Workgroup: Network Working Group
Internet-Draft:
draft-spaghetti-sidrops-rpki-validation-update-03
Obsoletes: 8360 (if approved)
Updates: 6482, 6487 (if approved)
Published: 7 November 2023
Intended Status: Standards Track
Expires: 10 May 2024
Authors: J. Snijders   B. Maddison
Fastly   Workonline

RPKI Validation Re-reconsidered

Abstract

This document describes an improved validation procedure for Resource Public Key Infrastructure (RPKI) signed objects. This document updates RFC 6482. This document updates RFC 6487. This document obsoletes RFC 8360.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction
  1.1. Requirements Language
2. Deprecation of RFC 8360
3. Updates to RFC 6482
4. Updates to RFC 6487
  4.1. Updates to Section 7.2
  4.2. Updates to Section 9
5. Implementation status - RFC EDITOR: REMOVE BEFORE PUBLICATION
6. Security Considerations
7. IANA Considerations
8. Acknowledgements
9. References
  9.1. Normative References
  9.2. Informative References
Authors' Addresses

1. Introduction

[RFC8360] describes an improved validation algorithm for signed objects published in the RPKI. This improved validation algorithm would help in situations such as described in this [Report]. However, analysis has shown the described procedure for deploying updates to the validation algorithm, as described in [RFC6487] Section 9, is impractical, and this specification is [incomplete].

This document deprecates the original [RFC6487] section 7 algorithm in favour of the [RFC8360] algorithm, and obsoletes [RFC8360] because a migration via those codepoints is infeasible. This document also deprecates the procedure set out in [RFC6487] section 9 for future changes to the validation algorithm.

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. Deprecation of RFC 8360

[RFC8360] defines several alternative OIDs for use in Resource Certificates [RFC6487]:

- *id-cp-ipAddr-asNumber-v2 - Section 4.2.1 [RFC8360]

* id-pe-ipAddrBlocks-v2 - Sections 4.2.2.1 and 4.2.2.2 [RFC8360]

* id-pe-autonomousSysIds-v2 - Sections 4.2.2.3 and 4.2.2.4 [RFC8360]

The stated purpose of the above OIDs is rendered obsolete by the updated specifications contained in this document.

Therefore:

* Issuing CAs MUST NOT include the above OIDs in newly issued Resource Certificates; and

* Relying parties encountering the above OIDs in Resource Certificates MUST proceed according to the updated procedures described below.

3. Updates to RFC 6482

This section updates Section 4 [RFC6482]. The following text:

> The IP address delegation extension [RFC3779] is present in the end-entity (EE) certificate (contained within the ROA), and each IP address prefix(es) in the ROA is contained within the set of IP addresses specified by the EE certificate's IP address delegation extension.

Is replaced with:

> Either the IP Address Delegation extension described in [RFC3779] or the alternative IP Address Delegation extension described in [RFC8360] (but not both) is present in the end entity (EE) certificate (contained within the ROA), and each IP address prefix(es) in the ROA is contained within the VRS-IP set that is specified as an outcome of EE certificate validation described in Section 7.2 (as updated by this document) [RFC6487].

Note that this ensures that ROAs can be valid only if all IP address prefixes in the ROA are encompassed by the VRS-IP of all certificates along the path to the trust anchor used to verify it.

Operators MAY issue separate ROAs for each IP address prefix, so that the loss of one or more IP address prefixes from the VRS-IP of any certificate along the path to the trust anchor would not invalidate authorizations for other IP address prefixes.

4. Updates to RFC 6487

This section updates [RFC6487] to specify an improved behavior of a Relying Party implementation.

4.1. Updates to Section 7.2

The following section replaces Section 7.2 [RFC6487] (Resource Certification Path Validation) in its entirety.

Validation of signed resource data using a target resource certificate consists of verifying that the digital signature of the signed resource data is valid, using the public key of the target resource certificate, and also validating the resource certificate in the context of the RPKI, using the path validation process.

There are two inputs to the validation algortihm:

1. A trust anchor

2. A certificate to be validated

The algorithm is initialized with two new variables for use in the RPKI: Verified Resource Set-IP (VRS-IP) and Verified Resource Set-AS (VRS-AS). These sets are used to track the set of INRs (IP address space and AS numbers) that are considered valid for each CA certificate. The VRS-IP and VRS-AS sets are initially set to the IP Address Delegation and AS Identifier Delegation values, respectively, from the trust anchor used to perform validation.

This path validation algorithm verifies, among other things, that a prospective certification path (a sequence of n certificates) satisfies the following conditions:

a. for all 'x' in {1, ..., n-1}, the subject of certificate 'x' is the issuer of certificate ('x' + 1);

b. certificate '1' is issued by a trust anchor;

c. certificate 'n' is the certificate to be validated; and

d. for all 'x' in {1, ..., n}, certificate 'x' is valid.

Certificate validation requires verifying that all of the following conditions hold, in addition to the certification path validation criteria specified in Section 6 of [RFC5280].

1. The signature of certificate x (x>1) is verified using the public key of the issuer's certificate (x-1), using the signature algorithm specified for that public key (in certificate x-1).

2. The current time lies within the interval defined by the NotBefore and NotAfter values in the Validity field of certificate x.

3. The Version, Issuer, and Subject fields of certificate x satisfy the constraints established in Sections 4.1 to 4.7 of RFC 6487.

4. If certificate x uses the Certificate Policy defined in Section 4.8.9 of [RFC6487], then the certificate MUST contain all extensions defined in Section 4.8 of [RFC6487] that must be present. The value(s) for each of these extensions MUST satisfy the constraints established for each extension in the respective sections. Any extension not thus identified MUST NOT appear in certificate x.

5. If certificate x uses the Certificate Policy defined in Section 4.2.4.1 [RFC8360], then all extensions defined in Section 4.8 of [RFC6487], except Sections 4.8.9, 4.8.10, and 4.8.11 MUST be present. The certificate MUST contain an extension as defined in Sections 4.2.4.2 or 4.2.4.3 [RFC8360], or both. The value(s) for each of these extensions MUST satisfy the constraints established for each extension in the respective sections. Any extension not thus identified MUST NOT appear in certificate x.

6. Certificate x MUST NOT have been revoked, i.e., it MUST NOT appear on a Certificate Revocation List (CRL) issued by the CA represented by certificate x-1.

7. Compute the VRS-IP and VRS-AS set values as indicated below:

   * If the IP Address Delegation extension is present in certificate x and x=1, set the VRS-IP to the resources found in this extension.

   * If the IP Address Delegation extension is present in certificate x and x>1, set the VRS-IP to the intersection of the resources between this extension and the value of the VRS-IP computed for certificate x-1.

   * If the IP Address Delegation extension is absent in certificate x, set the VRS-IP to NULL.

   * If the IP Address Delegation extension is present in certificate x and x=1, set the VRS-IP to the resources found in this extension.

   * If the AS Identifier Delegation extension is present in certificate x and x>1, set the VRS-AS to the intersection of the resources between this extension and the value of the VRS-AS computed for certificate x-1.

   * If the AS Identifier Delegation extension is absent in certificate x, set the VRS-AS to NULL.

8. If there is any difference in resources in the VRS-IP and the IP Address Delegation extension on certificate x, or the VRS-AS and the AS Identifier Delegation extension on certificate x, then a warning listing the overclaiming resources for certificate x SHOULD be issued.

These rules allow a CA certificate to contain resources that are not present in (all of) the certificates along the path from the trust anchor to the CA certificate. If none of the resources in the CA certificate are present in all certificates along the path, no subordinate certificates could be valid. However, the certificate is not immediately rejected as this may be a transient condition. Not immediately rejecting the certificate does not result in a security problem because the associated VRS sets accurately reflect the resources validly associated with the certificate in question.

4.2. Updates to Section 9

Section 9 "Operational Considerations for Profile Agility" is removed.

5. 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 RFC7942. 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.

As of today these changesets have been produced for commonly used Relying Party implementations:

*NLnet Labs Routinator [routinator]

*OpenBSD rpki-client [rpkiclient]

*FORT Validator [fort]

The 'public' OpenSSL X509v3_addr_validate_path() and X509v3_asid_validate_path() interfaces do not read the Policy OIDs. Also, these interfaces are not referenced outside OpenSSL itself: [codesearch] and [github].

At the time of writing there are zero (0) certificates in the RPKI carrying the extensions and policy defined in [RFC8360].

6. Security Considerations

The authors believe that the revised validation algortihm introduces no new security vulnerabilities into the RPKI, because it cannot lead to any ROA and/or router certificates to be accepted if they contain resources that are not held by the issuer.

7. IANA Considerations

IANA is requested to reference this document in the "SMI Security for PKIX Certificate Policies" registry at:

*id-cp-ipAddr-asNumber-v2

IANA is requested to reference this document in the "SMI Security for PKIX Certificate Extensions" registry at:

*id-pe-ipAddrBlocks-v2

*id-pe-autonomousSysIds-v2

IANA is requested to reference this document in the "SMI Security for PKIX Module Identifier" registry at:

*id-mod-ip-addr-and-as-ident-v2

*id-mod-ip-addr-and-as-ident-2v2

8. Acknowledgements

The authors would like to thank Tim Bruijnzeels, Mikael Abrahamsson, Nick Hilliard, and Peter Peele for their helpful review of this document.

9. References

9.1. 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>.

[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>.

[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>.

[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>.

[RFC8360] Huston, G., Michaelson, G., Martinez, C., Bruijnzeels, T., Newton, A., and D. Shaw, "Resource Public Key Infrastructure (RPKI) Validation Reconsidered", RFC 8360, DOI 10.17487/RFC8360, April 2018, <https://www.rfc-editor.org/info/rfc8360>.

9.2. Informative References

[codesearch] Debian, "Debian Codesearch", February 2021, <https://codesearch.debian.net/search?q=X509v3_addr_validate_path&literal=1>.

[fort] Snijders, J., "Harmonize RFC 8360 and RFC 6487 in FORT", February 2021, <https://github.com/job/FORT-validator/commit/ff5f4b9313d5c553fa13bae427acb69665977727>.

[github] Github, "Github Search", February 2021, <https://github.com/search?q=X509v3_addr_validate_path&type=commits>.

[incomplete] Snijders, J., "What are the RFC 5280 section 6.1.1 inputs for (c) (e) (f) (g) in context of RFC 8360?", October 2023, <https://mailarchive.ietf.org/arch/msg/sidrops/L02g9Z8OIUc1AOi_IoRViOvTSCY/>.

[Report] Snijders, J., "[routing-wg] RFC 8360 should be the default (Was: RPKI Outage Post-Mortem)", January 2021, <https://www.ripe.net/ripe/mail/archives/routing-wg/2021-January/004220.html>.

[routinator]
Snijders, J., "Harmonize RFC 8360 and RFC 6487 in rpki-rs", February 2021, <https://github.com/job/rpki-rs/commit/d9fa8c72cf83ed6f25e4420eaaa9054078f15bc3>.

[rpkiclient] Jeker, C., "rpki-client check IP and ASnum coverage only on ROAs", January 2021, <https://marc.info/?l=openbsd-tech&m=161011710120123&w=2>.

Authors' Addresses

Job Snijders
Fastly
Amsterdam
Netherlands

Email: job@fastly.com

Ben Maddison
Workonline
Cape-Town
South Africa

Email: benm@workonline.africa