RESOURCE PUBLIC KEY INFRASTRUCTURE

(RPKI)

ARIN Online users may now participate in RPKI: an opt-in service that allows users to certify their RSA/LRSA-covered Internet number resources to help secure Internet routing. Using cryptographically verifiable certificates, RPKI allows IP address holders to create public statements specifying which Autonomous Systems are authorized to originate their IP address prefixes.

These statements, known as Route Origin Authorizations (ROAs), allow network operators to make informed routing decisions, and help secure Internet routing in general. This has been an initiative that has been developed within the IETF's SIDR Working Group, with involvement from Regional Internet Registries (RIRs), Local Internet Registries (LIRs), and numerous Internet Service Providers (ISPs).

WHY USE RPKI?

Internet routing is dependent upon many chains of network relationships that are based on mutual trust. Each party trusts that the route used to transmit information is safe, accurate, and will not be maliciously altered. This model proved sufficient in the early stages of Internet development, but has become increasingly vulnerable to abuse and attack as the Internet's resources have undergone a massive increase in usage.

As IPv4 address space depletes, an urgent need exists to strengthen routing security. Using cryptographically verifiable statements, RPKI helps to ensure that Internet number resource holders are certifiably linked to those resources, and reliable routing origin data is available upon which to base routing decisions.

RPKI can help fill these requirements through the generation of:

- Resource certificates, which digitally verify that a resource has been allocated or assigned to a specific entity
- Route Origin Authorizations (ROAs): digital statements specifying which Autonomous System may originate a specific IP address or range

ARIN encourages members of the Internet community to certify their resources through RPKI. Internet routing today is vulnerable to hijacking and the provisioning/use of certificates is one of steps required to make routing more secure. Widespread RPKI adoption will help simplify IP address holder verification and routing decision-making throughout the ARIN region.

RPKI AT THE OTHER RIRs

More information about RPKI at other RIRs is available at the following URLs:

AFRINIC
http://afrinic.net/en/initiatives/rpki-certification

APNIC
http://www.apnic.net/services/services-apnic-provides/resource-certification

LACNIC
https://rpki.lacnic.net/rpki/

RIPE NCC
http://www.ripe.net/certification/

Hosted RPKI

Hosted RPKI is an infrastructure in which ARIN hosts a Certificate Authority (CA) and signs all ROAs for resources within the ARIN region via ARIN Online. Only direct resource holders can participate in RPKI. Any downstream organization must have their upstream provider submit ROA Requests on their behalf.

Delegated RPKI

Delegated RPKI refers to an infrastructure in which ARIN allows direct resource holders to host their own CA and sign ROAs on their own systems. Resources then are linked to ARIN's RPKI repository by selecting the "delegated" option when setting up RPKI. This hierarchical system of verification allows customers of direct Internet number resource holders to participate in RPKI, using their own provider as a CA.

WWW.ARIN.NET

ARIN
American Registry for Internet Numbers

What is a **Resource?**

In the context of RPKI, a **resource** is a grouping of Internet Protocol (IP) addresses or Autonomous Systems Numbers (ASNs) that uniquely identify a computer or a network on the Internet. Routers use these numbers much like the Post Office uses addresses to help route mail to recipients.

What is a **Resource Certificate?**

A **resource certificate** is an electronic file that serves as proof that a resource has been assigned to an individual or company for their use. These certificates list a collection of Internet number resources (IPv4 and IPv6 addresses, as well as ASNs) that are associated with a holder of those resources. Resource certificates provide a means of third-party validation of assertions related to resource allocations using proven cryptographic algorithms. These certificates contain no identifying information about who the holder of the resources is; resource holders can prove their legitimacy using their private key to sign information such as a Route Origination (ROA) Request. Relying Parties can then validate these signed objects with the corresponding public key.

What is a **Key Pair?**

The term ***key pair*** refers to the two separate pieces of data (a public key and a private key) created using public-key cryptography, a system used to secure data.

In Hosted RPKI, participants generate and use Route Origin Authorization (ROA) Request Generation Key Pairs to secure Route Origin Authorization (ROA) and resource certificate data and cryptographically verify their identity. Hosted RPKI users must create a ROA Request Generation Key Pair before requesting resource certificates or generating ROA Requests. **In Delegated RPKI**, participants generate and use Delegated RPKI Key Pairs to request, sign, and publish an RFC 3779 resource certificate from ARIN. The private key of this key pair is then used to sign information in the participant's RPKI repository.

What is a **Public Key?**

The **public key** is the part of the key pair that may be distributed safely to others. It is mathematically paired with the private key that was generated alongside it. This key is provided to ARIN when the user signs up to participate in RPKI, and is used to cryptographically verify Route Origin Authorization (ROA) Request which have been signed by the corresponding private key.

What is a **Private Key?**

The **private key** is the part of the key pair that **must** be securely stored, and may NOT be distributed. RPKI participants use private keys to sign Route Authorization (ROA) Requests. When a block of data is signed using a resource holder's private key, their public key can be used to verify that data.

Note: Private keys MUST be kept private, and must not be shared with anyone outside your organization. Should another entity have access to your private key, that entity would be able to effectively represent itself as your organization, voiding the security RPKI is designed to maintain.

If your private key is lost or compromised, you must start the resource certification process again from scratch.

How to Participate in RPKI

- Log into ARIN Online and select ***MANAGE RESOURCES*** on the left-hand side
- Choose the organization you wish to manage RPKI for
- Select Hosted or Delegated RPKI
- Select ***MANAGE RPKI*** on the right-hand side
  - *If you do not see this link, please ensure you meet the requirements for participation.*
- Select "***create resource certificate***" on the right-hand side
- Read and agree to the RPKI Terms of Service
- Generate a key pair
- Enter your public key (and Base Certificate Authority (CA) Repository URI if you are a Delegated RPKI participant) into the field(s) provided
- Click ***Submit***
  - *This will generate a ticketed request for ARIN to generate a resource certificate covering your Internet number resources*

Within the MANAGE RPKI section of ARIN Online, you may request and manage resource certificates and ROAs, as well as view which resources are currently covered.

ROA Data

Note: Before submitting ROA Requests, you must sign up for RPKI and submit your public key. ROA Requests may be submitted on behalf of your organization once ARIN has approved your resource certificate.

ROAs generated and signed by ARIN are published in ARIN's RPKI repository, and may be downloaded and validated (using publicly available tools) by network operators looking for statements to base their routing decisions upon. ROA data is secured by performing all cryptographic functions in a trusted environment on a Hardware Security Module (HSM) designed specifically for this type of encryption.

RELYING PARTIES WISHING TO UTILIZE RPKI DATA TO MAKE ROUTING DECISIONS

Any entity may become an RPKI relying party, which will allow them to retrieve data from ARIN's RPKI database.

ARIN's Trust Anchor Locator (TAL)

In RPKI, a validator is used to fetch repositories that can be located via a TAL. ARIN's TAL contains both the location of ARIN's repository and ARIN's public key, which is used to cryptographically verify that ARIN has signed the artifacts within ARIN's repository.

The validator can then verify the certificates and ROAs within the repository.

In order to access ARIN's TAL:

- Go to https://www.arin.net/rpki/tal/index.html
- Accept the ARIN Relying Party Agreement
- Select Continue
- Provide an email address to which ARIN will send the TAL
- Select Continue
  - *ARIN's TAL will then be emailed to the email address you provided.*

If you are logged into ARIN Online:

- Select DOWNLOADS on the left-hand side
- Select "ARIN Trust Anchor Locator" from the list of downloads
- Accept the ARIN Relying Party Agreement
- Select Continue
  - *ARIN's TAL will then be emailed to the email address you provided.*

ARIN Customers Wishing to Participate in RPKI:

In order to participate in RPKI, **you will need:**