NRO
Number Resource Organization
10 Years

What is Resource Certification (RPKI)?

Resource Certification, also referred to as Resource Public Key Infrastructure (RPKI), is an opt-in service offered by each Regional Internet Registry (RIR) that provides digital "resource certificates" for Internet number resources. These certificates are cryptographically verifiable attestations that a given set of IPv4 addresses, IPv6 addresses, or Autonomous System (AS) numbers have been assigned or allocated to an organization. The certificates follow the X.509 Public Key Infrastructure model, as documented by RFC5280 and related standards in the Internet Engineering Task Force (IETF).

Attestations are verified by evaluation of the whole signature and resource chain, without the need for storing identity information in the certificates themselves.

The standards used in Resource Certification are open and have been developed within the Internet Engineering Task Force (IETF) SIDR Working Group and among the various RIRs.

Why use RPKI?

The current Internet functions as a series of network relationships based upon mutual trust. Each party trusts that the route used to transmit information is safe, accurate, and will not be maliciously altered. This model has become increasingly open to abuse and attack as the Internet has grown larger and more diverse, making trust relationships harder to establish. Given the increasing incidents of IP address hijacking, stronger routing security is needed. A cryptographically secure model is required to help prevent a malicious entity or routing event from causing widespread security issues.

When routing information on the Internet is transferred between two parties, RPKI-backed technology can be used to authenticate transactions, because the recipient can be sure the resources have been legitimately allocated or assigned by an RIR when performing cryptographic validation.

How does RPKI help secure routing?

The Internet is made up of interconnected networks. Each network is identified by a unique Autonomous System (AS) number, which is used for routing decisions as packets move from their start to the end point. These AS numbers constitute a high-level view of the "path" a packet takes from the sender to the recipient.

Once a certificate is created using RPKI, the holder can use it to create a digital document stating that, as the holder of a given range of IP addresses, they allow those addresses to be initially routed from a specific AS. This digital document gives network operators certainty that the traffic source is legitimate and verifiable. Additional systems being designed by the IETF are intended to protect the path from the start to the end of the AS transitions in the network and use the same certified information as part of their protection.

AFRINIC The Internet Numbers Registry for Africa
www.afrinic.net

APNIC
www.apnic.net

ARIN American Registry for Internet Numbers
www.arin.net

lacnic
www.lacnic.net

RIPE NCC
www.ripe.net

Learn more about RPKI at each RIR:

AFRINIC:
www.afrinic.net/en/initiatives/resource-certification

APNIC:
www.apnic.net/rescert

ARIN:
www.arin.net/resources/rpki.html

LACNIC:
www.lacnic.net/en/web/lacnic/certificacion-de-recursos-rpki

RIPE NCC:
www.ripe.net/certification