Frequently Asked Questions

General

First, education - learn about RPKI and how it operates. We will provide a list of resources to help introduce the topic. You'll then be in a position to determine how you want to participate - creating ROAs (using the hosted or delegated model) and/or implementing validation.

There are two major components: creation of Route Origin Authorizations (ROAs) which are cryptographic objects that attest the validity of your BGP announcement. These ROAs are what other organizations will use to ensure that your prefixes are properly announced by the Autonomous System Numbers (ASNs) authorized to originate them. The second component is the collection and processing of the ROAs and the data they represent. As a network operator, you collect ROAs using validation software, and feed this processed information to your routers that can be used in routing policy logic.

Depending on which parts of the pilot you choose to participate in, it could range from very little to moderate. One thing we want to learn from this pilot is the operational commitment to running RPKI. Creation and managing ROAs requires very little effort. Validating ROAs requires a bit more effort. For validation, you'll need to install and run an RPKI validator to collect and process the ROAs, then deliver the processed data to your BGP routers.

Creating ROAs

The ROAs need to be made available to any organization that wants validate route origination. In the hosted model, the Regional Internet Registry (RIR, which for most I2 members will be ARIN) has the Certificate Authority and hardware infrastructure built to create, store, and distribute these ROAs. In the delegated model, you'll need to establish your own CA and distribution infrastructure.

If you select the hosted model, which we believe is most likely for most organizations, you will not need to purchase or dedicate any hardware or virtual machines for either the pilot or on going operation.

Creation of ROAs is outside both the control and data planes of your network. They are simply cryptographic artifacts that attest the validity of your BGP announcement. No changes are needed to your infrastructure to generate a ROA.

In order to validate the communication between you and ARIN, you will create a key pair that will be used to sign the ROA request. This key pair is not th e key pair that is used to sign the ROA itself, just the request for ARIN to sign the ROA. The public portion of this key pair is loaded into the Hardware Security Modules (HSMs) managed by ARIN and at that point, only the holder of the private portion of the pair can request that ROAs be created. The private key used to sign the ROA itself is stored HSMs operated by ARIN.

As more services move to the cloud, it is more and more common that important security functions are run by third party providers and partners. In this case, while it is true that ARIN's hosting infrastructure holds the private key used to sign your ROAs, the risk is low. The private key used to create your ROA is not held by ARIN. Specifically, no one, including ARIN, has access to this private key to generate ROAs. Only the holder of the private key you generated to communicate with ARIN will be able to request that ROAs be signed.

Worst case, you could make a ROA that doesn't cover your BGP announcement (eg, wrong autonomous system number) AND IF a network operator instituted a policy to reject invalid routes, then that operator would become unreachable.

There are a couple of different ways to check that your ROAs are distributed.

RIPE has a publicly accessible implementation of its Validator software: http://localcert.ripe.net:8088/

BGPMon offers a whois method of validation:

```
whois -h whois.bgpmon.net " --roa 4901 162.250.136.0/22"

0 - Valid

------------------------

ROA Details

------------------------

Origin ASN:      AS4901

Not valid Before: 2015-07-22 04:00:00

Not valid After:  2018-07-22 04:00:00  Expires in 1y268d21h28m55.6000000014901s

Trust Anchor:     rpki.arin.net

Prefixes:        162.250.136.0/22 (max length /24)
```

A browser plugin for Firefox and Chrome will display the ROA status for the site you are visiting:
http://rpki.realmv6.org/

Realmv6 has a publicly accessible RPKI Browser: http://rpki-browser.realmv6.org/

Yes. You can create ROAs for your prefix with the following caveat: if you are using provider-aggregatable address space (that is, address space provided by one of your upstreams, and not directly from ARIN), you'll need to discuss your plans with the organization that holds the address block. You'll still be able to create ROAs, and in fact, it is important to create ROAs for the more specific prefixes before aggregate prefix.

(if a campus gets addresses from a regional, what is the process with ARIN?)

ROA Validation

ROA creation and validation are two independent activities of RPKI. ROA creation is what you do to allow other operators to validate your announcements. Validation is when you collect other networks' ROAs to determine the validity of their announcements.

There are a number of open source validators available. We're not going to make any recommendations, rather, we hope that participants will use a variety and share their experiences.

RIPES's RPKI Validator

Dragon Research RPKI Toolkit
Yes, you'll still be able to collect and validate ROAs, even if the prefixes they cover are not present in your BGP feed.
Yes. Your validation activity and policy is independent of anything your upstream providers are doing.