MANRS

Mutually Agreed Norms for Routing Security

Common ROA Management Requirements and Security Standards for Operators of RPKI Services (ORS)

Version 1.3

Use of RPKI for securing BGP announcements has increased significantly over the last few years. In addition, we have seen an increase in networks, both small and large, filtering invalid BGP announcements. As the Internet adapts to these new security measures it is important that their implementation does not negatively affect network operations. Many network operators are new to these security measures and we have seen an increase in misconfigurations from networks, which can result in network disruptions. While some of these issues can be avoided by network operators themselves, others need to be addressed by the **O**perators of **R**PKI **S**ervices (ORS) responsible for the operation of a hosted RPKI[1]. With this document, we outline changes and improvements ORS can make to increase security and reliability of ROA. These requirements and security standards will make more networks adapt well to RPKI and avoid common mistakes with ROA management.

1. ROA (Route Origin Authorization)

[These action items cover the management of ROAs and do not cover other digitally signed objects associated with the organization membership or a resource certificate. These action items only apply for Hosted RPKI by ORSs and do not cover delegated RPKI.]

A ROA is a cryptographically signed object that states an Autonomous System (AS) is authorized to originate a particular IP address prefix or set of prefixes. A ROA also determines the validity period for that statement. Before use, a ROA has to be validated using the RPKI system (https://datatracker.ietf.org/doc/html/rfc6482#section-4). Once a ROA is validated, the resulting object contains at least one IP prefix, a maximum length, and an origin AS number. This object is referred to as a validated ROA payload (VRP). The VRPs in their turn can be used to check the validity of routing announcements received by a network. With the increasing adoption of RPKI, it is important that management of ROAs follows a set of standard practices to avoid network disruptions. Given the scale of ASNs on the Internet, it is likely that some networks will have network disruption due to incorrect or invalid ROAs. To avoid such outages, ORSs (Operators of RPKI Services) must take the following actions.

a) **Auto-renewal of a ROA** – Responsibility for ROA maintenance and renewal should be clearly defined. For all **hosted RPKI**, all such responsibility shall lay with the ORSs. In specific, auto-renewal of all ROAs for hosted RPKI should be no later than 90 days prior to its expiry. ORS can provide an option for network operators to opt out of auto-renewal, but the default option should auto-renew the certificates.

---

1 Hosted RPKI is an infrastructure in which the ORS hosts a Certificate Authority (CA) and signs all Route Origin Authorizations(ROAs) on behalf of resource holders. An ORS is responsible for operating hosted RPKI CAs and a repository. An alternative model is a delegated RPKI, when the resource holder operates the CA and is responsible for key management, generation, and signing of ROAs.

b) **Standard Validity** – ROA validity should follow standard industry practice. Network operators can have resources in multiple registries and should not require custom validity management in each registry. ORSs should provide at least two years of ROA validity. Periods shorter than two years can lead to more ROA/certificate expiry issues and longer periods can have ROA/certificate compliance issues. This does not prevent a network operator from deleting a ROA at any time, if needed.

c) **Alerting on ROA expiration or renewal** – network operators that opt out for auto-renewal should get an email alert of a ROA expiration 4 weeks before the expiry. Network operators that use auto-renewal should get an email alert when a ROA is renewed.

2. API and API Security for Hosted ROA Management

[This action item covers the management of a ROA and does not cover management for network operators other properties such as customers, routes, ASNs etc.]

Network operators with large address space rely on automated services to manage ROAs using hosted RPKI. There is a need for safe programmatic ways to list ROAs, add, update or delete ROAs. All operations related to ROA management (Create, update, and delete) should be supported via an API consistent among the ORSs. For security, it is important that the access token to the API has a time limit and access level. Below are the list specific action items:

a) **API for ROA Management** – ORSs should provide APIs for following ROA management operations. By preference the API should support signing of the payload by a private key of the corresponding resource certificate. The API specification is outside the scope of this document. Below is the list of essential API calls with examples of how they can possibly look like.

- **Get ROAs** [Example of an API call: **/GetRoas?Key=<api-key>**] Gets all ROAs in the member's account.

- **Add/Update ROAs:** [Example of an API call: **/PublishRoas?ROAId=<ROAID>&Key=<api-key>**] Add or update individual ROAs. The body should contain details regarding ROAs. Multiple ROAs can be submitted for addition or withdrawal as a butch, and processed as an atomic operation (for example, to avoid blocking or warning when one of the batch operations may invalidate the existing announcement). Below is a sample body for the request:

```
{
        "added": [
                {
                    "asn":" AS64500",
                    "prefix": "192.0.2.0/24",
                    " maxLength ":"24"
                },
                …
    ],
```

"withdrawn": [

{

"asn":" AS65200",

"prefix": "192.0.2.0/24",

"maxLength":"24"

},

…

]

}

- **Remove ROA** [Example of an API call: **/RemoveROA?ROAId=<ROAID>&Key=<api-key>**] Remove ROA from member account.

b. **API Security** - All APIs should have security measures that prevent persistent or undesirable access to them. This includes supporting automatic timeout and multi-factor authentication. The API should support different access privileges, such as:

- Admin -> Admin can perform all operations related to the management of ROAs and access privileges. These operations include Add or Remove ROA as well as Add or Remove users and set users permission. .
- Editor -> Editor can perform all operations related to ROA management. These operations include Add/Update or Remove ROA.
- Viewer -> Viewer only lists the ROAs or view the health metrics but cannot perform Add/Update or Remove ROA operations.

3. Infrastructure Health Metric

Infrastructure reliability is equally important for these registries to make sure that relying parties can download the ROAs and network operators can manage ROAs. The availability of RPKI repositories and being able to handle the expected load is very important. Additionally, ORSs need to provide the service health dashboard and notify users when service health is degraded. ORSs should also publish SLO data in the service dashboard. In specific, an ORS should do following actions:

a) **Service health Status** – ORS should provide service health status to include health of both control plane (ROA Management) and data plane (ROA updates to client).

b) **Service health degradation notification** – ORS should provide notification to registered subscribers in case of service health degradation.

Both of the above data can be provided through a health API request, e.g. **/GetServiceHealth** that can be polled periodically by the clients and acted upon whenever the reply signals an issue[2].

2 An example of such output is the Statuspage API (https://developer.statuspage.io/)

4. Safeguards for ROA changes

Change in a ROA can result in changes in the routing plane. Mistakenly created ROAs can result in network disruptions. ORSs should validate ROA changes against the current BGP announcements to make sure changes to a ROA would not result in undesirable behavior. Specifically, ORSs should perform following verification before ROA changes can be committed. The current suggestion is to issue a blocking warning with manual override option for the addition or deletion of a ROA that invalidates the status of the existing BGP announcements.

a) **Invalidation of subnets** – Changes to a ROA can impact more specific prefixes currently announced on the Internet (e.g., the change of a maximum length can make some subnets of the ROA prefix INVALID). ORSs must check if requested changes to ROAs may affect the validity of prefixes currently announced by the ASN on the Internet and issue a blocking warning.

b) **ASN migration verification** – ROA update propagation to all the filtering networks can take a few hours and depends on network polling for ROA updates. In the cases when a network operator desires to announce a prefix from a new ASN (presumably belonging to the same organization), if the network operator first changes the ROA (i.e. to withdraw the ROA with the old ASN and announce ROA with the new ASN), then the existing route can become INVALID or if the network operator changes the routing announcement first (i.e. start announcing the prefix from the new ASN), then the new route will be invalid. When a network operator wants to migrate the ASN on a given prefix, ORSs must check if the requested changes to the ROAs may affect the validity of prefixes currently announced by the ASN on the Internet and issue a blocking warning.

Acknowledgements

This document was developed by the MANRS CDN and Cloud task force. Special thanks to Somesh Chaturmohta, Brad Gorman, Carlos Marcelo Martinez, George Michaelson, Ali Monfared, Tom Harrison, Amreesh Phokeer, Andrei Robachevsky, Anees Shaikh, Nathalie Trenaman and Vamseedhar Raja for their hard work and contributions to this document.

Annex I. Compliance Status of the top-level ORSs (as of July 2021)

Registry	Index		ARIN	APNIC	LACNIC	AFRINIC	RIPE
ROA Certificate	1a	Auto Renewal of a ROA	NO	YES	YES	NO	YES
	1b	Standard Validity	825d	1yr	1yr	10yr	2yr
	1c	Alerting on expiration or renewal	YES	NO	YES	NO	NO
ROA Certificate	2a	API for ROA Management	YES	NO	NO	NO	YES
	2b	API Security	NO	NO	NO	NO	NO
nfrastructure Reliability	3a	Service health Status	YES	NO	NO	NO	NO
	3b	Service health degradation notification	YES	NO	NO	NO	NO
ROA Validation	4a	Invalid subnet validation	NO	NO	NO	NO	NO
	4b	ASN change validation	NO	NO	NO	NO	NO