Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: 1 November 2026

Z.W. Yan
CNNIC
T. Bruijnzeels
RIPE NCC
T. Harrison
APNIC
S. Silva Berenguer
NRO

30 April 2026

RPKI Terminology
draft-yan-sidrops-rpki-terminology-04

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 be inconsistent, 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.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 1 November 2026.

Copyright Notice

Table of Contents

1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. 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.

3. 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.

Certification Authority (CA): Certification Authorities in the RPKI are entities that receive an RPKI CA certificate 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 Origination 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, CRLs, manifests and other signed objects) 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. RP can sometimes be referred to as an "RPKI validator" and different definitions can be referenced interchangeably.

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

Resource Allocation: Resource allocation refers to the authoritative process of assigning Internet number resources to entities through a hierarchical trust framework, including sub allocation processes. This process establishes cryptographic binding between resources and their legitimate holders, enabling secure route validation.

Resource Revocation: Resource revocation refers to the process of invalidating compromised or deauthorized INRs or their associated digital certificates. This ensures unauthorized entities cannot misuse revoked resources for BGP route manipulation. In RPKI, resource delegation revocation involves cascading revocation of all sub certificates/objects.

4. Typical Routing Security Issues

Route leak: A route leak is defined in RFC 7908 as the propagation of routing announcement(s) beyond their intended scope. That is, an Autonomous System (AS) disseminates a learned BGP route to another AS in violation of the intended policies of one or more parties along the AS path. Route leaks may be caused by intentional manipulation or by human errors or misconfigurations. When misused, they can result in traffic attraction or diversion through an unintended path, potentially enabling eavesdropping or traffic analysis, and may result in an overload or black hole. The IETF RFC 7908 [RFC7908] categorizes route leaks into six types based on observed incidents on the Internet.

Prefix hijacking: A prefix hijack occurs when a network, whether intentionally or mistakenly, originates a prefix that belongs to another network without its permission. The attacker announces a BGP route for an IP prefix that they do not legitimately own, typically with the goal of attracting traffic destined for that prefix. The impact can range from a minor anomaly to a complete takeover of the victim ‘s traffic. Route Origin Validation (ROV) using ROAs is the primary RPKI-based defense mechanism against prefix hijacking. By cryptographically verifying that an AS is authorized to originate a particular prefix, RPKI can detect and filter invalid prefix announcements before they propagate.

Subprefix hijack: A subprefix hijack is a specific type of prefix hijacking where an AS announces a more specific prefix belonging to a victim’s larger prefix block. For example, if a victim legitimately owns 72.252.8.0/21, an attacker might announce 72.252.8.0/24. Due to longest-prefix-match routing, routers will prefer the more specific route, causing all traffic destined for addresses within that subprefix to be redirected to the attacker——regardless of whether the attacker has legitimate ownership of that subprefix.

BGP path manipulation: The act of altering BGP path attributes to influence the path selection process of other ASes. Adversaries may manipulate these attributes to force traffic to take a specific path, enabling traffic interception, prioritization of malicious traffic, or avoidance of RPKI validation checks. Path manipulation can undermine the effectiveness of ROV by redirecting traffic to RPKI-valid but unauthorized paths.

5. Signature Objects and Associated Trust Data

RPKI signed object: A cryptographically-secured data structure that has been signed by an RPKI End-Entity (EE) resource certificate. Currently, RPKI signed objects include six categories: Route Origination Authorization, Manifest, Ghostbusters, Autonomous System Provider Authorization, Trust Anchor Key, Signed Checklist. 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 [RFC9582] for more details. A ROA includes an authorised origin AS and a set of IP prefixes, each of them with an optional max length, which represents the maximum length of the IP prefix that the origin AS is authorised to advertise.

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. ASPA is used for route leakage protection. See [I-D.ietf-sidrops-aspa-profile] and [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.

Resource Certificate: Resource certificates are X.509 certificates that bind the holdership or "right-of-use" assertions of Internet Number Resources (INR) (i.e., IP Addresses and Autonomous System (AS) numbers) to a public key in the RPKI hierarchy. Allowing the entity that holds the corresponding private key to sign attestations pertaining to a non-strict subset of the INRs contained on the Resource Certificate. The CA and EE certificates, as well as the BGPsec router certificates in the RPKI system, are referred to as resource certificates and are profiled in [RFC6487] and [RFC8209].

End-Entity (EE) Certificate: EE Certificates are certificates for which the private key cannot be used to sign subordinate certificates. There are two types of EE certificates used by the RPKI: Embedded EE Certificates and BGPsec Router Certificates.

Embedded EE Certificate: Embedded EE Certificiates are issued by resource holder CAs to delegate the authority attested by their allocation certificates [RFC6480]. RPKI Signed Objects [RFC6488], such as ROAs and Manifests, use an embedded EE certificate. When issuing an RPKI signed object, the private key of the EE certificate is used to sign its content. A strict one-to-one exclusive mapping exists between the EE certificate and the signed object. This non reusable setting can reduce the attack surface.

BGPsec Router Certificates: The BGPsec router certificate in RPKI is an X.509 end entity (EE) certificate, which is used for authenticating the AS path in the BGPsec protocol, indicating that the router or routers holding the corresponding private key have the authority to send secure route announcements (BGPsec UPDATEs) on behalf of the AS specified in the certificate.The BGPsec router certificate is stored in the repository of the issuing CA. Compared to other parts of RPKI, BGPsec uses different algorithms, key formats, and signature formats, BGPsec RP needs to support the algorithms used to validate BGPsec signatures in [RFC8608], as well as the algorithms in [RFC7935] for validating signatures on BGPsec certificates, RPKI CA certificates, and RPKI CRLs.

Trust Anchor (TA): A self-signed X.509 certificate representing the apex of trust in the RPKI hierarchy. It attests holdership of Internet number resources and delegates authority to subordinate CAs. TA is the ultimate arbiter of the RPKI trust chain, and RPs must configure trust anchors to initialize RPKI validation.

Trust Anchor Locator (TAL): A TAL is used by relying parties (RPs) to retrieve and validate a trust anchor (TA) certification authority certificate used in RPKI validation, with its data format containing the TA URI and the public key corresponding to the referenced object. During validation, the RP fetches the TA via the URI and verifies the matching of the public key. It provides a secure bootstrap mechanism for the RPKI trust hierarchy without requiring pre-distribution of TA certificates. See [RFC8630] for more details.

Certificate Revocation List (CRL): A digitally signed list issued by a certificate authority (CA) in the RPKI system, enumerating the serial numbers of resource certificates that have been revoked before their scheduled expiration date. CRLs provide a real-time mechanism to invalidate compromised or erroneous certificates within the RPKI trust hierarchy. RPs can verify the revocation status of certificates during RPKI verification using CRL.

Chain of Trust: Resource Certificates in the RPKI are validated by way of an hierarchical chain of trust. At the top level a Trust Anchor (TA) certificates is used for which trust is assumed by a

Relying Party through a configured TAL. The private key of the TA certificate can be used to sign subordinate CA certificates that associate a public key with a non-strict subset of the INRs found in the TA. Trust in this association is derived by RPs through the assumed trust in the TA and the verification of signatures. The private keys of CA certificates can be used to sign further subordinate CA certificates. This resulting in an RPKI tree of TA and CA certificates.

6. RPKI Repository

Repository Publication Point: RPKI TA and CA certificates contain Subject Information Access fields with rsync and RRDP related URIs that can be used by RPs to retrieve files signed by the private key pertaining to this certificate. The 'id-ad-caRepository' entry is the Repository Publication Point for the certficate. It refers to an rsync directory that contains the current certificates issued under this CA certificate, the most recent CRL, the current manifest, and all other current signed objects that can be verified using an EE certificate issued under this CA certifcate. See [RFC6481] and [RFC8182] 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.

RPKI Repository Name Scheme: The RPKI Repository Name Scheme defines the filename extensions format for RPKI repository objects. Specifically, it includes:

Filename extension	RPKI Object	Reference
.asa	Autonomous System Provider Authorization	[I-D.ietf-sidrops-aspa-profile]
.cer	Certificate	[RFC6481]
.crl	Certificate Revocation List	[RFC6481]
.gbr	Ghostbusters Record	[RFC6493]
.mft	Manifest	[RFC6481]
.roa	Route Origination Authorization	[RFC9582]
.sig	Signed Checklist	[RFC9323]
.tak	Trust Anchor Key	[RFC9691]

Table 1

7. RPKI CA Deployment Models

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".

Hybrid model: An operating model where the address holder runs an independent RPKI CA instance as a child of the issuing registry's parent CA (like in the Delegated model) and uses the publication service provided by the issuing registry, who will take care of the 24/7 availability of the repository. Currently, some RIRs and NIRs offer the hybrid model.

8. Inter-CA and Publication Server communication

Parent CA: An entity that operates a CA that issues one or more CA subordintate certifates to child CAs.

Child CA: An entity that operates a CA that received on or more CA certificates from a parent. Note that an entity can be a child to its parent, but also be a parent to its own child CAs.

Provisioning Protocol: A protocol used by RPKI CAs to manage certificates issued by their parent CAs. See [RFC6492] for more details.

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. See [RFC8181] for more details.

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 publication protocol service.

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

9. 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, CRLs, manifests and other signed objects) 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.

10. Communication between RPKI and Routers

RPKI-Router Protocol (RTR): 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. See [RFC8210] and [I-D.ietf-sidrops-8210bis] for details.

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).

11. Using of signed objects

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 [RFC6907] 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.

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

ASPA validation states: When using ASPA to validate the Border Gateway Protocol (BGP) AS_PATH attribute of advertised routes, ASPA defines distinct verification algorithms and procedures for scenarios such as upstream paths and downstream paths, and establishes three possible validation outcomes.

* Valid: The AS_PATH fully complies with ASPA authorization rules.
* Invalid: The AS_PATH violates at least one ASPA authorization constraint.
* Unknown: Inconclusive result due to missing ASPA data in RPKI repositories.

12. Acknowledgments

To be determined.

13. References

13.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

13.2. Informative References

[I-D.ietf-sidrops-8210bis] Bush, R., Austein, R., and T. Harrison, "The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 2", Work in Progress, Internet-Draft, draft-ietf-

sidrops-8210bis-25, 2 March 2026,
<https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-8210bis-25>.

[I-D.ietf-sidrops-aspa-profile]
Snijders, J., Azimov, A., Uskov, E., Bush, R., Housley, R., and B. Maddison, "A Profile for Autonomous System Provider Authorization", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-profile-26, 19 April 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-profile-26>.

[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-25, 19 April 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-25>.

[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>.

[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>.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, DOI 10.17487/RFC6487, February 2012, <https://www.rfc-editor.org/info/rfc6487>.

[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>.

[RFC6907] Manderson, T., Sriram, K., and R. White, "Use Cases and Interpretations of Resource Public Key Infrastructure (RPKI) Objects for Issuers and Relying Parties", RFC 6907, DOI 10.17487/RFC6907, March 2013, <https://www.rfc-editor.org/info/rfc6907>.

[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>.

[RFC7908] Sriram, K., Montgomery, D., McPherson, D., Osterweil, E., and B. Dickson, "Problem Definition and Classification of BGP Route Leaks", RFC 7908, DOI 10.17487/RFC7908, June 2016, <https://www.rfc-editor.org/info/rfc7908>.

[RFC7935] Huston, G. and G. Michaelson, Ed., "The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure", RFC 7935, DOI 10.17487/RFC7935, August 2016, <https://www.rfc-editor.org/info/rfc7935>.

[RFC8181] Weiler, S., Sonalker, A., and R. Austein, "A Publication Protocol for the Resource Public Key Infrastructure (RPKI)", RFC 8181, DOI 10.17487/RFC8181, July 2017, <https://www.rfc-editor.org/info/rfc8181>.

[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>.

[RFC8209] Reynolds, M., Turner, S., and S. Kent, "A Profile for BGPsec Router Certificates, Certificate Revocation Lists, and Certification Requests", RFC 8209, DOI 10.17487/RFC8209, September 2017, <https://www.rfc-editor.org/info/rfc8209>.

[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>.

[RFC8608] Turner, S. and O. Borchert, "BGPsec Algorithms, Key Formats, and Signature Formats", RFC 8608, DOI 10.17487/RFC8608, June 2019, <https://www.rfc-editor.org/info/rfc8608>.

[RFC8630] Huston, G., Weiler, S., Michaelson, G., Kent, S., and T. Bruijnzeels, "Resource Public Key Infrastructure (RPKI) Trust Anchor Locator", RFC 8630, DOI 10.17487/RFC8630, August 2019, <https://www.rfc-editor.org/info/rfc8630>.

[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>.

[RFC9582] Snijders, J., Maddison, B., Lepinski, M., Kong, D., and S. Kent, "A Profile for Route Origin Authorizations (ROAs)", RFC 9582, DOI 10.17487/RFC9582, May 2024, <https://www.rfc-editor.org/info/rfc9582>.

[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>.

Authors' Addresses

Zhiwei Yan
CNNIC
Email: yan@cnnic.cn

Tim Bruijnzeels
RIPE NCC
Email: tim@ripe.net

Tom Harrison
APNIC
Email: tomh@apnic.net

Sofa Silva Berenguer
NRO
Email: sofia@apnic.net