ARIN
American Registry for Internet Numbers

RPKI 101

How to protect your resources and enhance your routing security using ARIN's Resource Public Key Infrastructure (RPKI) services

What is RPKI?

RPKI provides a cryptographically signed method for Internet number resource holders to make authoritative statements about the origin of a prefix; this is done by entering the prefix in a Route Origin Authorization (ROA). RPKI data gives network operators another dataset to make more informed routing decisions, also known as Route Origin Validation. Ultimately, RPKI helps protect resource holders from human error or nefarious activity, thereby reducing the overall impact of attempted hijacks on the greater Internet.

How does RPKI work?

1. **Legitimate resource holders obtain a resource certificate from ARIN.**
2. **That certificate allows resource holders to make cryptographically signed statements about the origin Autonomous System Number (ASN) of a prefix.**
3. **Data is fetched from ARIN that confirms the resources are valid.**
4. **Network operators act based on this validation, enhancing routing security on a global scale.**

How can my organization get started with RPKI?

To certify your resources with ARIN, you'll need:

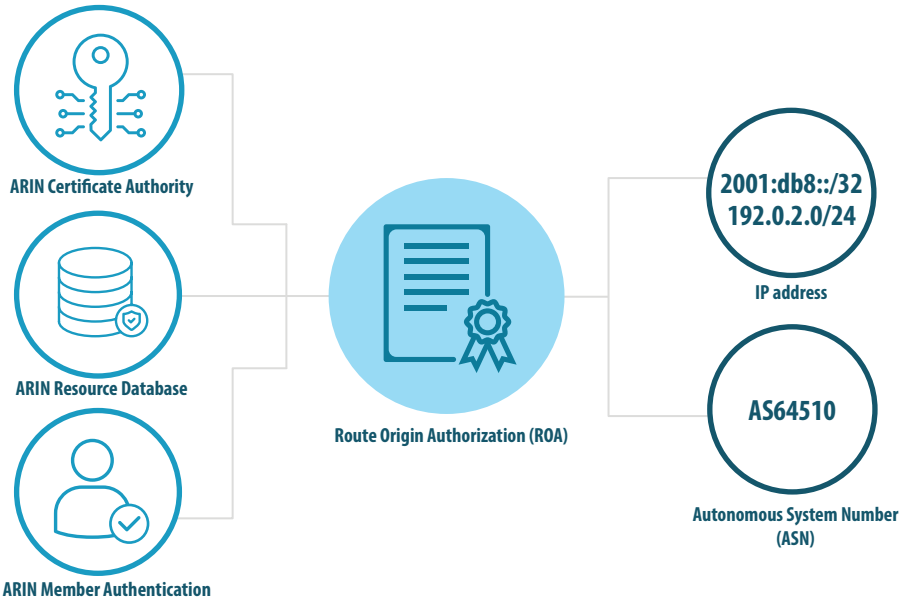
- IPv4 and/or IPv6 resources issued to you directly from ARIN;
- An Autonomous System Number (ASN) from ARIN or another Regional Internet Registry;
- A signed Registration Services Agreement (or Legacy Registration Services Agreement) covering the resources you want to certify; and
- An ARIN Online account linked to an Admin, Tech, or Routing Point of Contact with authority to manage those resources.

Ready to get started? Scan the QR code or visit **arin.net/rpki**

Why should my organization adopt RPKI?

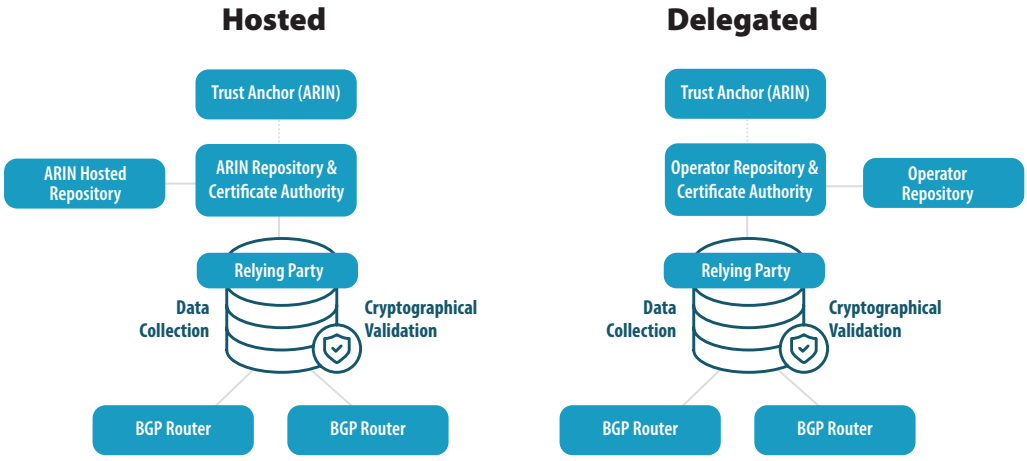
Adopting RPKI helps establish a more trusted and collaborative environment among Internet number resource holders and network operators connected to the Internet. By adopting RPKI, companies can rely on verifiable information about IP address and route legitimacy, which can help resolve routing issues and combat network attacks. This leads to a more reliable and secure Internet infrastructure for everyone.

- **Creating ROAs for your resources benefits more than just you:** Operators make decisions based on Route Origin Validation, leading to a more reliable and secure Internet infrastructure.
- **RPKI has been proven to interrupt hijacking attempts** before they impact the operation of the global Internet.
- **A growing number of Internet service providers require you to create ROAs for your resources** before a business relationship is established. Becoming familiar with how RPKI works can help you be prepared for future requests.
- The **Internet Engineering Task Force continually defines new features and use cases for RPKI**, which helps increase its effectiveness to benefit all Internet users.



What RPKI services does ARIN offer?

ARIN offers services supporting two models of RPKI deployment: Hosted and Delegated. With Hosted RPKI, ARIN hosts a Certificate Authority and signs all Route Origin Authorizations (ROAs) for resources allocated within the ARIN region. With Delegated RPKI, ARIN will produce a delegated resource certificate at your request that can be used in your own Certificate Authority to sign your ROAs. You can maintain your own repository and publication server, or you can choose to use ARIN's Repository and Publication Service. In both models, ARIN serves as the trust anchor certifying that the rightful resource holder is the one who created the ROA.



Which one is right for my organization?

If your organization is just getting started with RPKI, you may want to choose the Hosted option; it is the easiest to use since the only thing you need to do is create ROAs to cover your resources. In fact, **nearly 98 percent of ARIN RPKI deployments use the Hosted service**. The Delegated RPKI option is a good choice for an organization that wants to maintain cryptographic control and independence, but you should have in-depth knowledge about RPKI and the resources — both human and technological — to run a Certificate Authority and publication server.