Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 18 April 2026

J. Snijders
BSD
T. Buehler
OpenBSD

15 October 2025

Constraining RPKI Trust Anchors
draft-snij-sidrops-constraining-rpki-trust-anchors-00

Abstract

This document describes an approach for Resource Public Key Infrastructure (RPKI) Relying Parties (RPs) to impose locally configured Constraints on cryptographic products subordinate to Trust Anchors (TAs). The ability to constrain a Trust Anchor operator's effective signing authority to a limited set of Internet Number Resources (INRs) allows Relying Parties to enjoy the potential benefits of assuming trust - within a bounded scope. The specified approach and configuration format allow RPKI operators to communicate efficiently about observations related to Trust Anchor operations.

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 18 April 2026.

Table of Contents

1. Introduction

This document describes an approach for Resource Public Key Infrastructure (RPKI) Relying Parties (RPs) to impose locally configured Constraints on cryptographic products subordinate to trusted Trust Anchors (TAs). The ability to constrain a Trust Anchor operator's effective signing authority to a limited set of Internet Number Resources (INRs) allows Relying Parties to enjoy the potential benefits of assuming trust - within a bounded scope. The specified approach and configuration format allow RPKI operators to communicate efficiently about observations related to Trust Anchor operations.

It is important to emphasize that each Relying Party makes its Trust Anchor inclusion decisions independently, on its own timelines, based on its own inclusion criteria; and that imposed Constraints (if any) are a matter of local configuration.

This document is intended to address user (meaning, Network Operator and Relying Party) needs and concerns, and was authored to benefit users and providers of RPKI services by providing a common body of knowledge to be communicated within the global Internet routing system community.

1.1. Definitions

Assumed Trust In the RPKI hierarchical structure, a Trust Anchor is an authority for which trust is assumed and not derived. Assumed trust means that violation of that trust is out-of-scope for the threat model.

Derived Trust Derived Trust can be automatically and securely computed with subjective logic. In the context of the RPKI, trust is derived according to the rules for validation of RPKI Certificates and Signed Objects.

Constraints The locally configured union set of IP prefixes, IP address ranges, AS identifiers, and AS identifier ranges for which the Relying Party operator anticipates the Trust Anchor operator to issue cryptographic products.

1.2. Required Reading

Readers should be familiar with the RPKI, the RPKI repository structure, and the various RPKI objects, uses, and interpretations described in the following: [RFC3779], [RFC6480], [RFC6481], [RFC6487], and [RFC6488].

2. Considerations on Trust Anchor over-claiming

Currently, all five Regional Internet Registries (RIRs) list 'all-resources' (0.0.0.0/0, ::/0, and AS 0-4294967295) as subordinate on their Trust Anchor certificates in order to reduce some potential for risk of invalidation in the case of transient registry inconsistencies [I-D.rir-rpki-allres-ta-app-statement]. Such 'all-resources' listings demonstrate that - in the course of normal operations - Trust Anchors may claim authority for INRs outside the registry's current resource holdings.

The primary reason for transient registry inconsistencies to occur would be when resources are transferred from one registry to another. However, the ability to transfer resources between registries is not universally available: this ability depends on the implementation of registry-specific consensus-driven policy development reciprocated by other registries. Another source of churn would be the inflow of new resources following allocations made by the IANA; but because of IPv4 address exhaustion, IPv6 abundance, and 32-bit ASNs being allocated in large blocks - IANA allocations occur far less often than they used to.

Absent a registry's ability to execute inter-registry transfers or frequently receive new allocations from IANA, that registry's set of holdings would be a fairly static list of resources.

Therefore, a Relying Party need not trust each and every signed product in a derived trust relationship to any and all INRs subordinate to the registry's Trust Anchor, even when the Trust Anchor certificate lists 'all-resources' as subordinate. Following the widely deployed information security principle of least privilege [PRIVSEP], constraining a given Trust Anchor's capacity strictly to just that what relates to the their respective current INR holdings, provides some degree of risk reduction for all stakeholders involved.

Consequently, knowing a registry's current resource holdings and knowing this set of holdings will not change in the near-term future; following the principle of least privilege, operators can consider applying a restricted-service operating mode towards what otherwise would be an unbounded authority. The principle of constraining Trust Anchors might be useful when for example working with RPKI testbeds [OTE], risky Trust Anchors which cover unallocated space with AS0 ROAs [AS0TAL], but also in dealings with publicly-trusted registries.

3. Constraining Trust Anchors by constraining End-Entity Certificates

As noted in Section 2, the current set of publicly-trusted RPKI TA certificates are expected to overclaim in the course of normal operations. However, applying a bespoke implementation of the certification path validation algorithm to CA certificates to prune all possible certificate paths related to INRs not contained within the locally configured Constraints would not be a trivial task. Instead, an alternative and simpler approach operating on EE certificates is proposed.

To constrain a Trust Anchor, the IP address and AS number resources listed in a given EE certificate's [RFC3779] extensions MUST be fully contained within the locally configured union set of IP prefixes, IP address ranges, AS identifiers, and AS identifier ranges for which the Relying Party operator anticipates the Trust Anchor operator to issue cryptographic products. If a given EE certificate's listed resources are not fully contained within the Constraints, the RP should halt processing and consider the EE certificate invalid.

The above described approach applies to all RPKI objects for which an explicit listing of resources is mandated in their respective [RFC3779] extensions; such as BGPSec Router Certificates [RFC8209], ROAs [RFC9582], ASPAs [I-D.ietf-sidrops-aspa-profile], RSCs [RFC9323], and Geofeeds [RFC9632].

The approach has no application in context of Signed Objects unrelated to INRs (which thus use 'inherit' elements); such as Ghostbusters records [RFC6493], Signed TALs [RFC9691], and Manifests [RFC9286].

The validation of Constraint containment is a check in addition to all the validation checks specified in [RFC6487], [RFC6488], and each Signed Object's profile specification.

4. Operational Considerations

When assessing the feasibility of constraining a Trust Anchor's effective signing abilities to the registry's current set of holdings, it is important to take note of existing policies (or lack thereof) and possible future events which might impact the degree of churn in the registry's holdings. Examples are:

The ARIN policy development community abandoned a proposal to allow inter-regional IPv6 resource transfers [ARIN-2019-4]. Since it's currently not possible to transfer IPv6 resources from ARIN to any other RIR, ARIN's IANA-allocated IPv6 resources should not appear subordinate to any Trust Anchor other than ARIN's own Trust Anchor.

The APNIC policy development community has not developed policy [APNIC-interrir] to support inter-RIR IPv6 transfers.

The LACNIC policy development community has not developed policy [LACNIC-interrir] to support inter-RIR IPv6 or ASN transfers.

The RIPE NCC policy development community _did_ develop policy [RIPE-interrir] to support inter-RIR IPv6 transfers, but being the _only_ community to have done so, inter-RIR transfers are not possible.

AFRINIC has not ratified an inter-registry transfer policy [AFPUB-2020-GEN-006-DRAFT03]. The policy proposal indicates implementation is expected to take an additional 12 months after ratification. Since it's not possible to transfer resources into AFRINIC, non-AFRINIC resources should not appear subordinate to AFRINIC's Trust Anchor for the foreseeable future.

The RIRs collectively manage only a subset of 0.0.0.0/0 [IANA-IPV4] and 2000::/3 [IANA-IPV6]; and have no authority over any parts of 10.0.0.0/8 [RFC1918], 2001:db8::/32 [RFC3849], and AS 64512 - 65534 [RFC6996], for example. Since it's not possible to transfer private internet allocations, documentation prefixes, or private use ASNs into an RIR's management, such resources should not appear subordinate to any RIR's Trust Anchor.

In recent times IANA has not made allocations from the Current Recovered IPv4 Pool [IANA-RECOVERED], and Autonomous System Number allocations are also fairly infrequent [IANA-ASNS].

It is clear from the aforementioned observations that, while there are sound reasons to declare ’all resources’ as subordinate ([I-D.rir-rpki-allres-ta-app-statement]), there are resources which would never be subordinate to any particular Regional Internet Registry in the normal course of operations. Maintainers of Constraint lists disseminated as part of an operating system or a third-party software package release process would do well to assume a six month delay for users to update.

5. Security Considerations

The routing security benefits promised by the RPKI are derived from assuming trust in registry operators to run flawless certification services. Assuming such trust exposes users to some potential for [risks] and adverse actions by Certificate Authorities [RFC8211]. Restricting a Trust Anchor’s effective signing abilities to its respective registry’s current holdings - rather assuming unbounded trust in such authorities - is a constructive approach to limit some potential for risk.

6. References

6.1. Informative References

[AFPUB-2020-GEN-006-DRAFT03]
Ehoumi, G. O., Maina, N., and A. A. P. Aina, "AFRINIC Number Resources Transfer Policy (Draft-3)", February 2022, <https://afrinic.net/policy/proposals/2020-gen-006-d3>.

[APNIC-interrir]
APNIC, "Transfer of unused IPv4 addresses and/or AS numbers", 2023, <https://www.apnic.net/manage-ip/manage-resources/transfer-resources/transfer-of-unused-ip-and-as-numbers/>.

[ARIN-2019-4]
Snijders, J., Farmer, D., and J. Provo, "Draft Policy ARIN-2019-4: Allow Inter-regional IPv6 Resource Transfers", September 2019, <https://www.arin.net/vault/policy/proposals/2019_4.html>.

[AS0TAL] APNIC, "Important notes on the APNIC AS0 ROA", 2023, <https://www.apnic.net/community/security/resource-certification/apnic-limitations-of-liability-for-rpki-2/>.

[I-D.ietf-sidrops-aspa-profile] Azimov, A., Uskov, E., Bush, R., Snijders, J., Housley, R., and B. Maddison, "A Profile for Autonomous System Provider Authorization", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-profile-20, 18 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-profile-20>.

[I-D.rir-rpki-allres-ta-app-statement] Newton, A., Mart鱈nez, C. M., Shaw, D., Bruijnzeels, T., and B. Ellacott, "RPKI Multiple "All Resources" Trust Anchors Applicability Statement", Work in Progress, Internet-Draft, draft-rir-rpki-allres-ta-app-statement-02, 18 July 2017, <https://datatracker.ietf.org/doc/html/draft-rir-rpki-allres-ta-app-statement-02>.

[IANA-ASNS] IANA, "Autonomous System (AS) Numbers", August 2023, <https://www.iana.org/assignments/as-numbers/>.

[IANA-IPV4] IANA, "IANA IPv4 Address Space Registry", July 2023, <https://www.iana.org/assignments/ipv4-address-space/>.

[IANA-IPV6] IANA, "IPv6 Global Unicast Address Assignments", November 2019, <https://www.iana.org/assignments/ipv6-unicast-address-assignments/>.

[IANA-RECOVERED] IANA, "IPv4 Recovered Address Space", March 2019, <https://www.iana.org/assignments/ipv4-recovered-address-space/>.

[LACNIC-interrir] LACNIC, "LACNIC POLICY MANUAL (v2.19 - 22/08/2023)", August 2023, <https://www.lacnic.net/innovaportal/file/680/1/manual-politicas-en-2-19.pdf>.

[OTE] ARIN, "Operational Test and Evaluation (OT&E) Environment", 2023, <https://www.arin.net/reference/tools/testing/>.

[PRIVSEP] Obser, F., "Privilege drop, privilege separation, and restricted-service operating mode in OpenBSD", <https://sha256.net/privsep.html>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/info/rfc1918>.

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, DOI 10.17487/RFC3779, June 2004, <https://www.rfc-editor.org/info/rfc3779>.

[RFC3849] Huston, G., Lord, A., and P. Smith, "IPv6 Address Prefix Reserved for Documentation", RFC 3849, DOI 10.17487/RFC3849, July 2004, <https://www.rfc-editor.org/info/rfc3849>.

[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>.

[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>.

[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>.

[RFC6996] Mitchell, J., "Autonomous System (AS) Reservation for Private Use", BCP 6, RFC 6996, DOI 10.17487/RFC6996, July 2013, <https://www.rfc-editor.org/info/rfc6996>.

[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>.

[RFC8211] Kent, S. and D. Ma, "Adverse Actions by a Certification Authority (CA) or Repository Manager in the Resource Public Key Infrastructure (RPKI)", RFC 8211, DOI 10.17487/RFC8211, September 2017, <https://www.rfc-editor.org/info/rfc8211>.

[RFC9286] Austein, R., Huston, G., Kent, S., and M. Lepinski, "Manifests for the Resource Public Key Infrastructure (RPKI)", RFC 9286, DOI 10.17487/RFC9286, June 2022, <https://www.rfc-editor.org/info/rfc9286>.

[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>.

[RFC9632] Bush, R., Candela, M., Kumari, W., and R. Housley, "Finding and Using Geofeed Data", RFC 9632, DOI 10.17487/RFC9632, August 2024, <https://www.rfc-editor.org/info/rfc9632>.

[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>.

[RIPE-interrir] NCC, R., "Inter-RIR Transfers", February 2023, <https://www.ripe.net/manage-ips-and-asns/resource-transfers-and-mergers/inter-rir-transfers>.

[risks] Cooper, D., Heilman, E., Brogle, K., Reyzin, L., and S. Goldberg, "On the Risk of Misbehaving RPKI Authorities", <https://www.cs.bu.edu/~goldbe/papers/hotRPKI.pdf>.

[rpki-client]
Jeker, C., Snijders, J., Dzonsons, K., and T. Buehler, "rpki-client", July 2023, <https://www.rpki-client.org/>.

Appendix A. Example listing of Constraints

This section contains an example Constraints listing.

As it’s clumsy and error prone to calculate the complement of a block of resources, for efficiency a simple notation in the form of *allow* and *deny* keywords is used to indicate INRs which may or may not appear subordinate to a Trust Anchor (rather than merely using lengthy exhaustive allowlists of what INRs may appear under a given Trust Anchor). Denylist entries (entries prefixed with *deny*) take precedence over allowlist entries (entries prefixed with *allow*). Denylist entries may not overlap with other denylist entries. Allowlist entries may not overlap with other allowlist entries. The ordering of entries is not significant.

Constraints applicable to an Example Trust Anchor

If the below content is placed in a file named *example.constraints* next to a Trust Anchor Locator file named *example.tal*, the [rpki-client] implementation will only accept an End-Entity certificate subordinate to *example.tal* if all its resources are fully contained within the resources allowed in *example.constraints*.

```
# Example constraints following the format described in
# fdraft-spaghetti-sidrops-constraining-rpki-trust-anchors

# This is a comment

allow 10.0.0.0/8      # comments may follow entries

allow 192.168.0.0/12
deny 192.168.1.0/24   # carve a hole in the above entry

allow 192.0.2.0/24

allow 100.64.0.0 - 100.127.255.254 # this is a range
allow 203.0.113.0 - 203.0.113.255  # this too

allow 3fff::/20       # IPv6 is also supported
deny 3fff::/48

deny 2001:db8:: - 2001:db8::ffff # an IPv6 range

# From https://www.iana.org/assignments/as-numbers/
allow 64496 - 64511
deny 65123           # carve a hole in the above entry

allow 65536          # can declare for single ASN

deny 4200000000 - 4294967294

# There is an implicit deny for all resources which were not
# explicitly allowed through 'allow' declarations.
```

Appendix B. Implementation Status

The approach specified in this document has been implemented in [rpki-client] and has been enabled by default in releases since 2023.

Acknowledgements

Thanks to Niels Bakker, Joel Jaeggli, Tony Tauber, Tom Scholl, Erik Bais, Simon Leinen, and Nick Hilliard for their feedback and input.

Authors' Addresses

Job Snijders
BSD Software Development
Amsterdam
Netherlands
Email: job@bsd.nl

URI: https://www.bsd.nl/

Theo Buehler
OpenBSD
Switzerland
Email: tb@openbsd.org