Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 13, 2014

G. Huston
G. Michaelson
APNIC

February 9, 2014

RPKI Validation Reconsidered
draft-huston-rpki-validation-01.txt

Abstract

This document reviews the certificate validation procedure specified in RFC6487 and highlights aspects of operational management of certificates in the RPKI in response to the movement of resources across registries, and the associated actions of Certification Authorities to maintain certification of resources during this movement. The document describes an alternative validation procedure that reduces the operational impact of certificate management during resource movement.

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 http://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 August 13, 2014.

Table of Contents

1. Introduction

This document reviews the certificate validation procedure specified in [RFC6487] and highlights aspects of operational management of certificates in the RPKI in response to the movement of resources across registries, and the associated actions of Certification Authorities to maintain certification of resources during this movement. The document describes an alternative validation procedure that reduces the operational impact of certificate management during resource movement. The alternative validation procedure also offers a higher level of robustness in the face of resource inconsistencies in a putative certificate validation path.

As currently defined in section 7.2 of [RFC6487], validation of PKIX certificates that conform to the RPKI profile relies on the use of a path validation process where each certificate in the validation path is required to meet the certificate validation criteria. This can be considered to be a recursive validation process where, in the context of an ordered sequence of certificates, as defined by common Issuer and Subject Name pairs, a certificate is defined as valid if it satisfies basic validation criteria relating to the syntactic correctness, currency of validity dates and similar properties of the certificate itself, as described in [RFC5280], and also that it satisfies certain additional criteria with respect to the previous certificate in the sequence, and that this previous certificate is itself a valid certificate using the same criteria. This definition applies recursively to all certificates in the sequence apart from the initial sequence element, which is required to be a Trust Anchor.

For RPKI certificates, the additional criteria relating to the previous certificate in this sequence is that the certificate's number resource set, as defined in [RFC3779], is "encompassed" by the number resource set contained in the previous certificate.

Because [RFC6487] validation demands that all resources in a certificate be valid under the parent (and recursively, to the root), a digitally signed attestation, such as a Route Origin Authorization (ROA) object [RFC6482], which refers only to a subset of RFC3779-specified resources from that certificate chain can be concluded to be invalid, but not by virtue of the relationship between the RFC3779 extensions of the certificates on the putative certificate validation path and the resources in the ROA, but by other resources described in these certificates where the "encompassing" relationship of the resources does not hold. Any such invalidity along the certificate validation path can cause this outcome, not just at the immediate parent of the end entity certificate that attests to the key used to sign the ROA.

For example, in the certificate sequence:

Certificate 1:
Issuer A, Subject B, Resources 192.0.2.0/24, AS64496-AS64500

Certificate 2:
Issuer B, Subject C, Resources 192.0.2.0/24/24, AS64496-AS64511

Certificate 3:
Issuer C, Subject D, Resources 192.0.2.0/24

Certificate 3 is considered to be an invalid certificate, because the resources in Certificate 2 are not encompassed by the resources in Certificate 1, by virtue of certificate 2 holding the resources of the range AS64501 - AS64511 in this RFC3779 resource extension. Obviously, these Autonomous Systems numbers are not related to the IPv4 resources contained in Certificate 3.

2. Operational Considerations

There are two areas of operational concern with the current RPKI validation definition.

The first is that of the robustness of the operatinal management procesures in the issuance of certificates. If a subordinate CA issues a certificate that contains an Internet Number Resource (INR) collection that is not either exactly equal to, or a strict subset of, its parent CA, then this issued certificate, and all subordinate certificates of this issued certificate are invalid. These certificates are not only defined as invalid when being considered to validate an INR that is not in the parent CA certificate, but are defined as invalid for all INRs in the certificate. This creates a degree of operational fragility in the issuance of certificates, as all CA's are now required to exercise extreme care in the issuance and reissuance of certificates that they do not overclaim on the resources described in the parent CA, as the consequences of an operational lapse or oversight implies that all the subordinate certificates from the point of mismatch are invalid. It would be preferred if the consequences of such an operational lapse were limited in scope to the specific INRs that formed the mismatch, rather than including the sntire set of INRs within the scope of damage from this oversight.

The second operational consideration described here relates to the situation where a registry withdraws a resource from the current holder, and the resource to transferred to another registry, to be registered to a new holder in that registry. The reason why this is

a consideration in operational deployments of the RPKI lies in the movement of the "home" registry of number resources during cases of mergers, acquisitions, business re-alignments, and resource transfers and the desire to ensure that during this movement all other resources can continue to be validated.

If the original registry's certification actions are simply to issue a new certificate for the current holder with a reduced resource set, and to revoke the original certificate, then there is a distinct possibility of encountering the situation illustrated by the example in the previous section. This is a result of an operational process for certificate issuance by the parent CA being de-coupled from the certificate operations of child CA.

This de-coupled operation of CAs introduces a risk of unintended third party damage: since a CA certificate can refer to holdings which relate to two or more unrelated subordinate certificates, if this CA certificate becomes invalid due to the reduction in the resources allocated to this CA relating to one subordinate resource set, all other subordinate certificates are invalid until the CA certificate is reissued with a reduced resource set.

In the above example, all subordinate certificates issued by CA C are invalid until CA B issues a new certificate for CA C with a reduced resource set.

At the lover levels of the RPKI hierarchy the resource sets affected by such movements of resources may not encompass significantly large pools of resources. However, as one ascends through this hierarchy towards the apex, the larger the resource set that is going to be affected by a period of invalidity by virtue of such uncoordinated certificate management actions. In the case of a Regional Internet Registry (RIR) or National Internet Registry (NIR), the potential risk arising from uncoordinated certification actions relating to a transfer of resources is that the entire set of subordinate certificates that refer to resources administered by the RIR or the NIR cannot be validated during this period.

Avoiding such situations requires that CA's adhere to a very specific ordering of certificate issuance. In this framework, the common registry CA that describes (directly or indirectly) the resources being shifted from one registry to the other, and also contains in subordinate certificates (direct or indirect) the certificates for both registries who are parties to the resource transfer has to coordinate a specific sequence of actions.

This common registry CA has to first issue a new certificate towards the "receiving" registry that adds to the RFC3779 extension resource

set the specific resource being transferred into this receiving registry. The common registry CA then has to wait until all registries in the subordinate certificate chain to the receiving registry have also performed a similar issuance of new certificates, and in each case a registry must await the issuance of the immediate superior certificate with the augmented resource set before it, in turn, can issue its own augmented certificate to its subordinate CA. This is a "top down" issuance sequence."

It is possible for the common registry to issue a certificate to the "sending" registry with the reduced resource set at any time, but it should not revoke the previously issued certificate, nor overwrite this previously issued certificate in its repository publication point without specific coordination. Only when the common registry is assured that the top down certificate issuance process to the receiving registry CA chain has been completed can the common registry commence the revocation of the original certificate for the sending registry, However, it should not so until it is assured that the immediate subordinate registry CA in the path to the sending registry has issued a certificate with a reduced resource set, and so on. This implies that on the sending side the certificate issuance and revocation is a "bottom up" process.

If this process is not carefully followed, then the risk is that some or all or the subordinate certificates of this common registry CA will be unable to be validated until the entire process of certificate issuance and revocation has been completed. While this sequenced process is intended to preserve validity of certificates in the RPKI, it is a complex and operationally cumbersome process.

The underlying consideration here is that the operational coordination of these certificate issuance and revocation actions to effect a smooth resource transfer across registries is mandated by the nature of the certificate validation process described in [RFC6487].

3. A Specific Resource RPKI Certificate Validation Process

The question considered here is: Is there an alternate definition of RPKI certificate validity that could remove the requirement for such careful orchestration of certification actions across the RPKI to support resource transfers?

The general definition of certificate validity as defined in [RFC5280] assumes a validation question relating to the relying party's (RP's) level of trust in a subject's signed material, given knowledge of a subject's name, the subject's public key, the RP's

chosen trust anchor(s) and an overall PKI to define the domain of discourse.

The validation question assumed by the [RFC6487] RPKI certificate validation process relates to a RP's level of trust in the combination of some signed material, a certificate that attests to the public key used to sign this material and the set of all number resources that have been assigned or allocated to the subject of the certificate, given knowledge of the certificate, the RP's chosen trust anchor(s), the RPKI, and the application of the same test applied to the superior certificate in the RPKI hierarchy, and so on to a Trust Anchor.

There is a alternative certificate validation procedure that starts with an attestation containing the subject's signed material and an explicit enumeration of a set of number resources. The associated validation question relates to whether a RPKI validation process can attest to the validity of a subject's signed attestation relating to a particular set of number resources, rather than a signed attestation relating to all number resources held by this subject. We will term this alternate certificate validation process "specific resource" validation.

If the certificate validation procedure is specifically restricted to a question of ascertaining the validity of a particular set of number resources in the context of the RPKI, the RPKI validation procedure need not be as strict as a recursive "encompassing" condition for the resources contained in each pair of certificates in the validation path. It would be sufficient in the context of this "specific resource" validation procedure to require only that each certificate in the validation path has a number resource extension that "encompasses" the specific resources described in the original validation question. Rather than a validation test for all possible questions, this is a specific validation question in the context of specific resources.

This validation question can be informally described as: Given a certificate and a given resource set, is there an Issuer-Subject ordered sequence of certificates from a Trust Anchor to the certificate being validated, where each certificate on this sequence is well-formed, not revoked by a valid CRL, where the certificate's lifetimes are valid, and where the RFC3779 resource extension in the certificate encompass the given resource set?

In the example from Section 1, using a this alternate certificate validation process, a validation question of certificate 3 and the resource 10.0.1.0/24, the validation outcome would be positive, in that certificates 1, 2 and 3 all encompass the specific resource

10.0.1.0/24, assuming that the certificates are valid in all other respects.

3.1. Resource Transfers and Specific Resource Certificate Validation

When considering the transfer of resources across registries, and the associated certification actions, then if the validation process was one of "specific resource" validation, then there is no requirement for synchronized orchestration of the process of certificate issuance and revocation by the CAs involved in this transfer in order to preserve the validity of resources described in these certificates.

Along the chain of the "sending" registry CA hierarchy each registry CA can issue a certificate with a reduced resource set that removes the resource being transferred, and revoke the previously issued certificate without regard to the specific timing of similar actions by either it's superior or its subordinate registry CA.

Similarly, in the "receiving" registry hierarchy each CA can issue a certificate with an augmented resource set that includes the resource being transferred without particular regard to the timing of similar actions by the other superior or subordinate registry CAs.

Validation questions relating to the migrating resource made against certificates on the "sending registry" will return an invalid outcome as soon as any registry CA in this chain has performed revocation of the original certificate. Validation questions relating to the migrating resource made against certificates on the "receiving registry" will return an valid outcome only when all the registries in this chain have performed certificate re-issuance and included the resource in the new certificate.

Critically, at all times validation questions relating to any other resource using the "specific resource" validation approach will return the same outcomes throughout this issuance and revocation process. This "specific resource" validation process engenders a more robust outcome in RPKI certificate management. Validation questions relating to resources which are not being transferred from one registry to another cannot be compromised by any failure to adhere to a strict process of issuance and revocation relating to the certification of the resources being transferred.

3.2. A Specification of Specific Resource Validation

The following is a amended specification of certificate validation as described in [RFC6487] that describes the proposed "specific resource" certificate validation process.

Validation of signed resource data using a target resource certificate and a specific set of number resources 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. This path validation process verifies, among other things, that a prospective certification path (a sequence of n certificates) satisfies the following conditions:

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

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

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

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

Certificate validation entails verifying that all of the following conditions hold, in addition to the Certification Path Validation criteria specified in Section 6 of [RFC5280]:

1. The certificate can be verified using the Issuer's public key and the signature algorithm

2. The current time lies within the certificate's Validity From and To values.

3. The certificate contains all fields that MUST be present, as defined by this specification, and contains values for selected fields that are defined as allowable values by this specification.

4. No field, or field value, that this specification defines as MUST NOT be present is used in the certificate.

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.

6. The resource extension data contained in this certificate "encompasses" the entirety of the resources in the specific resource set.

7. The Certification Path originates with a certificate issued by a trust anchor, and there exists a signing chain across the Certification Path where the Subject of Certificate 'x' in the Certification Path matches the Issuer in Certificate 'x + 1' in the Certification Path, and the public key in Certificate 'x' can verify the signature value in Certificate 'x+1'.

A certificate validation algorithm MAY perform these tests in any chosen order.

4. Local Repository Cache Maintenance

This change in the validation process would have some impact on the operation of a local cache of validated RPKI certificates. Given that the validation process requires the specification of a specific resource set, it would appear that it would not be possible to validate an RPKI certificate without also specifying a specific resource set.

However, using a top-down validation process, and an additional local data structure associated with each locally held validated RPKI certificate, it is possible to maintain a local cache of validated certificates, and the set of valid and invalid resources for each certificate.

The additional data structures are the certificate's validated and invalidated resource set. These sets are defined as follows:

- If the certificate is used as a Trust Anchor, then the local validated resource set is copied from the certificate's RFC3779 resource set. There is no invalid resource set.

- Otherwise, the certificate's local validated resource set is defined as the intersection of this certificate's RFC3779 resource

set and the parent certificate's local validated resource set. The certificate's invalid resource set is the difference between this set and the certificate's RFC3779 resource set.

If the certificate's validated resource set is empty then the certificate is not valid.

If the invalid resource set is not empty, then any resources that are contained in this invalid resource set cannot be valid by virtue of this certificate.

In all operations on the local repository cache, local applications should use the certificate's local validated resource set in place of the resources described in the certificate's RFC3779 extension.

The invalid resource set can be used as a diagnostic aide in local cache management.

5. Security Considerations

The Security Considerations of [RFC6487] apply to the validation procedure described here.

6. IANA Considerations

No updates to the registries are suggested by this document.

7. Acknowledgements

TBA.

8. References

8.1. Normative References

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, June 2004.

[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, May 2008.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for

X.509 PKIX Resource Certificates", RFC 6487,
February 2012.

8.2. Informative References

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, February 2012.

Authors' Addresses

Geoff Huston
Asia Pacific Network Information Centre (APNIC)
6 Cordelia St
South Brisbane, QLD 4101
Australia

Phone: +61 7 3858 3100
Email: gih@apnic.net

George Michaelson
Asia Pacific Network Information Centre (APNIC)
6 Cordelia St
South Brisbane, QLD 4101
Australia

Phone: +61 7 3858 3100
Email: ggm@apnic.net