructure (RPKI)" [RFC9286].

1.3. Changes from RFC 6487

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

* Revision of CRL Number handling.

* Adjustment of step 5 of the Resource Certification Path Validation.

* Integration of Errata 3205 [Err3205].

2. Summary

This document clarifies that, in the RPKI, there is exactly one CRL that is 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 a matching hash (see Section 4.2.1 of [RFC9286]).

In particular, a resource certificate cannot be validated without consulting the current manifest of the certificate's issuer.

3. Updates to RFC 6487

3.1. Updates to Section 5

This section updates Section 5 of [RFC6487] as follows:

* 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

  | Per Section 5.2.3 of [RFC5280], CAs issue new CRLs using a
  | monotonically increasing sequence number in the "CRL Number"
  | extension. It is RECOMMENDED that the "CRL Number" match the
  | "manifestNumber" of the manifest that will include this CRL
  | (see Section 4.2.1 of [RFC9286]).

* 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.

3.2. Update to Section 7.2

This section updates Section 7.2 of [RFC6487] as follows:

OLD

| 5. The issuer has not revoked the certificate. A revoked
| certificate is identified by the certificate's serial number
| being listed on the issuer's current CRL, as identified by the
| CRLDP of the certificate, the CRL is itself valid, and the
| public key used to verify the signature on the CRL is the same
| public key used to verify the certificate itself.

NEW

| 5. The issuer has not revoked the certificate. A revoked
| certificate is identified by the certificate's serial number
| being listed on the issuer's current CRL, as identified by the
| issuer's current manifest and the CRLDP of the certificate.
| The CRL is itself valid and the public key used to verify the
| signature on the CRL is the same public key used to verify the
| certificate itself.

4. Operational Considerations

This document has no additional operational considerations beyond those described in Section 9 of [RFC6487].

5. Security Considerations

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

This document explicates that, in the RPKI, the CRL listed on the certificate issuer's current manifest is the one relevant and appropriate for determining the revocation status of a resource certificate. The hash in the manifest's fileList provides a cryptographic guarantee on the Certification Authority's intent that this is the most recent CRL and removes possible replay vectors.

6. IANA Considerations

This document has no IANA actions.

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/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>.

7.2. Informative References

[Err3205] RFC Errata, Erratum ID 3205, RFC 6487, <https://www.rfc-editor.org/errata/eid3205>.

[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>.

Acknowledgements

The authors wish to thank Tom Harrison whose observations prompted this document, Alberto Leiva, Tim Bruijnzeels, Mohamed Boucadair, Geoff Huston, and the IESG for their valuable comments and 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