Internet Engineering Task Force (IETF)
Request for Comments: 6907
Category: Informational
ISSN: 2070-1721

T. Manderson
ICANN
K. Sriram
US NIST
R. White
Verisign

March 2013

Use Cases and Interpretations of Resource Public Key Infrastructure (RPKI) Objects for Issuers and Relying Parties

Abstract

This document describes a number of use cases together with directions and interpretations for organizations and relying parties when creating or encountering Resource Public Key Infrastructure (RPKI) object scenarios in the public RPKI. All of these items are discussed here in relation to the Internet routing system.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

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). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6907.

Table of Contents

1. Introduction

This document describes a number of use cases together with directions and interpretations for organizations and relying parties when creating or encountering Resource Public Key Infrastructure (RPKI) object scenarios in the public RPKI. All of these items are discussed here in relation to the Internet routing system.

1.1. Terminology

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], "A Profile for X.509 PKIX Resource Certificates" [RFC6487], "X.509 Extensions for IP Addresses and AS Identifiers" [RFC3779], "A Profile for Route Origin Authorizations (ROAs)" [RFC6482], "Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)" [RFC6483], and "BGP Prefix Origin Validation" [RFC6811].

1.2. Documentation Prefixes

The documentation prefixes recommended in [RFC5737] are insufficient for use as example prefixes in this document. Therefore, this document uses RFC 1918 [RFC1918] address space for constructing example prefixes.

1.3. Definitions

For all of the use cases in this document, it is assumed that RPKI objects (e.g., resource certificates, ROAs) validate in accordance with [RFC6487] and [RFC6480]. In other words, we assume that corrupted RPKI objects, if any, have been detected and eliminated.

The following definitions are in use in this document. Some of these definitions are reused or adapted from [RFC6811] with authors' permission.

Resource: An IP address prefix (simply called prefix or subnet) or an Autonomous System Number (ASN).

Allocation: A set of resources provided to an entity or organization for its use.

Sub-allocation: A set of resources subordinate to an allocation assigned to another entity or organization.

Prefix: A prefix consists of a pair (IP address, prefix length), interpreted as is customary (see [RFC4632]).

Route: Data derived from a received BGP update, as defined in [RFC4271], Section 1.1. The route includes one prefix and an AS_PATH, among other things.

ROA: Route Origin Authorization (ROA) is an RPKI object signed by a prefix holder authorizing origination of said prefix from an origin AS specified in said ROA.

AS 0 ROA: A ROA with ASN value 0 (zero) in the AS ID field. AS 0 ROA is an attestation by a prefix holder that the prefix described in the ROA, and any more specific prefix, should not be used in a routing context [RFC6483].

ROA prefix: The prefix from a ROA.

ROA ASN: The origin ASN from a ROA.

maxLength: The maximum length up to which more specific prefixes of a ROA prefix may be originated from the corresponding ROA ASN. The maxLength is specified in the ROA.

Route prefix: A prefix derived from a route.

Route origin ASN: The origin AS number derived from a route. The origin AS number is:

- the rightmost AS in the final segment of the AS_PATH attribute in the route if that segment is of type AS_SEQUENCE, or
- the BGP speaker’s own AS number if that segment is of type AS_CONFED_SEQUENCE or AS_CONFED_SET or if the AS_PATH is empty, or
- the distinguished value "NONE" if the final segment of the AS_PATH attribute is of any other type.

Covering ROA prefix: A ROA prefix that is an exact match or a less specific when compared to the route prefix under consideration. In other words, the route prefix is said to have a covering ROA prefix when there exists a ROA such that the ROA prefix length is less than or equal to the route prefix length and the ROA prefix address matches the route prefix address for all bits specified by the ROA prefix length.

Covering ROA: If a ROA contains a covering ROA prefix for a route prefix under consideration, then the ROA is said to be a covering ROA for the route prefix.

No covering ROA: No covering ROA exists for a route prefix under consideration.

No other covering ROA: No other covering ROA exists (besides what is (are) already cited) for a route prefix under consideration.

Multi-homed prefix or subnet: A prefix (i.e., subnet) for which a route is originated through two or more autonomous systems.

Matched: A route's {prefix, origin AS} pair is said to be matched by a ROA when the route prefix has a covering ROA, and in addition, the route prefix length is less than or equal to the maxLength in said covering ROA and the route origin ASN is equal to the ASN in said covering ROA.

Given these definitions, any given BGP route will be found to have one of the following "validation states":

- NotFound: The route prefix has no covering ROA.
- Valid: The route's {prefix, origin AS} pair is matched by at least one ROA.
- Invalid: The route prefix has at least one covering ROA and the route's {prefix, origin AS} pair is not matched by any ROA.

It is to be noted that no ROA can have the value "NONE" as its ROA ASN. Thus, a route whose origin ASN is "NONE" cannot be matched by any ROA. Similarly, no valid route can have an origin ASN of zero [AS0-PROC]. Thus, no route can be matched by a ROA whose ASN is zero (i.e., an AS 0 ROA) [RFC6483].

2. Overview

2.1. General Interpretation of RPKI Object Semantics

In the interpretation of relying parties (RPs), or relying party routing software, it is important that a 'make before break' operational policy be applied. In part, this means that an RP should implement a routing decision process where a route is assumed to be intended (i.e., considered unsuspicious) unless proven otherwise by the existence of a valid RPKI object that explicitly invalidates the route (see Section 7.1 for examples). Also, especially in cases when a prefix is newly acquired by allocation/sub-allocation or due to

prefix-ownership transfer, a ROA should be registered in RPKI prior to advertisement of the prefix in BGP. This is highly recommended for the following reasons. Observe that in the transfer case (considering a prefix transfer from Org A to Org B), even though Org A's resource cert would be revoked before issuing a resource cert to Org B, there may be some latency before all relying parties discard the previously received ROA of Org A for that prefix. The latency may be due to CRL propagation delay in the RPKI system or due to periodic polling by RPs, etc. Also, observe that in the sub-allocation case (from parent Org A to child Org B), there may be an existing ROA registered by Org A (with their own origin ASN) for a covering aggregate prefix relative to the prefix in consideration. If the new prefix owner (Org B) has not already registered their own ROA (i.e., ROA with their origin ASN), then the presence of a different covering ROA (i.e., one with a different origin ASN) belonging to Org A would result in invalid assessment for the route advertised by the new owner (Org B). Thus, in both cases (transfer or sub-allocation), it is prudent for the new owner (Org B) to ensure that its route for the prefix will be valid by proactively issuing a ROA before advertising the route. The ROA should be issued with sufficient lead time taking into consideration the RPKI propagation delays.

As stated earlier in Section 1.3, for all of the use cases in this document, it is assumed that RPKI objects (e.g., resource certificates, ROAs) validate in accordance with [RFC6487] and [RFC6480]. In other words, we assume that corrupted RPKI objects, if any, have been detected and eliminated.

While many of the examples provided here illustrate organizations using their own autonomous system numbers to originate routes, it should be recognized that a prefix holder need not necessarily be the holder of the autonomous system number used for the route origination.

3. Origination Use Cases

This section deals with the various use cases where an organization has Internet resources and will announce routes to the Internet. It is based on operational observations of the existing routing system. In the following use cases, the phrase "relying parties interpret the route as intended" is generally meant to indicate that "relying parties interpret an announced route as having a valid origination AS".

3.1. Single Announcement

An organization (Org A with ASN 64496) has been allocated the prefix 10.1.2.0/24. It wishes to announce the /24 prefix from ASN 64496 such that relying parties interpret the route as intended.

The desired announcement (and organization) would be:

Prefix	Origin AS	Organization
10.1.2.0/24	AS 64496	Org A

The issuing party should create a ROA containing the following:

asID	address	maxLength
64496	10.1.2.0/24	24

3.2. Aggregate with a More Specific

An organization (Org A with ASN 64496) has been allocated the prefix 10.1.0.0/16. It wishes to announce the more specific prefix 10.1.0.0/20 from ASN 64496 as well as the aggregate route such that relying parties interpret the routes as intended.

The desired announcements (and organization) would be:

Prefix	Origin AS	Organization
10.1.0.0/16	AS 64496	Org A
10.1.0.0/20	AS 64496	Org A

The issuing party should create a ROA containing the following:

asID	address	maxLength
64496	10.1.0.0/16	16
	10.1.0.0/20	20

3.3. Aggregate with a More Specific from a Different ASN

An organization (Org A with ASN 64496 and ASN 64511) has been allocated the prefix 10.1.0.0/16. It wishes to announce the more specific prefix 10.1.0.0/20 from ASN 64511 as well as the aggregate route from ASN 64496 such that relying parties interpret the routes as intended.

The desired announcements (and organization) would be:

Prefix	Origin AS	Organization
10.1.0.0/16	AS 64496	Org A
10.1.0.0/20	AS 64511	Org A

The issuing party should create ROAs containing the following:

asID	address	maxLength
64496	10.1.0.0/16	16

asID	address	maxLength
64511	10.1.0.0/20	20

3.4. Sub-Allocation to a Multi-Homed Customer

An organization (Org A with ASN 64496) has been allocated the prefix 10.1.0.0/16; it wishes to announce the more specific prefix 10.1.0.0/20 from ASN 64496. It has further delegated 10.1.16.0/20 to a customer (Org B with ASN 64511) who is multi-homed and will originate the prefix route from ASN 64511. ASN 64496 will also announce the aggregate route such that relying parties interpret the routes as intended.

The desired announcements (and organizations) would be:

Prefix	Origin AS	Organization
10.1.0.0/16	AS 64496	Org A
10.1.0.0/20	AS 64496	Org A
10.1.16.0/20	AS 64511	Org B

The issuing party should create ROAs containing the following:

Org A:

asID	address	maxLength
64496	10.1.0.0/16	16
	10.1.0.0/20	20

Org B:

asID	address	maxLength
64511	10.1.16.0/20	20

3.5. Restriction of a New Allocation

An organization has recently been allocated the prefix 10.1.0.0/16. Its network deployment is not yet ready to announce the prefix and wishes to restrict all possible announcements of 10.1.0.0/16 and more specifics in routing using RPKI.

The following announcements would be considered undesirable:

Prefix	Origin AS	Organization
10.1.0.0/16	ANY AS	ANY
10.1.0.0/20	ANY AS	ANY
10.1.17.0/24	ANY AS	ANY

The issuing party should create a ROA containing the following:

asID	address	maxLength
0	10.1.0.0/16	32

This is known as an AS 0 ROA [RFC6483]. Also, please see the definition and related comments in Section 1.3.

3.6. Restriction of New ASN

An organization has recently been allocated an additional ASN 64511. Its network deployment is not yet ready to use this ASN and wishes to restrict all possible uses of ASN 64511 using RPKI.

The following announcement would be considered undesirable:

Prefix	Origin AS	Organization
ANY	AS 64511	ANY

It is currently not possible to restrict use of autonomous system numbers.

3.7. Restriction of a Part of an Allocation

An organization (Org A with ASN 64496) has been allocated the prefix 10.1.0.0/16. Its network topology permits the announcement of 10.1.0.0/17. Org A wishes to restrict any possible announcement of 10.1.128.0/17 or more specifics of that /17 using RPKI.

The desired announcement (and organization) would be:

Prefix	Origin AS	Organization
10.1.0.0/17	AS 64496	Org A

The following announcements would be considered undesirable:

Prefix	Origin AS	Organization
10.1.128.0/17	ANY AS	ANY
10.1.128.0/24	ANY AS	ANY

The issuing party should create ROAs containing the following:

asID	address	maxLength
64496	10.1.0.0/17	17

asID	address	maxLength
0	10.1.128.0/17	32

3.8. Restriction of Prefix Length

An organization (Org A with ASN 64496) has been allocated the prefix 10.1.0.0/16; it wishes to announce the aggregate and any or all more specific prefixes up to and including a maximum length of /20, but never any more specific than a /20.

Examples of the desired announcements (and organization) would be:

Prefix	Origin AS	Organization
10.1.0.0/16	AS 64496	Org A
10.1.0.0/17	AS 64496	Org A
...	AS 64496	Org A
10.1.128.0/20	AS 64496	Org A

The following announcements would be considered undesirable:

Prefix	Origin AS	Organization
10.1.0.0/21	ANY AS	ANY
10.1.0.0/22	ANY AS	ANY
...	ANY AS	ANY
10.1.128.0/24	ANY AS	ANY

The issuing party should create a ROA containing the following:

asID	address	maxLength
64496	10.1.0.0/16	20

3.9. Restriction of Sub-Allocation Prefix Length

An organization (Org A with ASN 64496) has been allocated the prefix 10.1.0.0/16. It sub-allocates several /20 prefixes to its multi-homed customers: Org B with ASN 64501 and Org C with ASN 64499, respectively. It wishes to restrict those customers from advertising any corresponding routes more specific than a /22.

The desired announcements (and organizations) would be:

Prefix	Origin AS	Organization
10.1.0.0/16	AS 64496	Org A
10.1.0.0/20	AS 64501	Org B
10.1.128.0/20	AS 64499	Org C
10.1.4.0/22	AS 64501	Org B

The following example announcements (and organizations) would be considered undesirable:

Prefix	Origin AS	Organization
10.1.0.0/24	AS 64501	Org B
10.1.128.0/24	AS 64499	Org C
.....	...	...
10.1.0.0/23	ANY AS	ANY

The issuing party (Org A) should create ROAs containing the following:

For Org A:

asID	address	maxLength
64496	10.1.0.0/16	16

For Org B:

asID	address	maxLength
64501	10.1.0.0/20	22

For Org C:

asID	address	maxLength
64499	10.1.128.0/20	22

3.10. Aggregation and Origination by an Upstream Provider

Consider four organizations with the following resources, which were acquired independently from any transit provider.

Organization	ASN	Prefix
Org A	AS 64496	10.1.0.0/24
Org B	AS 64505	10.1.3.0/24
Org C	AS 64499	10.1.1.0/24
Org D	AS 64511	10.1.2.0/24

These organizations share a common upstream provider Transit X (ASN 64497) that originates an aggregate of these prefixes with the permission of all four organizations.

The desired announcements (and organizations) would be:

Prefix	Origin AS	Organization
10.1.0.0/24	AS 64496	Org A
10.1.3.0/24	AS 64505	Org B
10.1.1.0/24	AS 64499	Org C
10.1.2.0/24	AS 64511	Org D
10.1.0.0/22	AS 64497	Transit X

It is currently not possible for an upstream provider to make a valid aggregate announcement of independent prefixes. However, the issuing parties should create ROAs containing the following:

Org A:

asID	address	maxLength
64496	10.1.0.0/24	24

Org B:

asID	address	maxLength
64505	10.1.3.0/24	24

Org C:

asID	address	maxLength
64499	10.1.1.0/24	24

Org D:

asID	address	maxLength
64511	10.1.2.0/24	24

3.11. Rogue Aggregation and Origination by an Upstream Provider

Consider four organizations with the following resources that were acquired independently from any transit provider.

Organization	ASN	Prefix
Org A	AS 64496	10.1.0.0/24
Org B	AS 64503	10.1.3.0/24
Org C	AS 64499	10.1.1.0/24
Org D	AS 64511	10.1.2.0/24

These organizations share a common upstream provider Transit X (ASN 64497) that originates an aggregate of these prefixes where possible. In this situation, Org B (ASN 64503, 10.1.3.0/24) does not wish for its prefix to be aggregated by the upstream provider.

The desired announcements (and organizations) would be:

Prefix	Origin AS	Organization
10.1.0.0/24	AS 64496	Org A
10.1.3.0/24	AS 64503	Org B
10.1.1.0/24	AS 64499	Org C
10.1.2.0/24	AS 64511	Org D
10.1.0.0/23	AS 64497	Transit X

The following announcement would be considered undesirable:

Prefix	Origin AS	Organization
10.1.0.0/22	AS 64497	Transit X

It is currently not possible for an upstream provider to make a valid aggregate announcement of independent prefixes. However, the issuing parties should create ROAs containing the following:

Org A:

asID	address	maxLength
64496	10.1.0.0/24	24

Org B:

asID	address	maxLength
64503	10.1.3.0/24	24

Org C:

asID	address	maxLength
64499	10.1.1.0/24	24

Org D:

asID	address	maxLength
64511	10.1.2.0/24	24

4. Adjacency or Path Validation Use Cases

Use cases pertaining to adjacency or path validation are beyond the scope of this document and would be addressed in a separate document.

5. Partial Deployment Use Cases

5.1. Parent Does Not Participate in RPKI

An organization (Org A with ASN 64511) is multi-homed and has been assigned the prefix 10.1.0.0/20 from its upstream (Transit X with ASN 64496). Org A wishes to announce the prefix 10.1.0.0/20 from ASN 64511 to its other upstream(s). Org A also wishes to create RPKI statements about the resource; however, Transit X (ASN 64496), which announces the aggregate 10.1.0.0/16, has not yet adopted RPKI.

The desired announcements (and organization with RPKI adoption) would be:

Prefix	Origin AS	Organization	RPKI
10.1.0.0/20	AS 64511	Org A	Yes
10.1.0.0/16	AS 64496	Transit X	No

RPKI is strictly hierarchical; therefore, if Transit X does not participate in RPKI, Org A is unable to validly issue RPKI objects.

5.2. Only Some Children Participate in RPKI

An organization (Org A with ASN 64496) has been allocated the prefix 10.1.0.0/16 and participates in RPKI; it wishes to announce the more specific prefix 10.1.0.0/20 from ASN 64496. It has further delegated 10.1.16.0/20 and 10.1.32.0/20 to customers Org B with ASN 64511 and Org C with ASN 64502 (respectively), who are multi-homed. Org B (ASN 64511) does not participate in RPKI. Org C (ASN 64502) participates in RPKI.

The desired announcements (and organizations with RPKI adoption) would be:

Prefix	Origin AS	Organization	RPKI
10.1.0.0/16	AS 64496	Org A	Yes
10.1.0.0/20	AS 64496	Org A	Yes
10.1.16.0/20	AS 64511	Org B	No
10.1.32.0/20	AS 64502	Org C	Yes

The issuing parties should create ROAs containing the following:

Org A:

asID	address	maxLength
64496	10.1.0.0/16	16
	10.1.0.0/20	20

Org A issues for Org B:

asID	address	maxLength
64511	10.1.16.0/20	20

Org C:

asID	address	maxLength
64502	10.1.32.0/20	20

5.3. Grandchild Does Not Participate in RPKI

Consider the previous example, with an extension by which Org B, who does not participate in RPKI, further allocates 10.1.17.0/24 to Org X with ASN 64505. Org X does not participate in RPKI.

The desired announcements (and organizations with RPKI adoption) would be:

Prefix	Origin AS	Organization	RPKI
10.1.0.0/16	AS 64496	Org A	Yes
10.1.0.0/20	AS 64496	Org A	Yes
10.1.16.0/20	AS 64511	Org B	No
10.1.32.0/20	AS 64502	Org C	Yes
10.1.17.0/24	AS 64505	Org X	No

The issuing parties should create ROAs containing the following:

Org A:

asID	address	maxLength
64496	10.1.0.0/16	16
	10.1.0.0/20	20

Org A issues for Org B:

asID	address	maxLength
64511	10.1.16.0/20	20

Org A issues for Org B's customer Org X:

asID	address	maxLength
64505	10.1.17.0/24	24

Org C:

asID	address	maxLength
64502	10.1.32.0/20	20

6. Transfer Use Cases

For transfer use cases, based on the preceding sections, it should be easy to deduce what new ROAs need to be created and what existing ROAs need to be maintained (or revoked). The resource transfer and timing of revocation/creation of the ROAs need to be performed based on the make-before-break principle and using suitable Regional Internet Registry (RIR) procedures (see Section 2.1).

6.1. Transfer of In-Use Prefix and Autonomous System Number

Org A holds the resource 10.1.0.0/20, and it is currently in use and originated from AS 64496 with valid RPKI objects in place. Org B has acquired both the prefix and ASN and desires an RPKI transfer on a particular date and time without adversely affecting the operational use of the resource.

The following RPKI objects would be created/revoked:

For Org A, revoke the following ROA:

asID	address	maxLength
64496	10.1.0.0/20	20

For Org B, add the following ROA:

asID	address	maxLength
64496	10.1.0.0/20	20

6.2. Transfer of In-Use Prefix

Org A holds the resource 10.1.0.0/16, and it is currently in use and originated from AS 64496 with valid RPKI objects in place. Org A has agreed to transfer the entire /16 address block to Org B and will no longer originate the prefix or more specifics of it. Consequently, Org B desires an RPKI transfer of this resource on a particular date and time. This prefix will be originated by AS 64511 as a result of this transfer.

The following RPKI objects would be created/revoked:

For Org A, revoke the following ROA:

asID	address	maxLength
64496	10.1.0.0/16	16

For Org B, add the following ROA when the resource certificate for 10.1.0.0/16 is issued to them (Org B):

asID	address	maxLength
64511	10.1.0.0/16	16

6.3. Transfer of Unused Prefix

Org A holds the resources 10.1.0.0/16 and AS 64507 (with RPKI objects). Org A currently announces 10.1.0.0/16 from AS 64507. Org B has acquired an unused portion (10.1.4.0/24) of the prefix from Org A and desires an RPKI transfer on a particular date and time. Org B will originate a route 10.1.4.0/24 from AS 64496.

The following RPKI objects would be created/sustained:

For Org A, leave the following ROA unchanged:

asID	address	maxLength
64507	10.1.0.0/16	16

For Org B, add the following ROA when the resource certificate for 10.1.4.0/24 is issued to them (Org B):

asID	address	maxLength
64496	10.1.4.0/24	24

Org A may optionally provide ROA coverage for Org B by creating the following ROA preceding the RPKI transfer. The ROA itself is then naturally revoked when 10.1.4.0/24 is transferred to Org B's resource certificate.

Org A adds the following ROA:

asID	address	maxLength
64496	10.1.4.0/24	24

7. Relying Party Use Cases

7.1. Prefix-Origin Validation Use Cases

These use cases try to systematically enumerate the situations a relying party may encounter while receiving a BGP update and making use of ROA information to interpret the validity of the prefix-origin information in the routes derived from the update. We enumerate the situations or scenarios and include a recommendation for the expected

outcome of prefix-origin validation. For a description of prefix-origin validation algorithms, see [RFC6483] and [RFC6811]. We use the terms Valid, Invalid, and NotFound as defined in [RFC6811] and summarized earlier in Section 1.3. Also see [RFC6472] for a recommendation to deprecate AS_SETs in BGP updates. The use cases described here can be potentially used as test cases for testing and evaluation of prefix-origin validation in router implementations; see, for example, [BRITE].

7.1.1. Covering ROA Prefix, maxLength Satisfied, and AS Match

ROA: {10.1.0.0/16, maxLength = 20, AS 64496}

Route has {10.1.0.0/17, Origin = AS 64496}

Recommended RPKI prefix-origin validation interpretation: Route is Valid.

Comment: The route prefix has a covering ROA prefix, and the route origin ASN matches the ROA ASN. This is a straightforward prefix-origin validation use case; it follows from the primary intention of creation of the ROA by a prefix holder.

7.1.2. Covering ROA Prefix, maxLength Exceeded, and AS Match

ROA: {10.1.0.0/16, maxLength = 20, AS 64496}

Route has {10.1.0.0/22, Origin = AS 64496}

No other covering ROA

Recommended RPKI prefix-origin validation interpretation: Route is Invalid.

Comment: In this case, the maxLength specified in the ROA is exceeded by the route prefix.

7.1.3. Covering ROA Prefix, maxLength Satisfied, and AS Mismatch

ROA: {10.1.0.0/16, maxLength = 24, AS 64496}

Route has {10.1.88.0/24, Origin = AS 64511}

No other covering ROA

Recommended RPKI prefix-origin validation interpretation: Route is Invalid.

Comment: In this case, an AS other than the one specified in the ROA is originating the route. This may be a prefix or subprefix hijack situation.

7.1.4. Covering ROA Prefix, maxLength Exceeded, and AS Mismatch

ROA: {10.1.0.0/16, maxLength = 22, AS 64496}

Route has {10.1.88.0/24, Origin = AS 64511}

No other covering ROA

Recommended RPKI prefix-origin validation interpretation: Route is Invalid.

Comment: In this case, the maxLength specified in the ROA is exceeded by the route prefix, and also an AS other than the one specified in the ROA is originating the route. This may be a subprefix hijack situation.

7.1.5. Covering ROA Prefix Not Found

Route has {10.1.3.0/24, Origin = AS 64511}

No covering ROA

Recommended RPKI prefix-origin validation interpretation: Route's validation status is NotFound.

Comment: In this case, there is no covering ROA for the route prefix. It could be a prefix or subprefix hijack situation, but this announcement does not contradict any existing ROA. During partial deployment, there would be some legitimate prefix-origin announcements for which ROAs may not have been issued yet.

7.1.6. Covering ROA Prefix and the ROA Is an AS 0 ROA

ROA: {10.1.0.0/16, maxLength = 32, AS 0}

Route has {10.1.5.0/24, Origin = AS 64511}

Recommended RPKI prefix-origin validation interpretation: Route's validation status is Invalid.

Comment: An AS 0 ROA implies by definition that the prefix listed in it and all of the more specifics of that prefix should not be used in a routing context [RFC6483] [AS0-PROC]. Also, please see related comments in Section 1.3.

7.1.7. Covering ROA Prefix Not Found but ROAs Exist for a Covering Set of More Specifics

ROA: {10.1.0.0/18, maxLength = 20, AS 64496}

ROA: {10.1.64.0/18, maxLength = 20, AS 64496}

ROA: {10.1.128.0/18, maxLength = 20, AS 64496}

ROA: {10.1.192.0/18, maxLength = 20, AS 64496}

Route has {10.1.0.0/16, Origin = AS 64496}

No covering ROA

Recommended RPKI prefix-origin validation interpretation: Route's validation status is NotFound.

Comment: In this case, the route prefix is an aggregate (/16), and it turns out that there exist ROAs for more specifics (/18s) that, if combined, can help support validation of the announced prefix-origin pair. But it is very hard in general to break up an announced prefix into constituent more specifics and check for ROA coverage for those more specifics, and hence this type of accommodation is not recommended.

7.1.8. AS_SET in Route and Covering ROA Prefix Not Found

Route has {10.1.0.0/16, AS_SET [AS 64496, AS 64497, AS 64498, AS 64499] appears in the rightmost position in the AS_PATH}

No covering ROA

Recommended RPKI prefix-origin validation interpretation: Route's validation status is NotFound.

Comment: An extremely small percentage (~0.1%) of external BGP (eBGP) updates are seen to have an AS_SET in them; this is known as proxy aggregation. In this case, the route with the AS_SET does not conflict with any ROA (i.e., the route prefix has no covering ROA prefix). Therefore, the route gets NotFound validation status.

7.1.9. Singleton AS in AS_SET (in the Route), Covering ROA Prefix, and AS Match

Route has {10.1.0.0/24, AS_SET [AS 64496] appears in the rightmost position in the AS_PATH}

ROA: {10.1.0.0/22, maxLength = 24, AS 64496}

Recommended RPKI prefix-origin validation interpretation: Route is Invalid.

Comment: In the spirit of [RFC6472], any route with an AS_SET in it should not be considered valid (by ROA-based validation). If the route contains an AS_SET and a covering ROA prefix exists for the route prefix, then the route should get an Invalid status. (Note: AS match or mismatch consideration does not apply.)

7.1.10. Singleton AS in AS_SET (in the Route), Covering ROA Prefix, and AS Mismatch

Route has {10.1.0.0/24, AS_SET [AS 64496] appears in the rightmost position in the AS_PATH}

ROA: {10.1.0.0/22, maxLength = 24, AS 64511}

Recommended RPKI prefix-origin validation interpretation: Route is Invalid.

Comment: If the route contains an AS_SET and a covering ROA prefix exists for the route prefix, then the route should get an Invalid status. (Note: AS match or mismatch consideration does not apply.)

7.1.11. Multiple ASs in AS_SET (in the Route) and Covering ROA Prefix

Route has {10.1.0.0/22, AS_SET [AS 64496, AS 64497, AS 64498, AS 64499] appears in the rightmost position in the AS_PATH}

ROA: {10.1.0.0/22, maxLength = 24, AS 64509}

No other covering ROA

Recommended RPKI prefix-origin validation interpretation: Route is Invalid.

Comment: If the route contains an AS_SET and a covering ROA prefix exists for the route prefix, then the route should get an Invalid status.

7.1.12. Multiple ASs in AS_SET (in the Route) and ROAs Exist for a Covering Set of More Specifics

ROA: {10.1.0.0/18, maxLength = 20, AS 64496}

ROA: {10.1.64.0/18, maxLength = 20, AS 64497}

ROA: {10.1.128.0/18, maxLength = 20, AS 64498}

ROA: {10.1.192.0/18, maxLength = 20, AS 64499}

Route has {10.1.0.0/16, AS_SET [AS 64496, AS 64497, AS 64498, AS 64499] appears in the rightmost position in the AS_PATH}

No covering ROA

Recommended RPKI prefix-origin validation interpretation: Route's validation status is NotFound.

Comment: In this case, the aggregate of the prefixes in the ROAs is a covering prefix (i.e., exact match or less specific) relative to the route prefix. The ASs in each of the contributing ROAs together form a set that matches the AS_SET in the route. But it is very hard in general to break up an announced prefix into constituent more specifics and check for ROA coverage for those more specifics. In any case, it may be noted once again that in the spirit of [RFC6472], any route with an AS_SET in it should not be considered valid (by ROA-based validation). In fact, the route under consideration would have received an Invalid status if the route prefix had at least one covering ROA prefix.

7.2. ROA Expiry or Receipt of a CRL Revoking a ROA

Here we enumerate use cases corresponding to router actions when RPKI objects expire or are revoked. In the cases that follow, the terms "expired ROA" or "revoked ROA" are shorthand and describe the expiry or revocation of the End Entity (EE) or resource certificate that causes a relying party to consider the corresponding ROA to have expired or been revoked, respectively.

7.2.1. ROA of Parent Prefix Is Revoked

A certificate revocation list (CRL) is received that reveals that the ROA {10.1.0.0/22, maxLength = 24, ASN 64496} is revoked. Further, a route exists in the Internet routing system for 10.1.3.0/24 originated from ASN 64496. In the absence of said revoked ROA, no covering ROA prefix exists for the route prefix (i.e., 10.1.3.0/24).

The Relying Party interpretation would be: Route's validation status is NotFound.

7.2.2. ROA of Prefix Revoked while Parent Prefix Has Covering ROA Prefix with Different ASN

A CRL is received that reveals that the ROA {10.1.3.0/24, maxLength = 24, ASN 64496} is revoked. Further, a route exists in the Internet routing system for 10.1.3.0/24 originated from ASN 64496. Additionally, a valid ROA exists for a parent prefix 10.1.0.0/22, and said ROA is {10.1.0.0/22, maxLength = 24, ASN 64511}. No other covering ROA exists for the 10.1.3.0/24 prefix.

The Relying Party interpretation would be: Route is Invalid.

7.2.3. ROA of Prefix Revoked while That of Parent Prefix Prevails

A CRL is received that reveals that the ROA {10.1.3.0/24, maxLength = 24, ASN 64496} is revoked. Further, a route exists in the Internet routing system for 10.1.3.0/24 originated from ASN 64496. Additionally, a valid ROA exists for a parent prefix 10.1.0.0/22, and said ROA is {10.1.0.0/22, maxLength = 24, ASN 64496}.

The Relying Party interpretation would be: Route is Valid.

(Clarification: Perhaps the revocation of the ROA for prefix 10.1.3.0/24 was initiated just to eliminate redundancy.)

7.2.4. ROA of Grandparent Prefix Revoked while That of Parent Prefix Prevails

A CRL is received that reveals that the ROA {10.1.0.0/20, maxLength = 24, ASN 64496} is revoked. Further, a route exists in the Internet routing system for 10.1.3.0/24 originated from ASN 64496. Additionally, a valid ROA exists for a parent prefix 10.1.0.0/22, and said ROA is {10.1.0.0/22, maxLength = 24, ASN 64496}.

The Relying Party interpretation would be: Route is Valid.

(Clarification: The ROA for less specific grandparent prefix 10.1.0.0/20 was revoked or withdrawn.)

7.2.5. Expiry of ROA of Parent Prefix

A scan of the ROA list reveals that the ROA {10.1.0.0/22, maxLength = 24, ASN 64496} has expired. Further, a route exists in the Internet routing system for 10.1.3.0/24 originated from ASN 64496. In the absence of said expired ROA, no covering ROA prefix exists for the route prefix (i.e., 10.1.3.0/24).

The Relying Party interpretation would be: Route's validation status is NotFound.

7.2.6. Expiry of ROA of Prefix while Parent Prefix Has Covering ROA with Different ASN

A scan of the ROA list reveals that the ROA {10.1.3.0/24, maxLength = 24, ASN 64496} has expired. Further, a route exists in the Internet routing system for 10.1.3.0/24 originated from ASN 64496. Additionally, a valid ROA exists for a parent prefix 10.1.0.0/22, and said ROA is {10.1.0.0/22, maxLength = 24, ASN 64511}. No other covering ROA exists for the prefix (i.e., 10.1.3.0/24).

The Relying Party interpretation would be: Route is Invalid.

7.2.7. Expiry of ROA of Prefix while That of Parent Prefix Prevails

A scan of the ROA list reveals that the ROA {10.1.3.0/24, maxLength = 24, ASN 64496} has expired. Further, a route exists in the Internet routing system for 10.1.3.0/24 originated from ASN 64496. Additionally, a valid ROA exists for a parent prefix 10.1.0.0/22, and said ROA is {10.1.0.0/22, maxLength = 24, ASN 64496}.

The Relying Party interpretation would be: Route is Valid.

7.2.8. Expiry of ROA of Grandparent Prefix while That of Parent Prefix Prevails

A scan of the ROA list reveals that the ROA {10.1.0.0/20, maxLength = 24, ASN 64496} has expired. Further, a route exists in the Internet routing system for 10.1.3.0/24 originated from ASN 64496. Additionally, a valid ROA exists for a parent prefix 10.1.0.0/22, and said ROA is {10.1.0.0/22, maxLength = 24, ASN 64496}.

The Relying Party interpretation would be: Route is Valid.

8. Acknowledgements

The authors are indebted to both Sandy Murphy and Sam Weiler for their guidance. Further, the authors would like to thank Steve Kent, Warren Kumari, Randy Bush, Curtis Villamizar, and Danny McPherson for their technical insight and review. The authors also wish to thank Elwyn Davies, Stephen Farrell, Barry Leiba, Stewart Bryant, Alexey Melnikov, and Russ Housley for their review and comments during the IESG review process.

9. Security Considerations

This memo requires no security considerations.

10. References

10.1. Normative References

[RFC4271] Rekhter, Y., Li, T., and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, February 2012.

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

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, February 2012.

10.2. Informative References

[AS0-PROC] Kumari, W., Bush, R., Schiller, H., and K. Patel, "Codification of AS 0 processing", Work in Progress, August 2012.

[BRITE] NIST, "BRITE - BGPSEC / RPKI Interoperability Test & Evaluation", Developed by the National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, 2011, <http://brite.antd.nist.gov/statics/about>.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

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

[RFC4632] Fuller, V. and T. Li, "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan", BCP 122, RFC 4632, August 2006.

[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.

[RFC5737] Arkko, J., Cotton, M., and L. Vegoda, "IPv4 Address Blocks Reserved for Documentation", RFC 5737, January 2010.

[RFC6472] Kumari, W. and K. Sriram, "Recommendation for Not Using AS_SET and AS_CONFED_SET in BGP", BCP 172, RFC 6472, December 2011.

[RFC6483] Huston, G. and G. Michaelson, "Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)", RFC 6483, February 2012.

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, January 2013.

Authors' Addresses

Terry Manderson
ICANN

EMail: terry.manderson@icann.org

Kotikalapudi Sriram
US NIST

EMail: ksriram@nist.gov

Russ White
Verisign

EMail: russ@riw.us