Network Working Group
Internet-Draft
Intended status: Experimental
Expires: September 8, 2019

G. Michaelson
APNIC
T. Bruijnzeels
opennetlabs

March 7, 2019

Deployment of Reconsidered Validation in the Resource Public Key Infrastructure (RPKI)
draft-va-sidrops-deploy-reconsidered-01

Abstract

This document defines a deployment model for reconsidered validation [RFC8360] in the Resource Public Key Infrastructure (RPKI).

It stipulates that Relying Parties in the RPKI MUST support reconsidered validation by 1 July TBD-Year, and that Certificate Authorities MAY use the reconsidered validation OIDs in CA certificates that they issue from this date. Furthermore Certificate Authorities should monitor whether the set of resources in CA certificate they receive has shrunk, and make adjustments in the CA certificates and/or other RPKI objects when appropriate.

Table of Contents

1. Overview

This document defines a deployment model for reconsidered validation [RFC8360] in the Resource Public Key Infrastructure (RPKI).

Reconsidered validation differs from normal validation [RFC6487] in that under reconsidered rules the intersection of resources between a child certificate and the resources contained in the (chain of) parent certificate(s) is accepted. Any resources that are contained in the child certificate only result in a warning about these resources, rather than the rejection of that certificate. Thus reconsidered validation limits the impact of over-claims in the RPKI to the set of resources under dispute.

The applicability of reconsidered validation is signalled by the use of a distinct set of OIDs on a Resource Certificate [RFC8360]. Because of this reconsidered validation can only be deployed when a majority of Relying Party software is updated to support this new

algorithm. This document stipulates that RP software MUST support [RFC8360] by 1 July TBD-Year. After 1 July TBD-Year Certificate Authorities MAY start to use [RFC8360] in CA certificates that they issue.

Note that the use of reconsidered validation is restricted to CA Certificates only. Issuing Certificate Authorities may (be forced to) re-issue delegated CA certificates with shrunk resource pro-actively, and therefore it's at the CA certificate level that mismatches between resources actually included on such a certificate and the resources the recipient believes to be included on these certificates may occur.

On the other hand, ROA and BGPSec Router Certificate reconsidered validation still requires that all resources are also held by the path of parent certificates to these objects. In other words, using the reconsidered validation here is unneccessary.

Furthermore, Certificate Authorities should monitor pro-actively whether the set of resources in the CA certificate they received has been shrunk by their parent. Resource Certificates that they in turn issue that use resources no longer validly held by them should be shrunk or revoked. BGPSec Router Certificates or ROAs that use such resources should be removed.

1.1. 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.

2. Phased Deployment of the Amended Certificate Profile

There is an existing BCP document that describes an algorithm agility procedure for the RPKI [RFC6919]. This procedure involves four distinct phases with requirements for CAs and RPs. During this process the entire RPKI tree is essentially duplicated, and two disctinct trees are maintained in paralel for some time, until the old tree can be withdrawn. The dates for each milestones are expected to be documented in a BCP.

In this case however, the amended validation process is very similar to the existing validation process. Moreover, as [RFC8360] describes there is no fundamental issue in having an RPKI tree in which a mix of regular [RFC6487] and amended [RFC8360] certificates can be found.

The use of the amended certificate profile communicates that over-claims for this particular certificate can occur, and if they do, that their impact should be limited to the resources that are in over-claim. Sections 4.2.5 and 4.2.6 of [RFC8360] stipulate that such over-claims on the EE certificate would invalidate ROA and BGPSec Router Certificates.

In conclusion the amended certificate profile MUST only be used on CA certificates for CA organisations where an overclaim may accidentally occur, and MUST NOT be used anywhere else: e.g. on a TA CA certificate which by definition cannot overclaim, or on any specific attestation about resources other than a delegation to another CA, e.g. ROAs and BGPSec Router Certificates.

So, contrary to the process described in [RFC6919] there is no desired outcome here to completely replace an existing algorithm with a new algorithm. And consequently a different approach to the deployment phases is applicable here.

We recognise the following phases:

1. Relying Party software MUST support the amended profile

2. Operators MUST use updated Relying Party software;

3. Certificate Authorities MAY use the amended profile

As suggested in [RFC6919] the dates for each of these phases can be documented in this BCP:

1. 1 July TBD-Year

2. 1 July TBD-Year - 1 January TBD-Year +1

3. 1 January TBD-Year +1

2.1. Phase 1: Requirements for RP Software

Relying Party software MUST support [RFC8360] by 1 July TBD-Year.

2.2. Phase 2: Requirements for operators

Network operators MUST update their Relying Party software between 1 July TBD-Year and 1 January TBD-Year +1.

2.3. Phase 3: Requirements for Certificate Authorities

Trust Anchor CA certificates referenced in Trust Anchor Locator (TAL) files [RFC7730] MUST NOT make use of amended Resource Certificates defined in [RFC8360].

From 1 January 2020 Certificate Authorities MAY use amended Resource Certificates [RFC8360] for CA certificates that they issue to delegated Certificate Authorities. Certificate Authorities MUST NOT use the amended Resource Certificate profile for any other certificates they issue.

3. Avoid over-claiming CA certificates

Even though the amended profile limits the impact of resource over-claims on CA certificates, this does not mean that such over-claims are intended to become the norm. As we will describe in the following sections:

- Issuing CAs should try to avoid invalidating delegated CAs
- Delegated CAs should self-monitor and take action in case resources are removed

3.1. Avoid Invalidating Delegated CAs

3.1.1. Graceperiod and Check Intervals

If resources need to be removed from a delegated CA it is reasonable to observe a graceperiod that will allow a delegated CA (and recursively their delegated CAs if applicable) to clean up objects. A reasonable duration for this period depends on the following factors:

- The frequency that a child CA can check with its parents about its CA certificate eligibility (Check Interval)
- The depth of the tree of delegated CAs

We believe that it's reasonable to require the child CAs MUST issue a Resource Class List Query [RFC6492] to their parent CA no less frequently than once per houri (Check Interval). It is not expected that the depth of delegated CA certificates will exceed 5 or 6 CA authorities. In conclusion a graceperiod of 24 hours seems reasonable.

3.1.2. Shrinking issued CA certificates

When a Certificate Authority finds that it needs to shrink the set of resources held by a delegated Certificate Authority, but still holds the resources to be removed on its own CA certificate, then it SHOULD give the delegated Certificate Authority up to 24 hours to request a shrunk CA certificate, e.g. through the provision protocol [RFC6492].

The CA SHOULD issue a new CA certificate immediately using a "notAfter" time that is set to whichever is soonest: 24 hours from now, or the "notAfter" time on the CA certificate held by this issuing CA. This will alert the delegated CA of both the limited lifetime of their current CA certificate, and which resources remain eligible after this time, when the delegated CA sends a Resource Class List Query [RFC6492].

If the Certificate Authority no longer holds the resources that are to be removed, or this 24 hour period has passed, then a shrunk CA certificate MUST be issued. Such shrunk certificate SHOULD use the amended Resource Certificate profile in order to limit the impact in the validation of objects issued by the subsidiary Certificate Authority.

3.2. Self monitoring and clean-up

CAs in the RPKI MUST monitor whether the CA certificate issued to them by their parent needs to be shrunk, for example by sending a Resource Class List Query [RFC6492] to their parent CA no less frequently than once per hour.

If the CA finds that a reduced resource set is in order, but their current certificate is still valid, and they have issued delegated CA certificates with the resources to be reduced to delegated CAs, then they SHOULD give these delegated CAs up to 24 hours, or the time until 1 hour before their own CA certificate "notAfter" time if this period is shorter, to request a shrunk CA certificate as described above.

The CA MUST now remove any other RPKI objects that it issued that reference any of the resources to be removed. If the CA issued ROAs that reference multiple prefixes, and some of these prefixes are not to be removed, then the CA SHOULD create new ROAs for these prefixes and use one ROA object per prefix rather than bundling multiple prefixes on a single ROA object.

If the CA no longer issues any CA certificates or RPKI objects referencing the resources to be removed, or it finds that its current CA certificate is no longer valid or will expire within 1 hour, then

the CA MUST request a new CA certificate to be issued by their parent CA.

4. Mixed mode operations

Since there is no clear intention to have a "flag day" and move all RP systems to a new OID and a new mode of operation the question arises: what is the mode of operation of an RPKI system where both OID exist concurrently?

In mixed-mode, the application of the OID is taken to refer to the CA certificate itself: The value is set by the issuer, and might represent a default inherited value.

Should a CA be signed over with the old OID, its validation MUST follow the old OID. if a certficate is signed over with the new OID, its validation MUST follow the new OID. Therefore, ether situation can be expected but the intent is understood to apply to that certificate in the path.

The application of the OID applies to the certificate in hand, not the children. This permits a "strict" OID to have a "lax" OID child, which is the only pattern of issuance which has a risk of mis-interpretation.

OID	State	Consequence in tree below
old	no overclaim	tree is valid
old	overclaiming	tree is invalid
new	no overclaim	tree is valid
new	overclaiming	tree is valid when pruned

5. Example use of the amended profile with transfers

Consider the following starting situation where a Trust Anchor issues a resource certificate to Certificate Auhtority CA1, which in turn issues a ROA and delegates some resources to CA2, which in turn also issues a ROA:

```
      TA CA Certificate:
        Issuer:    TA
        Subject:   TA
        Profile:   6487 (regular)
        Resources: 192.0.2.0/24, 198.51.100.0/24,
                   2001:db8::/32, AS64496-AS64500

      CA1 CA Certificate:
        Issuer:    TA
        Subject:   CA1
        Profile:   8360 (amended)
        Resources: 192.0.2.0/24, 198.51.100.0/24
                   2001:db8::/32, AS64496-AS64500

      CA1 ROA 1:
        Issuer:    CA1
        Subject:   R1
        Profile:   6487 (regular)
        Resources: 192.0.2.0/24

        ASN:       64496
        Prefixes:  192.0.2.0/24 (Max 24)

      CA2 CA Certificate:
        Issuer:    CA1
        Subject:   CA2
        Profile:   8360 (amended)
        Resources: 198.51.100.0/24,
                   2001:db8::/32, AS64496-AS64500

      CA2 ROA 1:
        Issuer:    CA2
        Subject:   R1
        Profile:   6487 (regular)
        Resources: 2001:db8::/32

        ASN:       64496
        Prefixes:  2001:db8::/32 (Max 48)

      CA2 ROA 2:
        Issuer:    CA2
        Subject:   R1
        Profile:   6487 (regular)
        Resources: 198.51.100.0/24

        ASN:       64496
        Prefixes:  198.51.100.0/24 (Max 24)
```

Now assume that the TA decides that CA1 should no longer hold the prefix 198.51.100.0/24. However, CA1 is offline for some reason and it does not check in with TA about its CA certificate eligibility.

After 24 hours TA will decided that it has waited long enough and it will now pro-actively issue an amended CA certificate for CA1. Because the amended profile is used for CA certificates the impact of this action is limited. CA2 has been unaware of the change, but only their ROA2 which is using the prefix is now invalidated:

```
      TA CA Certificate:
        Issuer:    TA
        Subject:   TA
        Profile:   6487 (regular)
        Resources: 192.0.2.0/24, 198.51.100.0/24,
                   2001:db8::/32, AS64496-AS64500

      CA1 CA Certificate:
        Issuer:    TA
        Subject:   CA1
        Profile:   8360 (amended)
        Resources: 192.0.2.0/24
                   2001:db8::/32, AS64496-AS64500

      CA1 ROA 1:
        Issuer:    CA1
        Subject:   R1
        Profile:   6487 (regular)
        Resources: 192.0.2.0/24

        ASN:       64496
        Prefixes:  192.0.2.0/24 (Max 24)

      CA2 CA Certificate:
        Issuer:    CA1
        Subject:   CA2
        Profile:   8360 (amended)
        Rejected:  198.51.100.0/24
        Accepted:  2001:db8::/32, AS64496-AS64500

      CA2 ROA 1:
        Issuer:    CA2
        Subject:   R1
        Profile:   6487 (regular)
        Resources: 2001:db8::/32

        ASN:       64496
        Prefixes:  2001:db8::/32 (Max 48)

      CA2 ROA 2 (INVALID):
        Issuer:    CA2
        Subject:   R1
        Profile:   6487 (regular)
        Resources: 198.51.100.0/24

        ASN:       64496
        Prefixes:  198.51.100.0/24 (Max 24)
```

Now CA1 comes back online. It discovers that it lost the prefix 198.51.100.0/24. It will now re-issue the CA certificate issued to CA2 immediately:

```
TA CA Certificate:
  Issuer:    TA
  Subject:   TA
  Profile:   6487 (regular)
  Resources: 192.0.2.0/24, 198.51.100.0/24,
             2001:db8::/32, AS64496-AS64500

CA1 CA Certificate:
  Issuer:    TA
  Subject:   CA1
  Profile:   8360 (amended)
  Resources: 192.0.2.0/24
             2001:db8::/32, AS64496-AS64500

CA1 ROA 1:
  Issuer:    CA1
  Subject:   R1
  Profile:   6487 (regular)
  Resources: 192.0.2.0/24

  ASN:       64496
  Prefixes:  192.0.2.0/24 (Max 24)

CA2 CA Certificate:
  Issuer:    CA1
  Subject:   CA2
  Profile:   8360 (amended)
  Resources: 2001:db8::/32, AS64496-AS64500

CA2 ROA 1:
  Issuer:    CA2
  Subject:   R1
  Profile:   6487 (regular)
  Resources: 2001:db8::/32

  ASN:       64496
  Prefixes:  2001:db8::/32 (Max 48)

CA2 ROA 2 (INVALID):
  Issuer:    CA2
  Subject:   R1
  Profile:   6487 (regular)
  Resources: 198.51.100.0/24

  ASN:       64496
  Prefixes:  198.51.100.0/24 (Max 24)
```

Finally CA2, who was trying to check in with CA1 even when it was unavailable, discovers that it lost the prefix '198.51.100.0/24'. It will therefore remove its ROA2:

```
TA CA Certificate:
  Issuer:    TA
  Subject:   TA
  Profile:   6487 (regular)
  Resources: 192.0.2.0/24, 198.51.100.0/24,
             2001:db8::/32, AS64496-AS64500

CA1 CA Certificate:
  Issuer:    TA
  Subject:   CA1
  Profile:   8360 (amended)
  Resources: 192.0.2.0/24
             2001:db8::/32, AS64496-AS64500

CA1 ROA 1:
  Issuer:    CA1
  Subject:   R1
  Profile:   6487 (regular)
  Resources: 192.0.2.0/24

  ASN:       64496
  Prefixes:  192.0.2.0/24 (Max 24)

CA2 CA Certificate:
  Issuer:    CA1
  Subject:   CA2
  Profile:   8360 (amended)
  Resources: 2001:db8::/32, AS64496-AS64500

CA2 ROA 1:
  Issuer:    CA2
  Subject:   R1
  Profile:   6487 (regular)
  Resources: 2001:db8::/32

  ASN:       64496
  Prefixes:  2001:db8::/32 (Max 48)
```

A few things to note:

- In this scenario CA1 was offline, and it was not performing the actions required to the occurance of an overclaiming CA certificate to remain for CA2 and CA2 was not aware of the coming change.

- The use of the amened profile for reconsidered validation rules limited the impact of this operational problem to just those resources that were being removed.

- Had CA2 not only monitored its CA certificate eligibility directly with its parent, but had they performed RPKI validation to monitor their own certificate and products. Then they would have removed their ROA2 sooner. Since CA1 was offline however, they would not have been able to request a shrunk CA certificate for themselves.

- Had CA1 and CA2 both been online and TA observed the 24 hour grace period, then things would have been changed without the occurance of invalid objects or warnings. CA2 would have removed ROA2, and then would have requested a shrunk CA certificate for itself. CA1 would have noticed that it was safe to reques its own CA certificate to be shrunk. The CA depth here is 2, so this would have happened within 2 hours, well within the 24 hours limit.

6. RFC-EDITOR Considerations

The exact year value TBD-Year and TBD-Year +1 are to be defined in WG process and will be set before WGLC

7. Security Considerations

TBD

8. Revision History

01 - mixed-mode operation text. 2019 00 - Initial draft. 2018

9. Acknowledgements

This draft is a product of conversations in the RIR/NRO Engineering Coordination Group.

10. 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>.

[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>.

[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>.

[RFC6919] Barnes, R., Kent, S., and E. Rescorla, "Further Key Words for Use in RFCs to Indicate Requirement Levels", RFC 6919, DOI 10.17487/RFC6919, April 2013, <https://www.rfc-editor.org/info/rfc6919>.

[RFC7730] Huston, G., Weiler, S., Michaelson, G., and S. Kent, "Resource Public Key Infrastructure (RPKI) Trust Anchor Locator", RFC 7730, DOI 10.17487/RFC7730, January 2016, <https://www.rfc-editor.org/info/rfc7730>.

[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>.

Authors' Addresses

George G. Michaelson
Asia Pacific Network Information Centre
6 Cordelia St
South Brisbane, QLD 4101
Australia

Email: ggm@apnic.net

Tim Bruijnzeels
Open Netlabs B.V.
Science Park 400
Amsterdam 1098 XH
The Netherlands

Email: timb@opennetlabs.nl