Secure Inter-Domain Routing
Internet-Draft
Intended status: Informational
Expires: April 29, 2010

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

October 26, 2009

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

Abstract

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

Table of Contents

1. Introduction

This document provides suggested use cases, direction and interpretations for organisations 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], "A Profile for Bogon Origin Authorizations (BOAs)" [I-D.ietf-sidr-bogons], "Validation of Route Origination in BGP using the Resource Certificate PKI" [I-D.ietf-sidr-roa-validation],

1.2. Definitions

The following definitions are in use in this document.

Autonomous System (AS) Number (ASN) - An officially registered number reprsenting a common, clearly defined routing policy for use in Internet routing systems.

Prefix - A network address and the prefix length.

Route - A tuple of prefix and Autonomous System Number announced to Internet routing systems.

Origin AS - The Autonomous System, designated by number, which originates a route.

Aggregate - The result of where multiple specific prefixes are aggregated into one covering route.

More specific - A route that has a longer prefix than a covering aggregate.

Multi-homed - An Autonomous System that has active connections to more than one other Autonomous System

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

Sub-allocation - Where a holder of a resource further allocates a

portion of the resource to another entity or organisation.

Allocation - The set of resources allocated to an entity or organisation.

Transit Provider - An Autonomous System that provides access to other networks through itself.

Upstream - See "Transit Provider".

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

Parent - An allocation from which the subject prefix was sub-allocated.

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

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 the interpretation of relying parties, or relying party routing software, that implements a level of routing decision, when a routing update ("route") is received in light of the existence or non-existence of a corresponding RPKI object a 'make before break' stance is taken. This means that the relying party should do all possible steps to ensure a route is valid, before attempting to declare it otherwise. 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], and [I-D.ietf-sidr-bogons] unless otherwise stated.

While many of the examples provided here demonstrate organisations with their own autonomous system numbers, it should be recognised that a prefix holder not necessarily be the holder of an autonomous system number, but simply use the autonomous system number for the purposes of origination.

3. Origination use cases

3.1. Single announcement

An organisation (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 to the Internet routing system such that relying parties interpret the route as valid.

The resulting valid announcement (and organisation) would be:

Prefix	Origin AS	Organisation
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 organisation (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 to the Internet routing system such that relying parties interpret the routes as valid.

The resulting valid announcements (and organisation) would be:

Prefix	Origin AS	Organisation
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 more specific from different ASN

An organisation (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 to the Internet routing system such that relying parties interpret the routes as valid.

The resulting valid announcements (and organisation) would be:

Prefix	Origin AS	Organisation
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 multi-homed customer

An organisation (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 route prefix route from ASN 64511. ASN 64496 will also announce the aggregate route to the Internet routing system such that relying parties interpret the routes as valid.

The resulting valid announcements (and organisation) would be:

Prefix	Origin AS	Organisation
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 new allocation

An organisation 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 invalid:

Prefix	Origin AS	Organisation
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 organisation has recently been allocated an additional 4 byte ASN 65551. Its network deployment is not yet ready to use this ASN and wishes to restrict all possible uses of ASN 65551 using RPKI.

The following announcements would be considered invalid:

Prefix	Origin AS	Organisation
ANY	AS65551	ANY

The issuing party would create the following RPKI objects: TBC

3.7. Restriction of part of allocation

An organisation (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 resulting valid announcements would be:

Prefix	Origin AS	Organisation
10.1.0.0/16	AS64496	Org A
10.1.0.0/17	AS64496	Org A

The following announcements would be considered invalid:

Prefix	Origin AS	Organisation
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 resulting valid announcements (and organisation) would be:

Prefix	Origin AS	Organisation
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 invalid:

Prefix	Origin AS	Organisation
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 65551, and Org C with ASN 64499. It wishes to restrict those customers from advertising any corresponding routes more specific than a /22.

The resulting valid announcements would be:

Prefix	Origin AS	Organisation
10.1.0.0/16	AS64496	Org A
10.1.0.0/20	AS65551	Org B
10.1.128.0/20	AS64499	Org C
10.1.4.0/22	AS65551	Org B

The following example announcements (and organisation) would be considered invalid:

Prefix	Origin AS	Organisation
10.1.0.0/24	AS65551	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. Permitted Aggregation and origination by an upstream

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

Organisation	ASN	Prefix
Org A	AS64496	10.1.0.0/24
Org B	AS65551	10.1.3.0/24
Org C	AS64499	10.1.1.0/24
Org D	AS64512	10.1.2.0/24

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

The resulting valid announcements (and organisation) would be:

Prefix	Origin AS	Organisation
10.1.0.0/24	AS64496	Org A
10.1.3.0/24	AS65551	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 organisations with the following resources which were acquired independently from any transit provider.

Organisation	ASN	Prefix
Org A	AS64496	10.1.0.0/24
Org B	AS65551	10.1.3.0/24
Org C	AS64499	10.1.1.0/24
Org D	AS64512	10.1.2.0/24

These organisations share a common upstream provider Transit A (ASN 64497) that originates an aggregate of these prefixes where possible. Org B (ASN 65551, 10.1.3.0/24) does not wish for its prefix to be aggregated by any upstream

The resulting valid announcements (and organisation) would be:

Prefix	Origin AS	Organisation
10.1.0.0/24	AS64496	Org A
10.1.3.0/24	AS65551	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 invalid:

Prefix	Origin AS	Organisation
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 is 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 organisation (Org A with ASN 64496) has been allocated the prefix 10.1.0.0/16. Its upstreams transit providers are Transit A with ASN 65551 and Transit B ASN 64499. The organisation announces the /16 aggregate. It permits that ASN 65551 and ASN 64499 may further pass on the aggregate route to their peers or upstreams.

The following announcements and paths would be considered valid:

Prefix	Origin AS	Path
10.1.0.0/16	AS64496	AS64499 AS64496
10.1.0.0/16	AS64496	AS65551 AS64496

The issuing parties would create the following RPKI objects: TBC

4.2. Restricting peers

An organisation (Org A with ASN 64496) has been allocated the prefix 10.1.0.0/16. Its two upstreams are Transit A with ASN 65551 and Transit B with ASN 64499. The organisation (ASN 64496) peers with a third AS, Peer A with ASN 64511. Org A announces the more specific 10.1.0.0/24 and the /16 aggregate. It wishes that only ASNs 65551 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 considered valid:

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	AS65551 AS64496
10.1.0.0/24	AS64496	AS65551 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 AS65551 AS64496
10.1.0.0/24	AS64496	Any_AS AS65551 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 invalid:

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 organisation (Org A with ASN 64511) is multi-homed has been assigned the prefix 10.1.0.0/20 from its upstream (Transit A 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 A (ASN 64496) which announces the aggregate 10.1.0.0/16 has not yet adopted RPKI.

The resulting valid announcements (and organisation with RPKI adoption) would be:

Prefix	Origin AS	Organisation	RPKI
10.1.0.0/20	AS64511	Org A	Yes
10.1.0.0/16	AS64496	Transit A	No

```
   +-----------------------------------------------------+
```

The issuing parties would create the following RPKI objects: TBC

5.2. Only some children participate

An organisation (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 65551 (respectively) who are multi-homed. Org B (ASN 64511) does not participate in RPKI. Org C (ASN 65551) participates in RPKI.

The resulting valid announcements (and organisation with RPKI adoption) would be:

Prefix	Origin AS	Organisation	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	AS65551	Org C	YES

The issuing parties would create the following RPKI objects: TBC

5.3. Grandchild allocations

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.

The resulting valid announcements (and organisation with RPKI adoption) would be:

Prefix	Origin AS	Organisation	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	AS65551	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

Organisation A holds the resource 10.1.0.0/20 and is currently is use and originated from AS64496 with valid RPKI objects in place. Organisation B has acquired these resources 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

Organisation A holds the resource 10.1.0.0/8 and it is currently is use and originated from AS64496 with valid RPKI objects in place. Organisation B has acquired this resource and desires an RPKI transfer on a particular date and time with the additional change of originating the prefix from AS65551.

The following RPKI objects would be created/revoked: TBC

6.3. Transfer of un-used prefix

Organisation A holds the resource 10.1.0.0/8 (with RPKI objects). Organisation B has acquired an unused portion of the resource (10.1.4.0/24) and desires an RPKI transfer on a particular date and time.

The following RPKI objects would be created/revoked: TBC

7. Relying Party use cases

7.1. Use Cases Related to ROA Expiry or receipt of a CRL covering a ROA

Note: In the cases which follow the terms "expired ROA" or "revoked ROA" are shorthand, and describe the appropriate revocation or expiry of EE or Resource Certificates which result in the RPKI invalidation of a ROA.

7.1.1. ROA of Parent Prefix is Revoked

A revocation certificate 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.

Note: Parent prefix here simply means a less specific prefix.

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 a valid ROA containing the (less specific) prefix 10.1.0.0/20; maxLength 24 with ASN64496.

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 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 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.)

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 and Danny McPherson for technical insight.

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-sidr-arch]
Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", draft-ietf-sidr-arch-08 (work in progress), July 2009.

[I-D.ietf-sidr-bogons]
Manderson, T., "A Profile for Bogon Origin Attestations (BOAs)", draft-ietf-sidr-bogons-03 (work in progress), May 2009.

[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-17 (work in progress), September 2009.

[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-05 (work in progress), July 2009.

[I-D.ietf-sidr-roa-validation]
Huston, G. and G. Michaelson, "Validation of Route Origination in BGP using the Resource Certificate PKI and ROAs", draft-ietf-sidr-roa-validation-03 (work in progress), August 2009.

[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
NIST

Email: ksriram@nist.gov

Russ White
Cisco

Email: russ@cisco.com