Constraining RPKI Trust Anchors

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 publicly-trusted Trust Anchors (TAs), as implemented in OpenBSD's rpki-client validator. 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.

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 11 August 2024.

Copyright Notice

Copyright (c) 2024 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.
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 publicly-trusted Trust Anchors (TAs), as implemented in the [OpenBSD] [rpki-client] validator. 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.

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. Assuming 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, 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 [I-D.ietf-sidrops-rfc6482bis], ASPAs [I-D.ietf-sidrops-aspa-profile], RSCs [RFC9323], and Geofeeds [I-D.ietf-opsawg-9092-update].

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 [I-D.ietf-sidrops-signed-tal], 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::/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].

The aforementioned observations suggest there is a lot of operational runway to manage and distribute Trust Anchor Constraints
in a timely manner. 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


**[OTE]**

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

**[RFC1918]**

**[RFC3779]**

**[RFC3849]**

**[RFC6480]**

**[RFC6481]**

**[RFC6487]**

**[RFC6488]**

**[RFC6493]**

**[RFC6996]**


Appendix A. Example listings of Constraints

This section contains examples of Constraints listings related to ARIN & AFRINIC managed INRs, and INRs allocated for private or non-public use. Constraint suggestions are offered specific to each of the five RIR Trust Anchors.

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 AFRINIC's Trust Anchor

The below listing is intended to be an exhaustive list of Constraints related to AFRINIC-managed Internet Number Resources. Inter-RIR resource transfers aren't possible into and out of the AFRINIC registry.

By placing the below contents in a file named `afrinic.constraints` next to a Trust Anchor Locator file named `afrinic.tal`, the [rpki-client] implementation will consider all End-Entity certificates invalid which list resources not fully contained within the resources listed in the `afrinic.constraints` file.
allow 41.0.0.0/8
allow 102.0.0.0/8
allow 105.0.0.0/8
allow 154.0.0.0/16
allow 154.16.0.0/16
allow 154.65.0.0 - 154.255.255.255
allow 196.0.0.0 - 196.1.0.255
allow 196.1.4.0/24
allow 196.1.7.0 - 196.1.63.255
allow 196.1.71.0/24
allow 196.1.74.0 - 196.1.103.255
allow 196.1.115.0 - 196.1.133.255
allow 196.1.137.0/24
allow 196.1.143.0 - 196.1.159.255
allow 196.1.176.0 - 196.1.255.255
allow 196.2.2.0/23
allow 196.2.8.0 - 196.2.255.255
allow 196.3.14.0/23
allow 196.3.57.0 - 196.3.64.255
allow 196.3.90.0/24
allow 196.3.92.0 - 196.3.94.255
allow 196.3.96.0/21
allow 196.3.105.0/24
allow 196.3.107.0 - 196.3.131.255
allow 196.3.148.0/22
allow 196.3.154.0 - 196.3.183.255
allow 196.3.224.0 - 196.4.45.255
allow 196.4.71.0 - 196.11.171.255
allow 196.11.174.0 - 196.11.239.255
allow 196.11.248.0/21
allow 196.12.10.0 - 196.12.31.255
allow 196.12.128.0/19
allow 196.12.192.0 - 196.15.15.255
allow 196.15.64.0 - 196.26.255.255
allow 196.27.64.0 - 196.28.47.255
allow 196.28.64.0 - 196.29.63.255
allow 196.29.96.0 - 196.31.255.255
allow 196.32.8.0 - 196.32.31.255
allow 196.32.96.0/19
allow 196.32.160.0 - 196.39.255.255
allow 196.40.96.0 - 196.41.255.255
allow 196.42.64.0 - 196.216.0.255
allow 196.216.2.0 - 197.255.255.255
allow 2001:4200::/23
allow 2c00::/12

# From https://www.iana.org/assignments/as-numbers/
allow 36864 - 37887
allow 327680 - 328703
allow 328704 - 329727

# From https://www.iana.org/assignments/ipv4-recovered-address-space
allow 45.96.0.0 - 45.111.255.255
allow 45.192.0.0 - 45.222.255.255
allow 45.240.0.0 - 45.247.255.255
allow 66.251.128.0 - 66.251.191.255
allow 139.26.0.0 - 139.26.255.255
allow 146.196.128.0 - 146.196.255.255
# 154.16.0.0 - 154.16.255.255 # already contained within 154/8
allow 160.19.36.0 - 160.19.39.255
allow 160.19.60.0 - 160.19.63.255
allow 160.19.96.0 - 160.19.103.255
allow 160.19.112.0 - 160.19.143.255
allow 160.19.152.0 - 160.19.155.255
allow 160.19.188.0 - 160.19.191.255
allow 160.19.192.0 - 160.19.199.255
allow 160.19.232.0 - 160.19.239.255
allow 160.20.24.0 - 160.20.31.255
allow 160.20.112.0 - 160.20.115.255
allow 160.20.213.0 - 160.20.213.255
allow 160.20.217.0 - 160.20.217.255
allow 160.20.221.0 - 160.20.221.255
allow 160.20.226.0 - 160.20.227.255
allow 160.20.252.0 - 160.20.255.255
allow 160.238.11.0 - 160.238.11.255
allow 160.238.48.0 - 160.238.49.255
allow 160.238.50.0 - 160.238.50.255
allow 160.238.57.0 - 160.238.57.255
allow 160.238.101.0 - 160.238.101.255
allow 161.123.0.0 - 161.123.255.255
allow 164.160.0.0 - 164.160.255.255
allow 192.12.110.0 - 192.12.111.255
allow 192.12.116.0 - 192.12.117.255
allow 192.47.36.0 - 192.47.36.255
allow 192.51.240.0 - 192.51.240.255
allow 192.76.200.0 - 192.76.201.255
allow 192.75.236.0 - 192.75.236.255
allow 192.83.208.0 - 192.83.215.255
allow 192.91.200.0 - 192.91.200.255
allow 192.142.0.0 - 192.143.255.255
allow 192.145.128.0 - 192.145.191.255
allow 192.145.230.0 - 192.145.230.255
allow 204.8.204.0 - 204.8.207.255
allow 208.85.156.0 - 208.85.159.255

# From https://afrinic.net/fr/library/policies/220-erx-transfer
allow 2561
allow 3208
allow 5536
allow 6127
allow 6713
allow 6879
allow 8524
allow 8770
allow 9129
allow 11380
allow 12455
allow 12556
allow 13224
allow 15399
allow 13569
allow 15475
allow 15706
allow 15804
allow 15825
allow 15834
allow 15964
allow 16058
allow 16214
allow 16284
allow 16853
allow 16907
allow 17652
allow 19676
allow 20294
allow 20484
allow 20858
allow 20928
allow 21003
allow 21152
allow 21242
allow 21271
allow 21278
allow 21280
allow 21391
allow 21452
allow 23549
allow 23889
allow 24736
allow 24757
allow 24788
allow 24801
allow 24835
allow 24863
allow 24878
allow 24987
allow 25163
allow 25250
allow 25362
allow 25364
allow 25543
allow 25568
allow 25576
allow 28683
allow 28698
allow 28913
allow 29091
allow 29338
allow 29340
allow 29428
allow 29495
allow 29544
allow 29571
allow 29614
allow 29674
allow 30896
allow 31065
allow 31245
allow 31619
allow 83.143.24.0 - 83.143.31.255
allow 84.205.96.0 - 84.205.127.255
allow 131.176.0.0 - 131.176.255.255
allow 163.121.0.0 - 163.121.255.255
allow 165.231.0.0 - 165.231.255.255
allow 192.52.232.0 - 192.52.232.255
allow 193.17.215.0 - 193.17.215.255
allow 193.41.146.0 - 193.41.147.255
allow 193.108.23.0 - 193.108.23.255
allow 193.108.28.0 - 193.108.28.255
allow 193.109.66.0 - 193.109.67.255
allow 193.110.104.0 - 193.110.105.255
allow 193.194.128.0 - 193.194.128.255
allow 193.227.128.0 - 193.227.128.255
allow 194.9.64.0 - 194.9.65.255
allow 194.9.82.0 - 194.9.83.255
allow 195.24.80.0 - 195.24.87.255
allow 195.39.218.0 - 195.39.219.255
allow 195.234.120.0 - 195.234.123.255
allow 195.234.168.0 - 195.234.168.255
allow 195.234.185.0 - 195.234.185.255
allow 195.234.252.0 - 195.234.255.255

allow 30980
allow 30982 - 30999

# From https://afrinic.net/ast/pdf/afrinic-whois-audit-report-full-20210
# 12.3 Appendix A3
allow 193.188.7.0/24
allow 193.189.0.0/18
allow 193.189.128.0/24
allow 193.194.160.0/19
allow 193.221.218.0/24

# From https://ftp.arin.net/afrinic/afrinic-transfers-by-resource.txt
# Feb 21, 2005
allow 1228 - 1232
allow 2018
allow 2905
allow 3067
allow 3068
allow 3741
allow 4178
allow 4571
allow 5713
allow 5734
allow 6083
allow 6089
allow 6149
allow 6180
allow 6187
allow 6351
allow 6529
allow 6560
allow 6968
allow 7020
allow 7154
allow 7231
allow 7390
allow 7420
allow 7460
allow 7971
allow 7972
allow 8094
allow 10247
allow 10262
allow 10331
allow 10393
allow 10474
allow 10505
allow 10540
allow 10575
allow 10798
allow 10803
allow 10898
allow 10922
allow 11125
allow 11157
allow 11201
allow 11259
allow 11265
allow 11569
allow 11645
allow 11744
allow 11845
allow 11909
allow 12091
allow 12143
allow 12258
allow 13402
allow 13519
allow 13854
allow 14029
allow 14115
allow 14331
allow 14360
allow 14429
allow 14516
allow 14988
allow 15022
allow 15159
allow 16416
allow 16547
allow 16630
allow 16637
allow 16800
allow 17148
allow 17220
allow 17260
allow 17312
allow 17400
allow 18775
allow 18922
allow 18931
allow 19136
allow 19232
allow 33579
allow 33762 - 33791
allow 64.57.112.0 - 64.57.127.255
allow 66.8.0.0 - 66.8.127.255
allow 66.18.64.0 - 66.18.95.255
allow 69.63.64.0 - 69.63.79.255
allow 69.67.32.0 - 69.67.47.255
allow 137.158.0.0 - 137.158.255.255
allow 137.214.0.0 - 137.214.255.255
allow 137.215.0.0 - 137.215.255.255
allow 139.53.0.0 - 139.53.255.255
allow 143.128.0.0 - 143.128.255.255
allow 143.160.0.0 - 143.160.255.255
allow 146.64.0.0 - 146.64.255.255
allow 146.141.0.0 - 146.141.255.255
allow 146.182.0.0 - 146.182.255.255
allow 146.230.0.0 - 146.230.255.255
allow 146.231.0.0 - 146.231.255.255
allow 146.232.0.0 - 146.232.255.255
allow 147.110.0.0 - 147.110.255.255
allow 152.106.0.0 - 152.106.255.255
allow 152.107.0.0 - 152.107.255.255
allow 152.108.0.0 - 152.108.255.255
allow 152.109.0.0 - 152.109.255.255
allow 152.110.0.0 - 152.110.255.255
allow 152.111.0.0 - 152.111.255.255
allow 152.112.0.0 - 152.112.255.255
allow 155.159.0.0 - 155.159.255.255
allow 155.232.0.0 - 155.232.255.255
allow 155.233.0.0 - 155.233.255.255
allow 155.234.0.0 - 155.234.255.255
allow 155.235.0.0 - 155.235.255.255
allow 155.236.0.0 - 155.236.255.255
allow 155.237.0.0 - 155.237.255.255
allow 155.238.0.0 - 155.238.255.255
allow 155.239.0.0 - 155.239.255.255
allow 155.240.0.0 - 155.240.255.255
allow 156.8.0.0 - 156.8.255.255
allow 160.115.0.0 - 160.115.255.255
allow 160.116.0.0 - 160.116.255.255
allow 160.117.0.0 - 160.117.255.255
allow 160.118.0.0 - 160.118.255.255
allow 160.119.0.0 - 160.119.255.255
allow 160.120.0.0 - 160.120.255.255
allow 160.121.0.0 - 160.121.255.255
allow 160.122.0.0 - 160.122.255.255
allow 160.123.0.0 - 160.123.255.255
allow 160.124.0.0 - 160.124.255.255
allow 163.195.0.0 - 163.195.255.255
allow 163.196.0.0 - 163.196.255.255
allow 163.197.0.0 - 163.197.255.255
allow 163.198.0.0 - 163.198.255.255
allow 163.199.0.0 - 163.199.255.255
allow 163.200.0.0 - 163.200.255.255
allow 163.201.0.0 - 163.201.255.255
allow 163.203.0.0 - 163.203.255.255
allow 164.88.0.0 - 164.88.255.255
allow 164.146.0.0 - 164.151.255.255
allow 164.155.0.0 - 164.155.255.255
allow 165.3.0.0 - 165.5.255.255
allow 165.8.0.0 - 165.11.255.255
allow 165.25.0.0 - 165.25.255.255
allow 165.143.0.0 - 165.149.255.255
allow 165.165.0.0 - 165.165.255.255
allow 165.180.0.0 - 165.180.255.255
allow 165.233.0.0 - 165.233.255.255
allow 166.85.0.0 - 166.85.255.255
allow 168.76.0.0 - 168.76.255.255
allow 168.80.0.0 - 168.81.255.255
allow 168.89.0.0 - 168.89.255.255
allow 168.128.0.0 - 168.128.255.255
allow 168.142.0.0 - 168.142.255.255
allow 168.155.0.0 - 168.155.255.255
allow 168.164.0.0 - 168.164.255.255
allow 168.167.0.0 - 168.167.255.255
allow 168.172.0.0 - 168.172.255.255
allow 168.206.0.0 - 168.206.255.255
allow 168.209.0.0 - 168.210.255.255
allow 169.129.0.0 - 169.129.255.255
allow 192.33.10.0 - 192.33.10.255
allow 192.42.99.0 - 192.42.99.255
allow 192.48.253.0 - 192.48.253.255
allow 192.68.138.0 - 192.68.138.255
allow 192.70.237.0 - 192.70.237.255
allow 192.82.142.0 - 192.82.142.255
allow 192.84.244.0 - 192.84.244.255
allow 192.94.61.0 - 192.94.61.255
allow 192.94.240.0 - 192.94.240.255
allow 192.94.241.0 - 192.94.241.255
allow 192.94.246.0 - 192.94.246.255
allow 192.96.0.0 - 192.96.255.255
allow 192.100.1.0 - 192.100.1.255
allow 192.101.142.0 - 192.101.142.255
allow 192.102.9.0 - 192.102.9.255
allow 192.133.250.0 - 192.133.250.255
allow 192.136.55.0 - 192.136.55.255
allow 192.136.56.0 - 192.136.56.255
allow 192.136.57.0 - 192.136.57.255
allow 192.157.190.0 - 192.157.190.255
allow 192.188.164.0 - 192.188.167.255
allow 192.189.75.0 - 192.189.75.255
allow 192.189.139.0 - 192.189.140.255
allow 192.231.237.0 - 192.231.237.255
allow 192.231.254.0 - 192.231.254.255
allow 192.245.148.0 - 192.245.148.255
allow 198.54.0.0 - 198.54.255.255
allow 200.16.8.0 - 200.16.15.255
allow 204.12.128.0 - 204.12.143.255
allow 204.87.179.0 - 204.87.179.255
allow 204.152.14.0 - 204.152.15.255
allow 204.235.32.0 - 204.235.43.255
allow 205.159.79.0 - 205.159.79.255
allow 206.223.136.0 - 206.223.136.255
allow 209.203.0.0 - 209.203.63.255
allow 209.212.96.0 - 209.212.127.255
allow 216.236.176.0 - 216.236.191.255

# From rpki.afrinic.net/repository/04E8B0D80F4D11E0B657D8931367AE7D/apnic
# CN=APNICTOAFRINIC/serialNumber=6F1A103E1427FF03483ABFD9E34DACBE1524FF8
# Not Before: Mar 30 14:17:08 2020 GMT / Not After : Mar 30 00:00:00 202
# SHA256:B6w5P1mkoNyJtM99GfGLaaKkGfSkQ6+4eC4tPijBLyM=
allow 202.123.0.0/19

# From rpki.afrinic.net/repository/04E8B0D80F4D11E0B657D8931367AE7D/ripe
# CN=RIPETOAFRINIC/serialNumber=7F7AC180897983E29E937C0A187803C072755545
# Not Before: Mar 30 14:17:12 2020 GMT / Not After : Mar 30 00:00:00 202
# SHA256:64eh2w7qQrFQVPaQrRJ4kA83gUgE3EDvm0D0AWhCXMH=
allow 62.8.64.0/19
allow 62.12.96.0/19
allow 62.24.96.0/19
allow 62.61.192.0/18
allow 62.68.32.0/19
allow 62.68.224.0/19
allow 62.114.0.0/16
allow 62.117.32.0/19
allow 62.135.0.0/17
allow 62.139.0.0/16
allow 62.140.64.0/18
allow 62.173.32.0/19
allow 62.193.64.0/18
allow 62.193.160.0/19
allow 62.240.32.0/19
allow 62.240.96.0/19
allow 62.241.128.0/19
allow 62.251.128.0/17
allow 77.220.0.0/19
allow 80.67.128.0/20
allow 80.72.96.0/20
allow 80.75.160.0/19
allow 80.87.64.0/19
allow 80.88.0.0/20
allow 80.95.0.0/20
allow 80.240.192.0/20
allow 80.246.0.0/20
allow 80.248.0.0/20
allow 80.248.64.0/20
allow 80.249.64.0/20
allow 80.250.32.0/20
allow 81.4.0.0/18
allow 81.10.0.0/17
allow 81.21.96.0/20
allow 81.22.64.0/19
allow 81.26.64.0/20
allow 81.29.96.0/20
allow 81.91.224.0/20
allow 81.192.0.0/16
allow 82.101.128.0/18
allow 82.128.0.0/17
allow 82.129.128.0/17
allow 82.151.64.0/19
allow 82.201.128.0/17
allow 84.36.0.0/16
allow 84.233.0.0/17
allow 87.255.96.0/19
allow 193.95.0.0/17
allow 193.108.214.0/24
allow 193.108.252.0/22
allow 193.189.64.0 - 193.189.65.255
allow 193.194.1.0 - 193.194.5.255
allow 193.194.32.0 - 193.194.95.255
allow 193.227.0.0/18
allow 194.6.224.0/24
allow 194.79.96.0/19
allow 194.204.192.0/18
allow 195.24.192.0/19
allow 195.43.0.0/19
allow 195.166.224.0/19
allow 195.202.64.0/19
allow 195.246.32.0/19
allow 212.0.128.0/19
allow 212.12.224.0/19
allow 212.22.160.0/19
allow 212.49.64.0/19
allow 212.52.128.0/19
allow 212.60.64.0/19
allow 212.85.192.0/19
allow 212.88.96.0/19
allow 212.96.0.0/19
allow 212.100.64.0/19
allow 212.103.160.0/19
allow 212.122.224.0/19
allow 212.217.0.0/17
allow 213.55.64.0/18
allow 213.131.64.0/19
allow 213.136.96.0/19
allow 213.147.64.0/19
allow 213.150.96.0/19
allow 213.150.160.0 - 213.150.223.255
allow 213.152.64.0/19
allow 213.154.32.0 - 213.154.95.255
allow 213.158.160.0/19
allow 213.172.128.0/19
allow 213.179.160.0/19
allow 213.181.224.0/19
allow 213.193.32.0/19
allow 213.212.192.0/18
allow 213.247.0.0/19
allow 213.255.128.0/19
allow 217.14.80.0/20
allow 217.20.224.0/20
allow 217.21.112.0/20
allow 217.29.128.0/20
allow 217.29.208.0/20
allow 217.52.0.0/14
allow 217.64.96.0/20
allow 217.77.64.0/20
allow 217.78.64.0/20
allow 217.117.0.0/20
allow 217.139.0.0/16
allow 217.170.144.0/20
allow 217.199.144.0/20

# From rpki.afrinic.net/repository/04E8B0D80F4D11E0B657D8931367AE7D/arin
# CN=ARINTOAFRINIC/serialNumber=B87C5A75F3D957413AB998646946D4541D511455
# Not Before: Mar 30 14:17:09 2020 GMT / Not After : Mar 30 00:00:00 202
# SHA256:wmJV3qcw1PcLtmELBcvvyjs4V1Lz690bK3b8cv5v8F8=
allow 129.0.0.0/16
allow 129.18.0.0/16
allow 129.45.0.0/16
allow 129.56.0.0/16
allow 129.122.0.0/16
allow 129.140.0.0/16
allow 129.205.0.0/16
allow 129.232.0.0/16
allow 137.63.0.0 - 137.64.255.255
allow 137.115.0.0/16
allow 137.171.0.0/16
allow 137.196.0.0/16
allow 137.255.0.0/16
allow 155.0.0.0/16
allow 155.11.0.0 - 155.12.255.255
allow 155.89.0.0/16
allow 155.196.0.0/16
allow 155.251.0.0/16
allow 155.255.0.0 - 156.0.255.255
allow 156.38.0.0/16
allow 156.155.0.0 - 156.255.255.255
allow 160.0.0.0/16
allow 160.77.0.0/16
allow 160.89.0.0 - 160.90.255.255
allow 160.105.0.0/16
allow 160.113.0.0/16
allow 160.152.0.0/16
allow 160.154.0.0 - 160.179.255.255
allow 160.181.0.0 - 160.184.255.255
allow 160.224.0.0 - 160.226.255.255
allow 160.242.0.0/16
allow 160.255.0.0/16
allow 165.0.0.0/16
allow 165.16.0.0/16
allow 165.49.0.0 - 165.63.255.255
allow 165.73.0.0/16
allow 165.90.0.0/16
allow 165.169.0.0/16
allow 165.210.0.0/15
allow 165.255.0.0/16
allow 168.211.0.0 - 168.211.255.255
allow 168.253.0.0/16
allow 169.0.0.0/15
allow 169.159.0.0/16
allow 169.239.0.0/16
allow 169.255.0.0/16
allow 192.109.242.0/24
Constraints applicable to ARIN's Trust Anchor

Most of the below constraints relate to IP addresses and ASNs which are not globally unique and not managed by any RIR, as such these INRs are not expected to appear subordinate to any publicly-trusted Trust Anchor. LACNIC ASNs cannot be transferred to ARIN. Finally, since inter-RIR transfers involving ARIN may not include IPv6 addresses; ARIN's Trust Anchor is constrained to just its own IANA allocated IPv6 blocks.

By placing the below content in a file named arin.constraints; the associated Trust Anchor reachable via arin.tal is constrained such that any EE certificates listing private-use INRs, or non-ARIN IPv6 blocks, or AFRINIC superblocks, are considered invalid.
allow 2001:400::/23
allow 2001:1800::/23
allow 2001:4800::/23
allow 2600::/12
allow 2610::/23
allow 2620::/23
allow 2630::/12

deny 27648 - 28671
deny 52224 - 53247
deny 61440 - 61951
deny 64099 - 64197
deny 262144 - 273820

deny 41.0.0.0/8
deny 102.0.0.0/8
deny 105.0.0.0/8
deny 154.0.0.0/16
deny 154.16.0.0/16
deny 154.65.0.0 - 154.255.255.255
deny 196.0.0.0 - 196.1.0.255
deny 196.1.4.0/24
deny 196.1.7.0 - 196.1.63.255
deny 196.1.71.0/24
deny 196.1.74.0 - 196.1.103.255
deny 196.1.115.0 - 196.1.133.255
deny 196.1.137.0/24
deny 196.1.143.0 - 196.1.159.255
deny 196.1.176.0 - 196.1.255.255
deny 196.2.2.0/23
deny 196.2.8.0 - 196.2.255.255
deny 196.3.14.0/23
deny 196.3.57.0 - 196.3.64.255
deny 196.3.90.0/24
deny 196.3.92.0 - 196.3.94.255
deny 196.3.96.0/21
deny 196.3.105.0/24
deny 196.3.107.0 - 196.3.131.255
deny 196.3.148.0/22
deny 196.3.154.0 - 196.3.183.255
deny 196.3.224.0 - 196.4.45.255
deny 196.4.71.0 - 196.11.171.255
deny 196.11.174.0 - 196.11.239.255
deny 196.11.248.0/21
deny 196.12.10.0 - 196.12.31.255
deny 196.12.128.0/19
deny 196.12.192.0 - 196.15.15.255
deny 196.15.64.0 - 196.26.255.255
deny 196.27.64.0 - 196.28.47.255
deny 196.28.64.0 - 196.29.63.255
deny 196.29.96.0 - 196.31.255.255
deny 196.32.8.0 - 196.32.31.255
deny 196.32.96.0/19
deny 196.32.160.0 - 196.39.255.255
deny 196.40.96.0 - 196.41.255.255
deny 196.42.64.0 - 196.216.0.255
deny 196.216.2.0 - 197.255.255.255

# AFRINIC ASNs cannot be transferred to ARIN
# From https://www.iana.org/assignments/as-numbers/
deny 36864 - 37887
deny 327680 - 328703
deny 328704 - 329727

# Private use IPv4 & IPv6 addresses and ASNs
deny 0.0.0.0/8               # RFC 1122 Local Identification
deny 10.0.0.0/8              # RFC 1918 private space
deny 100.64.0.0/10           # RFC 6598 Carrier Grade NAT
deny 127.0.0.0/8             # RFC 1122 localhost
deny 169.254.0.0/16          # RFC 3927 link local
deny 172.16.0.0/12           # RFC 1918 private space
deny 192.0.2.0/24            # RFC 5737 TEST-NET-1
deny 192.88.99.0/24          # RFC 7526 6to4 anycast relay
deny 192.168.0.0/16          # RFC 1918 private space
deny 198.18.0.0/15           # RFC 2544 benchmarking
deny 198.51.100.0/24         # RFC 5737 TEST-NET-2
deny 203.0.113.0/24          # RFC 5737 TEST-NET-3
deny 224.0.0.0/4             # Multicast
deny 240.0.0.0/4             # Reserved
deny 23456                   # RFC 4893 AS_TRANS
deny 64496 - 64511           # RFC 5398
deny 64512 - 65534           # RFC 6996
deny 65535                   # RFC 7300
deny 65536 - 65551           # RFC 5398
deny 65552 - 131071          # IANA Reserved
deny 4200000000 - 4294967294 # RFC 6996
deny 4294967295              # RFC 7300

# ARIN supports IPv4 and ASN transfers: allow the complement of what is
# allow 0.0.0.0/0
allow 1 - 4199999999
Constraints applicable to APNIC's Trust Anchor

Given that ARIN, LACNIC, and RIPE NCC IPv6 resources cannot be transferred to APNIC, only APNIC IPv6 resources should appear subordinate to APNIC's Trust Anchor, private use INRs are not managed by any RIR, LACNIC ASNs cannot be transferred, and AFRINIC resources of any type cannot be transferred to and from any other RIR; the below constraints can be applied to APNIC Trust Anchor.

By placing the below content in files named apnic.constraints; the associated Trust Anchor reachable via apnic.tal is constrained such that any EE certificates or Signed Objects related to out-of-scope resources are considered invalid.
allow 2001:200::/23
allow 2001:c00::/23
allow 2001:e00::/23
allow 2001:4400::/23
allow 2001:8000::/19
allow 2001:a000::/20
allow 2001:b000::/20
allow 2400::/12

# IX Assignments
allow 2001:7fa::/32

# LACNIC ASNs cannot be transferred to APNIC
# From https://www.iana.org/assignments/as-numbers/as-numbers.xhtml
deny 27648 - 28671
deny 52224 - 53247
deny 61440 - 61951
deny 64099 - 64197
deny 262144 - 273820

# AFRINIC IPv4 resources cannot be transferred to APNIC
# From https://www.iana.org/assignments/ipv4-address-space/
deny 41.0.0.0/8
deny 102.0.0.0/8
deny 105.0.0.0/8
deny 154.0.0.0/16
deny 154.16.0.0/16
deny 154.65.0.0 - 154.255.255.255
deny 196.0.0.0 - 196.1.0.255
deny 196.1.4.0/24
deny 196.1.7.0 - 196.1.63.255
deny 196.1.71.0/24
deny 196.1.74.0 - 196.1.103.255
deny 196.1.115.0 - 196.1.133.255
deny 196.1.137.0/24
deny 196.1.143.0 - 196.1.159.255
deny 196.1.176.0 - 196.1.255.255
deny 196.2.2.0/23
deny 196.2.8.0 - 196.2.255.255
deny 196.3.14.0/23
deny 196.3.57.0 - 196.3.64.255
deny 196.3.90.0/24
deny 196.3.92.0 - 196.3.94.255
deny 196.3.96.0/21
deny 196.3.105.0/24
deny 196.3.107.0 - 196.3.131.255
deny 196.3.148.0/22
deny 196.3.154.0 - 196.3.183.255
deny 196.3.224.0 - 196.4.45.255
deny 196.4.71.0 - 196.11.171.255
deny 196.11.174.0 - 196.11.239.255
deny 196.11.248.0/21
deny 196.12.10.0 - 196.12.31.255
deny 196.12.128.0/19
deny 196.12.192.0 - 196.15.15.255
deny 196.15.64.0 - 196.26.255.255
deny 196.27.64.0 - 196.28.47.255
deny 196.28.64.0 - 196.29.63.255
deny 196.29.96.0 - 196.31.255.255
deny 196.32.8.0 - 196.32.31.255
deny 196.32.96.0/19
deny 196.32.160.0 - 196.39.255.255
deny 196.40.96.0 - 196.41.255.255
deny 196.42.64.0 - 196.216.0.255
deny 196.216.2.0 - 197.255.255.255

deny 36864 - 37887
deny 327680 - 328703
deny 328704 - 329727

# AFRINIC ASNs cannot be transferred to APNIC
# From https://www.iana.org/assignments/as-numbers/
deny 0.0.0.0/8               # RFC 1122 Local Identification
deny 10.0.0.0/8              # RFC 1918 private space
deny 100.64.0.0/10           # RFC 6598 Carrier Grade NAT
deny 127.0.0.0/8             # RFC 1122 localhost
deny 169.254.0.0/16          # RFC 3927 link local
deny 172.16.0.0/12           # RFC 1918 private space
deny 192.0.2.0/24            # RFC 5737 TEST-NET-1
deny 192.88.99.0/24          # RFC 7526 6to4 anycast relay
deny 192.168.0.0/16          # RFC 1918 private space
deny 198.18.0.0/15           # RFC 2544 benchmarking
deny 198.51.100.0/24         # RFC 5737 TEST-NET-2
deny 203.0.113.0/24          # RFC 5737 TEST-NET-3
deny 224.0.0.0/4             # Multicast
deny 240.0.0.0/4             # Reserved
deny 23456                    # RFC 4893 AS_TRANS
deny 64496 - 64511           # RFC 5398
deny 64512 - 65534            # RFC 6996
deny 65535                    # RFC 7300
deny 65536 - 65551            # RFC 5398
deny 65552 - 131071           # IANA Reserved
deny 4200000000 - 4294967294 # RFC 6996
deny 4294967295               # RFC 7300

# Private use IPv4 & IPv6 addresses and ASNs
# APNIC supports IPv4 and ASN transfers: allow the complement of what is
allow 0.0.0.0/0
allow 1 - 4199999999
Constraints applicable to LACNIC's Trust Anchor

Given that Autonomous System Numbers & IPv6 resources cannot be transferred from ARIN, APNIC, and RIPE NCC to LACNIC, only LACNIC ASNs & IPv6 resources should appear subordinate to LACNIC's Trust Anchor, private use INRs are not managed by any RIR, and AFRINIC resources of any type cannot be transferred to and from any other RIR; the below constraints can be applied to LACNIC Trust Anchor.

By placing the below content in files named `lacnic.constraints`; the associated Trust Anchor reachable via `lacnic.tal` is constrained such that any EE certificates or Signed Objects related to out-of-scope resources are considered invalid.
allow 2001:1200::/23
allow 2800::/12

allow 27648 - 28671
allow 52224 - 53247
allow 61440 - 61951
allow 64099 - 64197
allow 262144 - 273820

AFRINIC Internet Number Resources cannot be transferred

deny 41.0.0.0/8
deny 102.0.0.0/8
deny 105.0.0.0/8
deny 154.0.0.0/16
deny 154.16.0.0/16
deny 154.65.0.0 - 154.255.255.255
deny 196.0.0.0 - 196.1.0.255
deny 196.1.4.0/24
deny 196.1.7.0 - 196.1.63.255
deny 196.1.71.0/24
deny 196.1.74.0 - 196.1.103.255
deny 196.1.115.0 - 196.1.133.255
deny 196.1.137.0/24
deny 196.1.143.0 - 196.1.159.255
deny 196.1.176.0 - 196.1.255.255
deny 196.2.2.0/23
deny 196.2.8.0 - 196.2.255.255
deny 196.3.14.0/23
deny 196.3.57.0 - 196.3.64.255
deny 196.3.90.0/24
deny 196.3.92.0 - 196.3.94.255
deny 196.3.96.0/21
deny 196.3.105.0/24
deny 196.3.107.0 - 196.3.131.255
deny 196.3.148.0/22
deny 196.3.154.0 - 196.3.183.255
deny 196.3.224.0 - 196.4.45.255
deny 196.4.71.0 - 196.11.171.255
deny 196.11.174.0 - 196.11.239.255
deny 196.11.248.0/21
deny 196.12.10.0 - 196.12.31.255
deny 196.12.128.0/19
deny 196.12.192.0 - 196.15.15.255
deny 196.15.64.0 - 196.26.255.255
deny 196.27.64.0 - 196.28.47.255
deny 196.28.64.0 - 196.29.63.255
deny 196.29.96.0 - 196.31.255.255
deny 196.32.8.0 - 196.32.31.255
deny 196.32.96.0/19
deny 196.32.160.0 - 196.39.255.255
deny 196.40.96.0 - 196.41.255.255
deny 196.42.64.0 - 196.216.0.255
deny 196.216.2.0 - 197.255.255.255

# Private use IPv4 & IPv6 addresses and ASNs
deny 0.0.0.0/8               # RFC 1122 Local Identification
deny 10.0.0.0/8              # RFC 1918 private space
deny 100.64.0.0/10           # RFC 6598 Carrier Grade NAT
deny 127.0.0.0/8             # RFC 1122 localhost
deny 169.254.0.0/16          # RFC 3927 link local
deny 172.16.0.0/12           # RFC 1918 private space
deny 192.0.2.0/24            # RFC 5737 TEST-NET-1
deny 192.88.99.0/24          # RFC 7526 6to4 anycast relay
deny 192.168.0.0/16          # RFC 1918 private space
deny 198.18.0.0/15           # RFC 2544 benchmarking
deny 198.51.100.0/24         # RFC 5737 TEST-NET-2
deny 203.0.113.0/24          # RFC 5737 TEST-NET-3
deny 224.0.0.0/4              # Multicast
deny 240.0.0.0/4              # Reserved

# LACNIC supports only IPv4 transfers: allow the complement of what is denied
allow 0.0.0.0/0
Constraints applicable to LACNIC's Trust Anchor

Given that ARIN, APNIC, and LACNIC IPv6 resources cannot be transferred to RIPE NCC, only RIPE NCC IPv6 resources should appear subordinate to RIPE NCC's Trust Anchor, LACNIC ASNs cannot be transferred, private use INRs are not managed by any RIR, and AFRINIC resources of any type cannot be transferred to and from any other RIR; the below constraints can be applied to RIPE NCC Trust Anchor.

By placing the below content in files named ripe.constraints; the associated Trust Anchor reachable via ripe.tal is constrained such that any EE certificates or Signed Objects related to out-of-scope resources are considered invalid.
allow 2001:600::/23
allow 2001:800::/22
allow 2001:1400::/22
allow 2001:1a00::/23
allow 2001:1c00::/22
allow 2001:2000::/19
allow 2001:4000::/23
allow 2001:4600::/23
allow 2001:4a00::/23
allow 2001:4c00::/23
allow 2001:5000::/20
allow 2003::/18
allow 2a00::/12
allow 2a10::/12

# LACNIC ASNs cannot be transferred to RIPE NCC
# From https://www.iana.org/assignments/as-numbers/
deny 27648 - 28671
deny 52224 - 53247
deny 61440 - 61951
deny 64099 - 64197
deny 262144 - 273820

# AFRINIC IPv4 resources cannot be transferred to RIPE NCC
# From https://www.iana.org/assignments/ipv4-address-space/
deny 41.0.0.0/8
deny 102.0.0.0/8
deny 105.0.0.0/8
deny 154.0.0.0/16
deny 154.16.0.0/16
deny 154.65.0.0 - 154.255.255.255
deny 196.0.0.0 - 196.1.0.255
deny 196.1.4.0/24
deny 196.1.7.0 - 196.1.63.255
deny 196.1.71.0/24
deny 196.1.74.0 - 196.1.103.255
deny 196.1.115.0 - 196.1.133.255
deny 196.1.137.0/24
deny 196.1.143.0 - 196.1.159.255
deny 196.1.176.0 - 196.1.255.255
deny 196.2.2.0/23
deny 196.2.8.0 - 196.2.255.255
deny 196.3.14.0/23
deny 196.3.57.0 - 196.3.64.255
deny 196.3.90.0/24
deny 196.3.92.0 - 196.3.94.255
deny 196.3.96.0/21
deny 196.3.105.0/24
deny 196.3.107.0 - 196.3.131.255
deny 196.3.148.0/22
deny 196.3.154.0 - 196.3.183.255
deny 196.4.71.0 - 196.11.171.255
deny 196.11.174.0 - 196.11.239.255
deny 196.11.248.0/21
deny 196.12.10.0 - 196.12.31.255
deny 196.12.128.0/19
deny 196.12.192.0 - 196.15.15.255
deny 196.15.64.0 - 196.26.255.255
deny 196.27.64.0 - 196.28.47.255
deny 196.28.64.0 - 196.29.63.255
deny 196.29.96.0 - 196.31.255.255
deny 196.32.8.0 - 196.32.31.255
deny 196.32.96.0/19
deny 196.32.160.0 - 196.39.255.255
deny 196.40.96.0 - 196.41.255.255
deny 196.42.64.0 - 196.216.0.255
deny 196.216.2.0 - 197.255.255.255

deny 36864 - 37887
deny 327680 - 328703
deny 328704 - 329727

# Private use IPv4 & IPv6 addresses and ASNs
deny 0.0.0.0/8 # RFC 1122 Local Identification
deny 10.0.0.0/8 # RFC 1918 private space
deny 100.64.0.0/10 # RFC 6598 Carrier Grade NAT
deny 127.0.0.0/8 # RFC 1122 localhost
deny 169.254.0.0/16 # RFC 3927 link local
deny 172.16.0.0/12 # RFC 1918 private space
deny 192.0.2.0/24 # RFC 5737 TEST-NET-1
deny 192.88.99.0/24 # RFC 7526 6to4 anycast relay
deny 192.168.0.0/16 # RFC 1918 private space
deny 198.18.0.0/15 # RFC 2544 benchmarking
deny 198.51.100.0/24 # RFC 5737 TEST-NET-2
deny 203.0.113.0/24 # RFC 5737 TEST-NET-3
deny 224.0.0.0/4 # Multicast
deny 240.0.0.0/4 # Reserved
deny 23456 # RFC 4893 AS_TRANS
deny 64496 - 64511 # RFC 5398
deny 64512 - 65534 # RFC 6996
deny 65535 # RFC 7300
deny 65536 - 65551 # RFC 5398
deny 65552 - 131071          # IANA Reserved
deny 4200000000 - 4294967294 # RFC 6996
deny 4294967295              # RFC 7300

# RIPE NCC supports IPv4 and ASN transfers: allow the complement of what
allow 0.0.0.0/0
allow 1 - 4199999999

Acknowledgements

Thanks to Niels Bakker, Joel Jaeggli, Tony Tauber, and Tom Scholl for their feedback and input.

Authors' Addresses

Job Snijders
Fastly
Netherlands

Email: job@fastly.com

Theo Buehler
OpenBSD
Switzerland

Email: tb@openbsd.org