Secure Inter-Domain Routing
Internet-Draft
Intended status: Informational
Expires: June 25, 2011

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

December 22, 2010

Use Cases and interpretation of RPKI objects for issuers and relying parties
draft-ietf-sidr-usecases-01

Abstract

This document provides use cases, directions, and interpretations for organizations and relying parties when creating or encountering RPKI object scenarios in the public RPKI in relation to the Internet routing system.

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 June 25, 2011.

Copyright Notice

Table of Contents

1. Introduction

This document provides suggested use cases, directions, and interpretations for organizations and relying parties when creating or encountering RPKI object scenarios in the public RPKI 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" [I-D.ietf-sidr-res-certs] "X.509 Extensions for IP Addresses and AS Identifiers" [RFC3779], "A Profile for Route Origin Authorizations (ROAs)" [I-D.ietf-sidr-roa-format], "Validation of Route Origination in BGP using the Resource Certificate PKI and ROAs" [I-D.ietf-sidr-roa-validation], and BGP Prefix Origin Validation" [I-D.pmohapat-sidr-pfx-validate].

1.2. Definitions

The following definitions are in use in this document.

Autonomous System - A network under a single technical administration that presents a consistent picture of what destinations are reachable through it.

Autonomous System Number (ASN) - An officially registered number

representing an autonomous system.

Prefix - A network address and an integer that specifies the length of a mask to be applied to the address to represent a set of numerically adjacent addresses.

Route - A prefix and a sequence of one or more autonomous system numbers.

Origin AS - The Autonomous System, designated by an ASN, which originates a route. Seen as the "First" ASN in a route.

Specific route - A route that has a longer prefix than an aggregate.

Aggregate route - A more general route in the presence of a specific route.

Covering Aggregate - A route that covers one or more specific routes.

Multi-homed Autonomous System - An Autonomous System that is connected, and announces routes, to two or more Autonomous Systems.

Multi-homed prefix or subnet - A prefix (i.e., subnet) that is originated via two or more Autonomous Systems to which the subnet is connected.

Resource - Internet (IP) addresses or Autonomous System Number.

Allocation - The set of resources provided to an entity or organization for its use.

Sub-allocation - The set of a resources subordinate to an allocation assigned to another entity or organization.

Transit Provider - An Autonomous System that carries traffic that neither originates nor is the destination of that traffic.

Upstream - See "Transit Provider".

Child - A Sub-allocation that has resulted from an Allocation.

Parent - An allocation from which the subject prefix is a Child.

Grandchild - A Sub-allocation from one or more previous Sub-allocations.

Grandparent - The allocation from which the prefix is a Grandchild.

Update prefix - The prefix seen in a routing update.

ROA prefix - The prefix described in a ROA.

Covering Prefix - The ROA Prefix is an exact match or a less specific when compared to the update prefix.

No relevant ROA - No ROA exists that has a covering prefix for the update prefix.

No other relevant ROA - No other ROA (besides any that is(are) already cited) that has a covering prefix for the update prefix.

1.3. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

2. Overview

2.1. General interpretation of RPKI object semantics

It is important that in the interpretation of relying parties (RP), or relying party routing software, that a 'make before break' stance is applied. This means that a RP should implement a routing decision process where a routing update ("route") is assumed to be intended unless proven otherwise by the existence of a valid RPKI object. For all of the cases in this document it is assumed that RPKI objects validate (or otherwise) in accordance with [I-D.ietf-sidr-res-certs], [I-D.ietf-sidr-arch], [I-D.ietf-sidr-roa-validation] unless otherwise stated.

While many of the examples provided here illustrate organizations

using their own autonomous system numbers to originate routes, it should be recognised 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.

3.1. Single Announcement

An organization (Org A with ASN 64496) has been allocated the prefix 192.168.2.0/24. 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
192.168.2.0/24	AS64496	Org A

The issuing party would create the following RPKI objects: TBC

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	AS64496	Org A

| 10.1.0.0/20 | AS64496 | Org A |
+---+

The issuing party would create the following RPKI objects: TBC

3.3. Aggregate with a More Specific from a Different ASN

An organization (Org A with ASN 64496 and ASN 64499) 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 64499 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	AS64496	Org A
10.1.0.0/20	AS64499	Org A

The issuing party would create the following RPKI objects: TBC

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 desirable announcements (and organization) would be:

+---+

Prefix	Origin AS	Organization
10.1.0.0/16	AS64496	Org A
10.1.0.0/20	AS64496	Org A
10.1.16.0/20	AS64511	Org B

The issuing parties would create the following RPKI objects: TBC

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 would create the following RPKI objects: TBC

3.6. Restriction of New ASN

An organization has recently been allocated an additional 4 byte ASN 65535. Its network deployment is not yet ready to use this ASN and wishes to restrict all possible uses of ASN 65535 using RPKI.

The following announcements would be considered undesirable:

Prefix	Origin AS	Organization
ANY	AS65535	ANY

The issuing party would create the following RPKI objects: TBC

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 and the /16 aggregate. However it wishes to restrict any possible announcement of 10.1.128.0/17 or more specifics of that /17 using RPKI.

The desired announcements would be:

Prefix	Origin AS	Organization
10.1.0.0/16	AS64496	Org A
10.1.0.0/17	AS64496	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 would create the following RPKI objects: TBC

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	AS64496	Org A
10.1.0.0/17	AS64496	Org A
...	AS64496	Org A
10.1.128.0/20	AS64496	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 would create the following RPKI objects: TBC

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 65535, and Org C with ASN 64499. It wishes to restrict those customers from advertising any corresponding routes more specific than a /22.

The desired announcements would be:

Prefix	Origin AS	Organization
10.1.0.0/16	AS64496	Org A
10.1.0.0/20	AS65535	Org B
10.1.128.0/20	AS64499	Org C
10.1.4.0/22	AS65535	Org B

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

Prefix	Origin AS	Organization
10.1.0.0/24	AS65535	Org B
10.1.128.0/24	AS64499	Org C
.....	...	...

| 10.1.0.0/23 | ANY AS | ANY |
+---+

The issuing party would create the following RPKI objects: TBC

3.10. Aggregation and Origination by an Upstream

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

Organization	ASN	Prefix
Org A	AS64496	10.1.0.0/24
Org B	AS65535	10.1.3.0/24
Org C	AS64499	10.1.1.0/24
Org D	AS64512	10.1.2.0/24

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

The desired announcements (and organization) would be:

Prefix	Origin AS	Organization
10.1.0.0/24	AS64496	Org A
10.1.3.0/24	AS65535	Org B
10.1.1.0/24	AS64499	Org C
10.1.2.0/24	AS64512	Org D
10.1.0.0/22	AS64497	Transit A

The issuing parties would create the following RPKI objects: TBC

3.11. Rogue Aggregation and Origination by an Upstream

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

Organization	ASN	Prefix
Org A	AS64496	10.1.0.0/24
Org B	AS65535	10.1.3.0/24
Org C	AS64499	10.1.1.0/24
Org D	AS64512	10.1.2.0/24

These organizations share a common upstream provider Transit A (ASN 64497) that originates an aggregate of these prefixes where possible. In this situation organization B (ASN 65535, 10.1.3.0/24) does not wish for its prefix to be aggregated by the upstream

The desired announcements (and organization) would be:

Prefix	Origin AS	Organization
10.1.0.0/24	AS64496	Org A
10.1.3.0/24	AS65535	Org B
10.1.1.0/24	AS64499	Org C
10.1.2.0/24	AS64512	Org D
10.1.0.0/23	AS64497	Transit A

The following announcement would be undesirable:

Prefix	Origin AS	Organization
10.1.0.0/22	AS64497	Transit A

The issuing parties would create the following RPKI objects: TBC

4. Adjacency Use Cases

Issues regarding validation of adjacency, or path validation, are currently out of scope of the SIDR-WG charter. The use cases in this

section are listed here as a reminder that the work goes beyond origination and at the stage when origination has been addressed by the WG, a re-charter to encompass adjacency will allow consideration of these use cases.

4.1. Multi-homed

An organization (Org A with ASN 64496) has been allocated the prefix 10.1.0.0/16. Its upstream transit providers are Transit A with ASN 65535 and Transit B with ASN 64499. The organization announces the /16 aggregate. It permits that ASN 65535 and ASN 64499 may further pass on the aggregate route to their peers or upstreams.

The following announcements and paths would be desired:

Prefix	Origin AS	Path
10.1.0.0/16	AS64496	AS64499 AS64496
10.1.0.0/16	AS64496	AS65535 AS64496

The issuing parties would create the following RPKI objects: TBC

4.2. Restricting Peers

An organization (Org A with ASN 64496) has been allocated the prefix 10.1.0.0/16. Its two upstreams are Transit X with ASN 65535 and Transit Y with ASN 64499. The organization (ASN 64496) peers with a third AS, Peer Z with ASN 64511. Org A announces the more specific 10.1.0.0/24 and the /16 aggregate. It wishes that only ASNs 65535 and 64499 may announce the aggregate and more specifics to their upstreams. ASN 64511, the peer, may not further announce (pass on, or leak) any routes for 10.1.0.0/16 and 10.1.0.0/24.

The following announcements and paths would be desired:

Prefix	Origin AS	Path
10.1.0.0/16	AS64496	AS64499 AS64496
10.1.0.0/24	AS64496	AS64499 AS64496

10.1.0.0/16	AS64496	AS65535 AS64496
10.1.0.0/24	AS64496	AS65535 AS64496
10.1.0.0/16	AS64496	Any_AS AS64499 AS64496
10.1.0.0/24	AS64496	Any_AS AS64499 AS64496
10.1.0.0/16	AS64496	Any_AS AS65535 AS64496
10.1.0.0/24	AS64496	Any_AS AS65535 AS64496
10.1.0.0/16	AS64496	AS64511 AS64496
10.1.0.0/24	AS64496	AS64511 AS64496

The following announcements and paths would be considered undesirable:

Prefix	Origin AS	Path
10.1.0.0/16	AS64496	Any_AS AS64511 AS64496
10.1.0.0/24	AS64496	Any_AS AS64511 AS64496

The issuing parties would create the following RPKI objects: TBC

5. Partial Deployment Use Cases

5.1. Parent does not do RPKI

An organization (Org A with ASN 64511) is multi-homed 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	AS64511	Org A	Yes

| 10.1.0.0/16 | AS64496 | Transit X | No |
+---+

The issuing parties would create the following RPKI objects: TBC

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 and Org C with ASN 65535 (respectively) who are multi-homed. Org B (ASN 64511) does not participate in RPKI. Org C (ASN 65535) participates in RPKI.

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

Prefix	Origin AS	Organization	RPKI
10.1.0.0/16	AS64496	Org A	Yes
10.1.0.0/20	AS64496	Org A	Yes
10.1.16.0/20	AS64511	Org B	No
10.1.32.0/20	AS65535	Org C	YES

The issuing parties would create the following RPKI objects: TBC

5.3. Grandchild Does Not Participate in RPKI

Consider the previous example with an extension by where Org B, who does not participate in RPKI, further allocates 10.1.17.0/24 to Org X with ASN 64512. Org X does not participate in RPKI.

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

Prefix	Origin AS	Organization	RPKI
10.1.0.0/16	AS64496	Org A	Yes

10.1.0.0/20	AS64496	Org A	Yes
10.1.16.0/20	AS64511	Org B	No
10.1.32.0/20	AS65535	Org C	YES
10.1.17.0/24	AS64512	Org X	No

The issuing parties would create the following RPKI objects: TBC

6. Transfer Use Cases

6.1. Transfer of in-use prefix and autonomous system number

Organization A holds the resource 10.1.0.0/20 and it is currently in use and originated from AS64496 with valid RPKI objects in place. Organization 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: TBC

6.2. Transfer of in-use prefix

Organization A holds the resource 10.1.0.0/8 and it is currently in use and originated from AS64496 with valid RPKI objects in place. Organization B has acquired the address and desires an RPKI transfer on a particular date and time. This prefix will be originated by AS65535 as a result of this transfer.

The following RPKI objects would be created/revoked: TBC

6.3. Transfer of un-used prefix

Organization A holds the resource 10.1.0.0/8 and AS65535 (with RPKI objects). Organization B has acquired an unused portion (10.1.4.0/24) of the prefix and desires an RPKI transfer on a particular date and time. Organization B will originate a route 10.1.4.0/24 from AS64496

The following RPKI objects would be created/revoked: TBC

7. Relying Party Use Cases

7.1. ROA Expiry or receipt of a CRL covering a ROA

In the cases which follow, the terms "expired ROA" or "revoked ROA" are shorthand, and describe the appropriate expiry or revocation of the EE or Resource Certificates that causes a relying party to consider the corresponding ROA to be viewed as expired or revoked.

7.1.1. ROA of Parent Prefix is Revoked

A certificate revocation list (CRL) is received which reveals that the ROA containing the prefix 10.1.0.0/16; maxLength 24 with ASN64496 is revoked. Further, a prefix route exists in the Internet routing system for 10.1.4.0/24 originated from ASN64496.

The Relying Party interpretation would be: TBC

7.1.2. ROA of Prefix Revoked

A CRL is received which reveals that the ROA containing the prefix 10.1.4.0/24; maxLength 24 with ASN64496 is revoked. Further, a prefix route exists in the Internet routing system for 10.1.4.0/24 originated from ASN64496.

The Relying Party interpretation would be: TBC

A counter example: If there was simultaneously a valid ROA containing the (less specific) prefix 10.1.0.0/20; maxLength 24 with ASN64496. (see Section 7.1.4)

The Relying Party interpretation would be: TBC

7.1.3. ROA of Grandparent Prefix Revoked while that of Parent Prefix Prevails

A CRL is received which reveals that the ROA containing the prefix 10.1.0.0/16; maxLength 24 with ASN64496 is revoked. Further, a prefix route exists in the Internet routing system for 10.1.4.0/24 originated from ASN64496. Additionally, the current ROA list has a valid ROA containing the prefix 10.1.0.0/20; maxLength 24 with ASN64496.

The Relying Party interpretation would be: TBC

(Clarification: ROA for less specific grandparent prefix 10.1.0.0/16 was revoked or withdrawn)

The Relying Party interpretation would be: TBC

7.1.4. ROA of Prefix Revoked while that of Parent Prefix Prevails

A CRL is received which reveals that the ROA containing the prefix 10.1.4.0/24; maxLength 24 with ASN64496 is revoked. Further, a prefix route exists in the Internet routing system for 10.1.4.0/24 originated from ASN64496. Additionally, the current ROA list has a valid ROA containing the prefix 10.1.0.0/20; maxLength 24 with ASN64496.

The Relying Party interpretation would be: TBC

(Clarification: Perhaps the revocation of ROA for prefix 10.1.4.0/24 was initiated just to eliminate redundancy.)

7.1.5. Expiry of ROA of Parent Prefix

A scan of the ROA list reveals that the ROA containing the prefix 10.1.0.0/16; maxLength 24 with ASN64496 has expired. Further, a prefix route exists in the Internet routing system for 10.1.4.0/24 originated from ASN64496.

The Relying Party interpretation would be: TBC

7.1.6. Expiry of ROA of Prefix

A scan of the ROA list reveals that the ROA containing the prefix 10.1.4.0/24; maxLength 24 with ASN64496 has expired. Further, a prefix route exists in the Internet routing system for 10.1.4.0/24 originated from ASN64496.

The Relying Party interpretation would be: TBC

7.1.7. Expiry of ROA of Grandparent Prefix while ROA of Parent Prefix Prevails

A scan of the ROA list reveals that the ROA containing the prefix 10.1.0.0/16; maxLength 24 with ASN64496 has expired. Further, a prefix route exists in the Internet routing system for 10.1.4.0/24

originated from ASN64496. Additionally, the current ROA list has a valid ROA containing the prefix 10.1.0.0/20; maxLength 24 with ASN64496.

The Relying Party interpretation would be: TBC

(Clarification: ROA for less specific grandparent prefix 10.1.0.0/16 has expired.)

7.1.8. Expiry of ROA of Prefix while ROA of Parent Prefix Prevails

A scan of the ROA list reveals that the ROA containing the prefix 10.1.4.0/24; maxLength 24 with ASN64496 has expired. Further, a prefix route exists in the Internet routing system for 10.1.4.0/24 originated from ASN64496. Additionally, the current ROA list has a valid ROA containing the prefix 10.1.0.0/20; maxLength 24 with ASN64496.

The Relying Party interpretation would be: TBC

(Clarification: Perhaps the expiry of the ROA for prefix 10.1.4.0/24 was meant to eliminate redundancy.)

7.2. 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 update. We enumerate the situations or scenarios but do not make a final recommendation on any RPKI interpretation. For work on development of prefix-origin validation algorithms, see [I-D.ietf-sidr-roa-validation] and [I-D.pmohapat-sidr-pfx-validate]. Also see [I-D.ietf-idr-deprecate-as-sets] for work-in-progress in the IDR WG to deprecate AS_SETs in BGP updates (especially in the context of RPKI-based validation).

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

ROA: {10.1.0.0/16, maxLength = 20, AS64496}

Update has {10.1.0.0/17, Origin = AS64496}

Recommended RPKI prefix-origin validation interpretation: TBC

Comment: This is a straight forward prefix-origin validation use case; it follows from the primary intention of creation of ROA by a resource owner.

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

ROA: {10.1.0.0/16, maxLength = 20, AS64496}

Update has {10.1.0.0/22, Origin = AS64496}

No other relevant ROA

Recommended RPKI prefix-origin validation interpretation: TBC

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

7.2.3. Covering ROA Prefix, maxLength Satisfied, and AS Mismatch:

ROA: {10.1.0.0/16, maxLength = 24, AS64496}

Update has {10.1.88.0/24, Origin = AS65535}

No other relevant ROA

Recommended RPKI prefix-origin validation interpretation: TBC

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

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

ROA: {10.1.0.0/16, maxLength = 22, AS64496}

Update has {10.1.88.0/24, Origin = AS65535}

No other relevant ROA

Recommended RPKI prefix-origin validation interpretation: TBC

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

7.2.5. Covering ROA Prefix Not Found

Update has {240.1.1.0/24, Origin = AS65535}

No relevant ROA

Recommended RPKI prefix-origin validation interpretation: TBC

Comment: In this case there is no relevant ROA that has a covering prefix for the update prefix. It could be a case of 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.

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

ROA: {10.1.0.0/18, maxLength = 20, AS64496}

ROA: {10.1.64.0/18, maxLength = 20, AS64496}

ROA: {10.1.128.0/18, maxLength = 20, AS64496}

ROA: {10.1.192.0/18, maxLength = 20, AS64496}

Update has {10.1.0.0/16, Origin = AS64496}

No relevant ROA

Recommended RPKI prefix-origin validation interpretation: TBC

Comment: In this case the update prefix is an aggregate, and it turns out that there exit ROAs for more specifics which, if combined, can

help support validation of the announced prefix-origin pair. But it is very hard in general to breakup an announced prefix into constituent more specifics and check for ROA coverage for those more specifics.

7.2.7. AS_SET in Update and Covering ROA Prefix Not Found

Update has {10.1.0.0/16, Origin = [AS64496, AS64497, AS64498, AS64497]}

No relevant ROA

Recommended RPKI prefix-origin validation interpretation: TBC

Comment: An extremely small percentage (~0.1%) of eBGP updates are seen to have an AS_SET in them as origin; this is known as proxy aggregation. In this case, update with the AS_SET does not conflict with any ROA.

7.2.8. Singleton AS in AS_SET (in the Update), Covering ROA Prefix, and AS Match

Update has {10.1.0.0/24, Origin = [AS64496]} (Note: AS_SET with singleton AS appears in origin AS position.)

ROA: {10.1.0.0/22, maxLength = 24, AS64496}

Recommended RPKI prefix-origin validation interpretation: TBC

Comment: In the spirit of [I-D.ietf-idr-deprecate-as-sets], possibly any update with an AS_SET in it should not be considered valid (by ROA-based validation). But does a scenario as described in the example here need be treated differently?

7.2.9. Singleton AS in AS_SET (in the Update), Covering ROA Prefix, and AS Mismatch

Update has {10.1.0.0/24, Origin = [AS64496]}

(Note: AS_SET with singleton AS appears in origin AS position.)

ROA: {10.1.0.0/22, maxLength = 24, AS65535} No other relevant ROA.

Recommended RPKI prefix-origin validation interpretation: TBC

Comment: In this case, update with the AS_SET does conflict with a ROA and there is no other relevant ROA.

7.2.10. Multiple ASs in AS_SET (in the Update) and Covering ROA Prefix

Update has {10.1.0.0/22, Origin = [AS64496, AS64497, AS64498, AS64497]}

ROA: {10.1.0.0/22, maxLength = 24, AS65535} No other relevant ROA.

Recommended RPKI prefix-origin validation interpretation: TBC

Comment: In this case, update with the AS_SET conflicts with a ROA and there is no other relevant ROA.

7.2.11. Update has an AS_SET as Origin and ROAs Exist for a Covering Set of More Specifics

ROA: {10.1.0.0/18, maxLength = 20, AS64496} ROA: {10.1.64.0/18, maxLength = 20, AS64497} ROA: {10.1.128.0/18, maxLength = 20, AS64498} ROA: {10.1.192.0/18, maxLength = 20, AS64499}

Update has {10.1.0.0/16, Origin = [AS64496, AS64497, AS64498, AS64497]}

No (directly) relevant ROA

Recommended RPKI prefix-origin validation interpretation: TBC

Comment: In this case the aggregate of the prefixes in the ROAs is a covering prefix for the update prefix. The ASs in each of the contributing ROAs together form a set that matches the AS_SET in the

update. But it is very hard in general to breakup 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 [I-D.ietf-idr-deprecate-as-sets], possibly any update with an AS_SET in it should not be considered valid (by ROA-

based validation).

8. Acknowledgements

The authors are indebted to both Sandy Murphy and Sam Weiler for their guidance. Further, the authors would like to thank Curtis Villamizar, Steve Kent, and Danny McPherson for their technical insight and review.

9. IANA Considerations

This memo includes no request to IANA.

10. Security Considerations

This memo requires no security considerations

11. Normative References

[I-D.ietf-idr-deprecate-as-sets]
Kumari, W., "Deprecation of BGP AS_SET, AS_CONFED_SET.", draft-ietf-idr-deprecate-as-sets-00 (work in progress), November 2010.

[I-D.ietf-sidr-arch]
Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", draft-ietf-sidr-arch-11 (work in progress), September 2010.

[I-D.ietf-sidr-res-certs]
Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", draft-ietf-sidr-res-certs-21 (work in progress), December 2010.

[I-D.ietf-sidr-roa-format]
Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", draft-ietf-sidr-roa-format-09 (work in progress),

November 2010.

[I-D.ietf-sidr-roa-validation]
Huston, G. and G. Michaelson, "Validation of Route Origination using the Resource Certificate PKI and ROAs", draft-ietf-sidr-roa-validation-10 (work in progress), November 2010.

[I-D.pmohapat-sidr-pfx-validate]
Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", draft-pmohapat-sidr-pfx-validate-07 (work in progress), April 2010.

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

[RFC3852] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3852, July 2004.

[RFC4055] Schaad, J., Kaliski, B., and R. Housley, "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 4055, June 2005.

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

[RFC4893] Vohra, Q. and E. Chen, "BGP Support for Four-octet AS Number Space", RFC 4893, May 2007.

[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.

Authors' Addresses

Terry Manderson
ICANN

Email: terry.manderson@icann.org

Kotikalapudi Sriram
US NIST

Email: ksriram@nist.gov

Russ White
Cisco

Email: russ@cisco.com