SIDROPS
Internet-Draft
Intended status: Best Current Practice
Expires: 4 September 2025

Z. Yan
CNNIC
T. Bruijnzeels
RIPE NCC
T. Harrison
APNIC

3 March 2025

RPKI Terminology
draft-yan-sidrops-rpki-terminology-01

Abstract

The Resource Public Key Infrastructure (RPKI) is defined in dozens of different RFCs. The terminology used by implementers and developers of RPKI protocols, and by operators of RPKI systems, can at times beinconsistent, leading to confusion. In an effort to improve consistency in this respect, this document provides a single location for definitions of commonly-used RPKI terms.

Table of Contents

1. Introduction

The Resource Public Key Infrastructure (RPKI) is defined in dozens of different RFCs. The terminology used by implementers and developers of RPKI protocols, and by operators of RPKI systems, can at times be inconsistent or imprecise, leading to confusion.

An example of this sort of problem arises in the context of RPKI implementation models. The model where an address holder runs their own CA software deployment that communicates with the relevant registry is often referred to as "delegated RPKI", but at least some Regional Internet Registries (RIRs) instead use the term "self-hosted RPKI".

In an effort to improve consistency and precision in this respect, this document provides a single location for definitions of commonly-used RPKI terms.

2. Basic

Internet Number Resources (INRs): Autonomous System (AS) numbers, IPv4 addresses, and IPv6 addresses.

Regional Internet Registry (RIR): An INR registry recognized by IANA as a regional authority for INR management. At the time of writing, these are AfriNIC, APNIC, ARIN, LACNIC, and RIPE NCC. See [RFC7020] for more details.

National Internet Registry (NIR): An INR registry that is primarily concerned with the delegation of resources within a specific economy, as opposed to the larger geographical regions covered by an RIR.

Internet Service Provider (ISP): An organization that provides internet services to other organizations. An ISP will typically have an IP address or AS number delegation from an RIR or an NIR.

Local Internet Registry (LIR): A term used in some regions as a synonym for ISP.

Origin ASN: The AS number of the originating BGP speaker for a BGP announcement.

Certification Authority (CA): Certification Authorities in the RPKI are entities that a receive an RPKI CA certififcate from an issuer. RPKI CA certificates bind a public key to INRs. CAs can use the corresponding private keys to sign verifiable statements pertaining to those INRs, such as CA certificates issued to a subordinate CA with INRs that are a subset of the INRs held by the CA, or ROAs, etc.

Repository: The repository is the component responsible for storing and distributing RPKI-signed objects, such as Route Origin Authorizations (ROAs), Certificates, Certificate Revocation Lists (CRLs), and Manifest files. It acts as a centralized or distributed database that enables RPKI validators (relying parties) to fetch and validate routing security data. The key functions include storing RPKI objects issued by CAs, using protocols like RRDP (RPKI Repository Delta Protocol) [RFC8182] or rsync to synchronize data with RPKI validators, and ensuring validators globally access the same authoritative data.

Relying Party (RP): A Relying Party (RP) is an entity that utilizes validated RPKI data to enhance the security of Border Gateway Protocol (BGP) routing decisions. Key responsibilities include the retrieval of RPKI objects (CA certificates, signed objects, CRLs, and manifests) from RPKI repositories using protocols like rsync or RRDP. It will validate the certificate chain of trust from end-entity certificates up to trusted root CA certificates, and also ensure that additional signed object validation is performed as expected. RPs will typically generate validation results that users can review, and will often also operate as an RPKI-Router [RFC8210] server.

Address space holder: An entity that has been delegated INRs by an RIR or other authorized body.

3. Signed Objects

RPKI signed object: A cryptographically-secured data structure that has been signed by an RPKI End-Entity (EE) resource certificate. See [RFC6488] for more details.

Route Origination Authorization (ROA): A type of RPKI signed object that can be issued by an IP address holder in order to authorize an AS to originate routes to one or more of the holder’s prefixes. See [RFC6482] for more details.

Manifest: A type of RPKI signed object that provides a complete list of all the signed objects that an authority has published to a given repository publication point. The manifest includes the hashes of each file as well. The list of files and hashes helps RPs to detect unauthorized changes or deletions. See [RFC6486] for more details.

Ghostbusters record: A type of RPKI signed object for providing contact details for a given RPKI repository publication point. See [RFC6493] for more details.

Autonomous System Provider Authorization (ASPA): A type of RPKI signed object that can be issued by an AS holder as a statement about the ASes that operate as providers (upstreams) for the holder’s AS. See [I-D.ietf-sidrops-aspa-verification] for more details.

Trust Anchor (TA) Key: A type of RPKI signed object that can be issued by a TA key holder as a statement about the current public key for the TA, as well as the successor public key for the TA, in order to facilitate the transition of RPs to that successor key. See [RFC9691] for more details.

RPKI Signed Checklist (RSC): A type of RPKI signed object that can be issued by an INR holder over an arbitrary set of files. See [RFC9323] for more details.

4. RPKI Repository

Hosted model: An operating model where the issuing registry (typically an RIR) manages the RPKI objects and associated repository on behalf of the resource holder. Resource holders use an interface provided by the registry to create and manage their RPKI objects, which are then hosted by the registry. This is sometimes referred to in a registry-specific sense, e.g. "APNIC-hosted RPKI".

Delegated model: An operating model where the address holder runs an independent RPKI CA instance as a child CA of the issuing registry's parent CA. The address holder's CA typically relies on the provisioning protocol [RFC6492] in order to communicate with the registry's CA. This is sometimes referred to as "self-hosted RPKI".

Repository Publication Point: A directory containing the objects published by an RPKI CA: CA certificates, signed objects, CRLs, and manifests. Relying Parties (RPs) can access this content by way of an rsync URI, though there may be other mechanisms available as well: see e.g. [RFC8182]. See [RFC6481] for more details.

Repository Instance: A host comprising one or more repository publication points.

Repository Object (or Object): A terminal object in a repository publication point.

Repository Directory: Synonymous with Repository Publication Point.

5. CA and Publication Repository Communication

Provisioning Protocol: A protocol used by RPKI CAs to manage certificates issued by their parent CAs.

Publication Protocol: A protocol used by RPKI CAs to send their RPKI objects to a server, with that server then handling the distribution of those objects to RPs via rsync and other protocols.

Business PKI (BPKI): A PKI used in the RPKI out-of-band (OOB) protocol in order to establish and secure subsequent interactions via the provisioning protocol and the publication protocol [RFC8183].

Publication engine/publication server: The server providing the the publication protocol service.

Publisher: An entity acting as a client of a publication server.

6. RPKI Repository and the Relying Party Communication

rsync: rsync is a file synchronization and transfer tool designed to minimize data transfer time and bandwidth usage by copying only the differences between source and destination files. It allows relying parties to synchronize a local copy of the RPKI repository used for validation with the corresponding remote repositories.

RPKI Repository Delta Protocol (RRDP): Data synchronization protocol between repositories and the relying parties ([RFC8182]). It aims to replace rsync in the RPKI context, providing a more reliable, scalable, and HTTPS-based incremental data synchronization mechanism, and ensuring that RPKI validators can quickly obtain the latest RPKI data.

Update Notification File: A type of file in RRDP that acts as a directory pointing to the latest snapshot and delta files. This file allows relying parties to discover any changes between the repository state and the relying party's cache.

Snapshot File: A type of file in RRDP that provides a complete copy of all RPKI objects (certificates. signed objects, manifests, and CRLs) in a repository at a specific moment.

Delta File: A type of file in RRDP that contains incremental changes (additions, modifications, deletions) to the relevant repository's RPKI data.

Same-Origin Policy (SOP): The Same-Origin Policy is a web security mechanism that restricts how resources from one origin (domain, protocol, and port) can interact with resources from another origin. Used in RRDP to reduce problems associated with inadvertent or malicious repository data. See [RFC9674] for details.

7. RPKI and Router Protocol Communication

RPKI-Router Protocol: A protocol designed to securely distribute validated routing information from RPKI validators to BGP routers. It enables routers to enforce Route Origin Validation (ROV) by dynamically receiving and applying authorized prefix-to-AS mappings.

Protocol Data Unit (PDU): A discrete protocol message in the RPKI-Router protocol.

Payload PDU: An RPKI-Router PDU that contains data for use by the router (e.g. the IPv4 Prefix PDU), as opposed to the PDUs for the control mechanisms of the protocol (e.g. the End of Data PDU).

8. Route Origin Validation

Route Origin Validation (ROV): A security mechanism designed to prevent route hijacking and misorigination in BGP by verifying whether a given AS is authorized to announce specific IP address prefixes. Also known as Prefix Origin Validation.

Validated ROA Payload (VRP): A data structure containing an origin ASN, a prefix, and the max-length for the prefix, derived from a validated ROA. VRPs are typically produced by RPs as the the base output format for ROA data.

Route Origin ASN: The origin AS number derived from a BGP route as follows (See [RFC6811] for details.):

* the rightmost AS in the final segment of the AS_PATH attribute in the route if that segment is of type AS_SEQUENCE; or

* the BGP speaker’s own AS number if that segment is of type AS_CONFED_SEQUENCE or AS_CONFED_SET or if the AS_PATH is empty; or

* the distinguished value "NONE" if the final segment of the AS_PATH attribute is of any other type.

Covered: An IP address prefix ’covers’ another prefix if the second prefix is a non-strict subset of the first prefix.

Validation states: There are three validation states in ROV: Valid, Invalid, and Unknown (or Not Found). See [RFC6483] for details.

9. Acknowledgment

TBA.

10. References

10.1. Normative References

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/info/rfc6480>.

[RFC6481] Huston, G., Loomans, R., and G. Michaelson, "A Profile for Resource Certificate Repository Structure", RFC 6481, DOI 10.17487/RFC6481, February 2012, <https://www.rfc-editor.org/info/rfc6481>.

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, DOI 10.17487/RFC6482, February 2012, <https://www.rfc-editor.org/info/rfc6482>.

[RFC6483] Huston, G. and G. Michaelson, "Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)", RFC 6483, DOI 10.17487/RFC6483, February 2012, <https://www.rfc-editor.org/info/rfc6483>.

[RFC6486] Austein, R., Huston, G., Kent, S., and M. Lepinski, "Manifests for the Resource Public Key Infrastructure (RPKI)", RFC 6486, DOI 10.17487/RFC6486, February 2012, <https://www.rfc-editor.org/info/rfc6486>.

[RFC6488] Lepinski, M., Chi, A., and S. Kent, "Signed Object Template for the Resource Public Key Infrastructure (RPKI)", RFC 6488, DOI 10.17487/RFC6488, February 2012, <https://www.rfc-editor.org/info/rfc6488>.

[RFC6492] Huston, G., Loomans, R., Ellacott, B., and R. Austein, "A Protocol for Provisioning Resource Certificates", RFC 6492, DOI 10.17487/RFC6492, February 2012, <https://www.rfc-editor.org/info/rfc6492>.

[RFC6493] Bush, R., "The Resource Public Key Infrastructure (RPKI) Ghostbusters Record", RFC 6493, DOI 10.17487/RFC6493, February 2012, <https://www.rfc-editor.org/info/rfc6493>.

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2013, <https://www.rfc-editor.org/info/rfc6811>.

[RFC7020] Housley, R., Curran, J., Huston, G., and D. Conrad, "The Internet Numbers Registry System", RFC 7020, DOI 10.17487/RFC7020, August 2013, <https://www.rfc-editor.org/info/rfc7020>.

[RFC8182] Bruijnzeels, T., Muravskiy, O., Weber, B., and R. Austein, "The RPKI Repository Delta Protocol (RRDP)", RFC 8182, DOI 10.17487/RFC8182, July 2017, <https://www.rfc-editor.org/info/rfc8182>.

[RFC8183] Austein, R., "An Out-of-Band Setup Protocol for Resource Public Key Infrastructure (RPKI) Production Services", RFC 8183, DOI 10.17487/RFC8183, July 2017, <https://www.rfc-editor.org/info/rfc8183>.

[RFC8210] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1", RFC 8210, DOI 10.17487/RFC8210, September 2017, <https://www.rfc-editor.org/info/rfc8210>.

[RFC9323] Snijders, J., Harrison, T., and B. Maddison, "A Profile for RPKI Signed Checklists (RSCs)", RFC 9323, DOI 10.17487/RFC9323, November 2022, <https://www.rfc-editor.org/info/rfc9323>.

[RFC9674] Snijders, J., "Same-Origin Policy for the RPKI Repository Delta Protocol (RRDP)", RFC 9674, DOI 10.17487/RFC9674, December 2024, <https://www.rfc-editor.org/info/rfc9674>.

[RFC9691] Martinez, C., Michaelson, G., Harrison, T., Bruijnzeels, T., and R. Austein, "A Profile for Resource Public Key Infrastructure (RPKI) Trust Anchor Keys (TAKs)", RFC 9691, DOI 10.17487/RFC9691, December 2024, <https://www.rfc-editor.org/info/rfc9691>.

10.2. Informative References

[I-D.ietf-sidrops-aspa-verification] Azimov, A., Bogomazov, E., Bush, R., Patel, K., Snijders, J., and K. Sriram, "BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-verification-20, 4 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-20>.

Authors' Addresses

Zhiwei Yan
CNNIC
Email: yanzhiwei@cnnic.cn

Tim Bruijnzeels
RIPE NCC
Email: tim@ripe.net

Tom Harrison
APNIC
Email: tomh@apnic.net