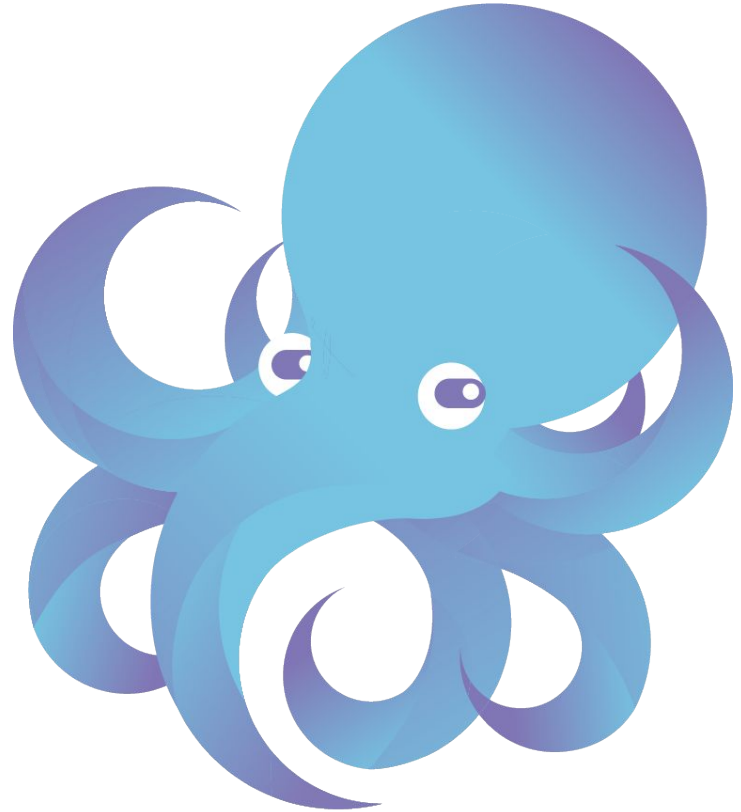




Cloudflare's RPKI Validator - LACNIC31

Louis Poinsignon



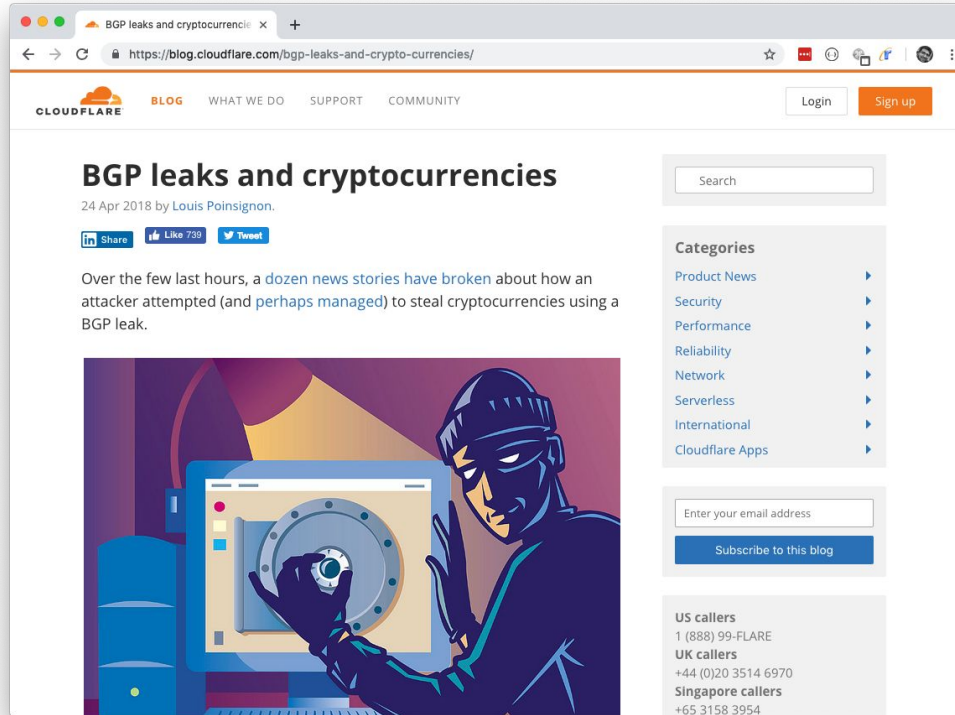
Introduction

Network Engineer at Cloudflare in San Francisco

Open-source projects including flows and RPKI

Network data collection (BGP, flows, peering-portal)

Story 1/4



The screenshot shows a web browser window displaying a blog post on the Cloudflare website. The browser's address bar shows the URL <https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/>. The page header includes the Cloudflare logo, navigation links for 'BLOG', 'WHAT WE DO', 'SUPPORT', and 'COMMUNITY', and buttons for 'Login' and 'Sign up'. The main content area features the article title 'BGP leaks and cryptocurrencies', the date '24 Apr 2018', and the author 'Louis Poinignon'. Below the title are social sharing buttons for LinkedIn, Facebook (with 'Like 739'), and Twitter. The article text begins with 'Over the few last hours, a dozen news stories have broken about how an attacker attempted (and perhaps managed) to steal cryptocurrencies using a BGP leak.' An illustration of a person in a dark hood and mask working at a computer monitor is positioned below the text. To the right of the main content is a sidebar with a search bar, a 'Categories' list with arrows, an email subscription form with a 'Subscribe to this blog' button, and contact information for US, UK, and Singapore callers.

BGP leaks and cryptocurrencies

24 Apr 2018 by Louis Poinignon.

[Share](#) [Like 739](#) [Tweet](#)

Over the few last hours, a dozen news stories have broken about how an attacker attempted (and perhaps managed) to steal cryptocurrencies using a BGP leak.

Categories

- Product News
- Security
- Performance
- Reliability
- Network
- Serverless
- International
- Cloudflare Apps

Enter your email address

Subscribe to this blog

US callers
1 (888) 99-FLARE

UK callers
+44 (0)20 3514 6970

Singapore callers
+65 3158 3954

Story 2/4

Authority DNS route hijack in April 2018.

This affected our DNS Resolver.

The route was sent to us on a Chicago peering session.

What should we do?

Story 3/4

At the time...

150+ PoPs, 26000 BGP sessions, IP space in 5 RIRs

Just the RIPE Validator^[1]

How to distribute a prefix list efficiently?

Story 4/4

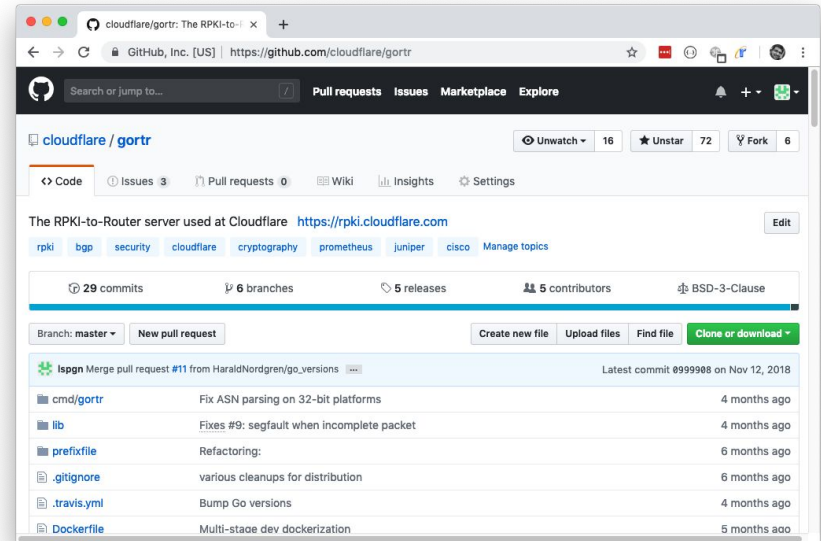
July: started deploying internally GoRTR.

August: open-source release.

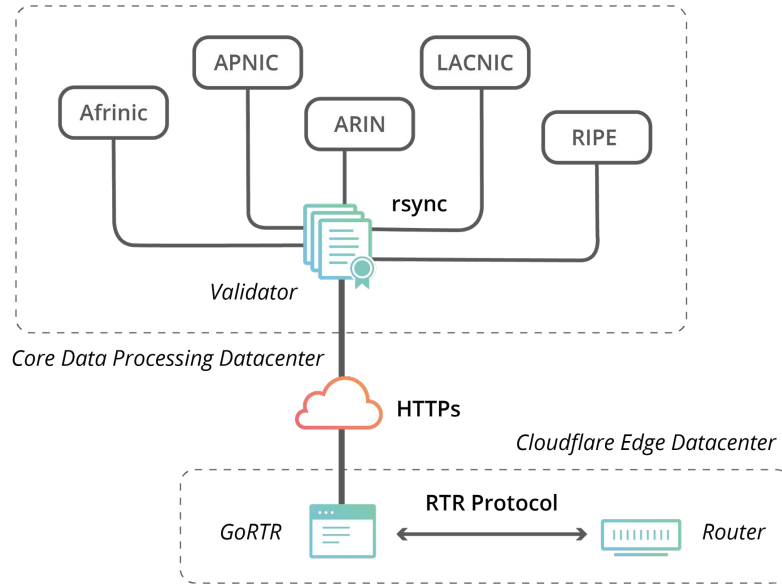
<https://github.com/cloudflare/gotr>

September → December:

- Turn up RTR sessions
- Signing prefixes



Diagram



Behind the scene (until January 2019)

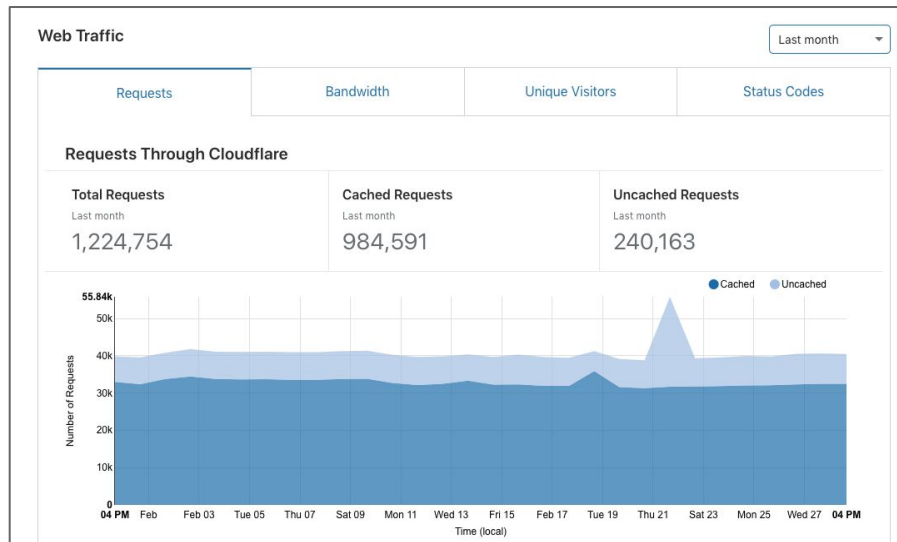
RIPE Validator providing list of prefixes.

Running in a Mesos cluster.

With a cronjob:

- Fetching the data
- Filtering it
(remove > /24 and > /48 and duplicates)
- Signing it
- Making it available to our edge.

<https://rpki.cloudflare.com/rpki.json> was born.



Effects

The question everyone asked us.

How much traffic was affected?

Many invalids. Little traffic in practice (default or valid less specific).

Except in one place. Few gigabits per seconds displaced due to geographical more specific.



<https://www.flickr.com/photos/thure/6287816628/>

Signing the routes

Signing the routes

IP space in 5 RIRs (*no twnic/jpnic/cnnic*).

Not a unified experience.

RIR	Features	Ease of use	API
AFRINIC	★	★	★
APNIC	★★	★★	★
ARIN	★★	★★	★★
LACNIC	★	★★★★	★
RIPE	★★★★	★★★★	★★★★

Rankings

Features: RRDP, 2 factors, extra info, CA.

Ease of use: steps to sign a ROA, multi user.

API: functional, complete and accessible.

Comparison - AFRINIC

Hard to set up: client TLS certificate to create (BPKI) in order to do RPKI.

Buggy.

No RRDP.

No API.

No auto-renew.

Hosted CA possible.

Extensive certificate informations.

Manage Your RPKI Resources

You can manage your RPKI resources from this page

RPKI Operations

- [List certificates](#)
- [View ROAs](#)
- [View Old ROAs](#)
- [Issue ROA](#)

Add ROA

*** Name:** Please enter a unique ROA name. Spaces will be replaced by '_'.

Your AS Numbers: Please select your ASN from this list or enter any other valid ASN in the field below.

*** AS Number:** ASN must be between 0 - 4294967295 in ASPLAIN format. "Reserved" and "Unallocated" ASNs will be rejected.

IPv4 address range: Please select your prefix in the drop down list and click the '+' button, then you can specify the details

IPv6 address range: Please select your prefix in the drop down list and click the '+' button, then you can specify the details

*** Not Valid Before (YYYY-MM-DD):**

*** Not Valid After (YYYY-MM-DD):**

Comparison - APNIC

Two factors or client certificate.

RRDP.

Auto-renew.

Allow BGP batch signing.

(slight bugs with big amount of prefixes).

Hosted CA possible.

Draft for API:

<https://www.apnic.net/manage-ip/apnic-services/services-roadmap/public-api-draft-for-members/>



The screenshot shows the APNIC Routes management interface. At the top, there is a "Routes" section with an information icon and the text: "Register your routes in MyAPNIC using the tool below. It will automatically create route objects for you. RPKI ROAs will also be created at the same time, if the ROA option is enabled (check the ROA status will not be updated until then)." Below this is an "Import routes" section with the text: "BGP announcements associated with your resources but not managed under this tool were found. Review & Import from BGP" and a "Dismiss" button. The bottom part of the screenshot shows a "Create route" modal form with the following fields and options:

- Prefix:** Route's prefix. E.g. 203.10.0.0/20
- Origin AS:** Route's origin. E.g. AS123
- Most specific announcement:** Route's most specific announcement. E.g. /22
- ROA:** Enabled
- Whois:** Enabled
 - Define Whois route attributes
- Options:** Notify additional contacts

At the bottom right of the modal are "Cancel" and "Next" buttons.

Comparison - ARIN

Two factors. Separate signing key.

No RRDP.

No auto-renew.

Semi-functional API (add).

Dashboard not easy to find.

Hosted CA possible.

Slow rsync update (4 times a day).

Some certificate information.



Create a Route Origin Authorization

[Browser Signed](#) [Signed](#)

* denotes required field

***ROA Name:**
Any name of your choosing.

***Origin AS:**
The AS Number you are authorizing.

***Start Date:**
The first date your ROA can be considered valid.

***End Date:**
The last date your ROA can be considered valid.

***Prefixes:**

The prefixes you authorize to originate from this AS.

***Private Key:**
This key will not be uploaded to ARIN.

Comparison - LACNIC

No two factors. Single user.

No RRDP.

No API.

Auto-renew opt-in.

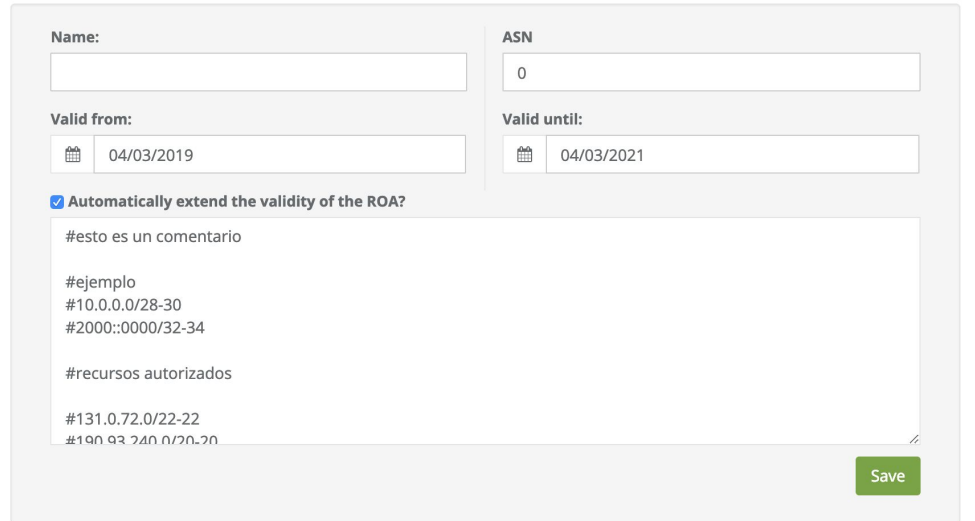
Allow BGP batch signing.

Based off RIPE.

No Hosted CA.

Some extra info (revoked, path).

Incorrect certificate encoding (BER). High turnover of certificate (few days).



The screenshot shows a web form with the following fields and options:

- Name:** An empty text input field.
- ASN:** A text input field containing the value "0".
- Valid from:** A date picker field showing "04/03/2019".
- Valid until:** A date picker field showing "04/03/2021".
- Automatically extend the validity of the ROA?**
- Comments:** A large text area containing the following text:

```
#esto es un comentario  
  
#ejemplo  
#10.0.0.0/28-30  
#2000::0000/32-34  
  
#recursos autorizados  
  
#131.0.72.0/22-22  
#190 93 240 0/20-20
```
- Save:** A green button located at the bottom right of the form.

Comparison - RIPE

Two factors.

RRDP.

Auto-renew.

Nice API.

Allow BGP batch signing.

No Hosted CA (theoretically).

No extra information. But history.

Incorrect certificate encoding (BER).

The screenshot shows the RIPE website's interface for managing Route Origin Authorisations (ROAs). At the top, there are three tabs: "BGP Announcements", "Route Origin Authorisations (ROAs)", and "History". A search bar is located to the right of the tabs. Below the tabs, there are several action buttons: "Discard Changes", "Delete ROAs", "Causing Problems", "Not Causing Problems", and a blue "+ New ROA" button. The main content area is a table with columns for "AS number", "Prefix", "Most specific length allowed", and "Affects". Below the table, there are input fields for "AS Number", "Prefix", and "Max length", along with a save icon and a refresh icon.

Automation

We automated prefixes adding on **ARIN and RIPE** with a **Salt state**.

Two secrets to store (API key and signing key).

Cannot delete or list via API for ARIN: very prone to mistakes if user wants to reduce the amount of ROA files.

```
def _format_payload(roas, signature):
    template = """-----BEGIN ROA REQUEST-----
{roas}
-----END ROA REQUEST-----
-----BEGIN SIGNATURE-----
{signature}
-----END SIGNATURE-----
"""
    payload = template.format(
        roas=roas, signature="\n".join(textwrap.wrap(signature, width=64))
    )
    return payload

def _make_roa(name, asn, t, start_val, end_val, prefix, length, maxlength):
    template = (
        '1|{time}|{name}|{asn}|{start_val}|{end_val}|{prefix}|{length}|{maxlength}|'
    )
    time_str = calendar.timegm(t.timetuple())
    start_val_str = start_val.strftime(_TIME_FORMAT)
    end_val_str = end_val.strftime(_TIME_FORMAT)
    roa = template.format(
        time=time_str,
        name=name,
        asn=asn,
        start_val=start_val_str,
        end_val=end_val_str,
        prefix=prefix,
        length=length,
        maxlength=maxlength,
    )
    return roa

def _sign(pkey, roas):
    signature = pkey.sign(roas.encode('utf-8'), padding.PKCS1v15(), hashes.SHA256())
    return base64.b64encode(signature).decode('utf-8')
```

Validator

Why making a validator?

First release of Routinator in November 2018.

We were still using RIPE Validator.

We wanted something more custom: with monitoring and RRDP.

By building it in Go:

- Many APIs and easy for concurrency
- Community doing cryptography
- Cloudflare uses Go a lot (cfssl, sidh, etc.)

Challenges

Juniper bugs: Routing Validation disabled.

Difficulties: rsync, BER encoded instead of DER, conditions in cryptography

```
3) a subjectPublicKeyInfo [RFC5280] in DER format [X.509],  
   encoded in Base64 (see Section 4 of \[RFC4648\]). To avoid long  
   lines, <CRLF> or <LF> line breaks MAY be inserted into the  
   Base64-encoded string.
```

```
where the URI section is comprised of one of more of the ordered  
sequence of:
```

Cloudflare's RPKI Toolkit

Sets of libraries and tools written in Go.

Including ***OctoRPKI*** 

Cloudflare's RPKI Toolkit

Libraries

- CER/ROA/MFT decoder
- PKI manager (exploring, validating)
- RRDP/rsync fetcher
- Validation of prefixes



Cloudflare's RPKI Toolkit

Software

- Local validator (without RRDp/Rsync)
- API tools for a distributed version without filesystem
- OctoRPKI
- Certificate Transparency tool

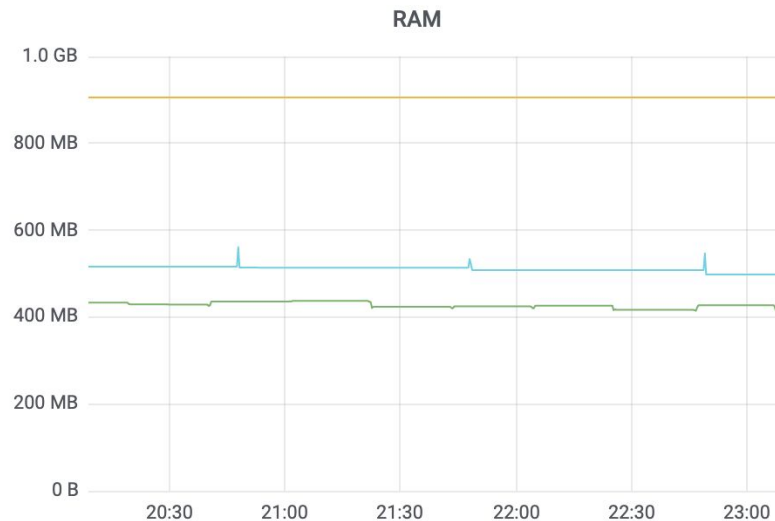
OctoRPKI - Features (1/2)

- Decodes TAL/CER/ROA/MFT
- Explore via Manifest or directory.
- RRDP support (and failover to Rsync)
- Monitoring (Prometheus and JSON API which includes logs)
- Dockerizeable
- Handle stability (generate file when done)

OctoRPKI - Features (2/2)

- Full compatibility with GoRTR (including signing the JSON file)
- Server + caching options for generated file (CDN friendly)
- Configuration options
 - Disable/Enable components
 - Modes (server, one-off)
- ~5-15 minutes for a full cold-start sync

OctoRPKI - Compute footprint

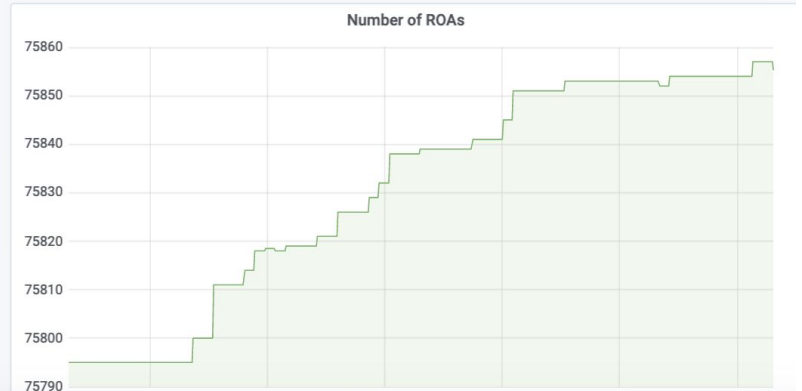
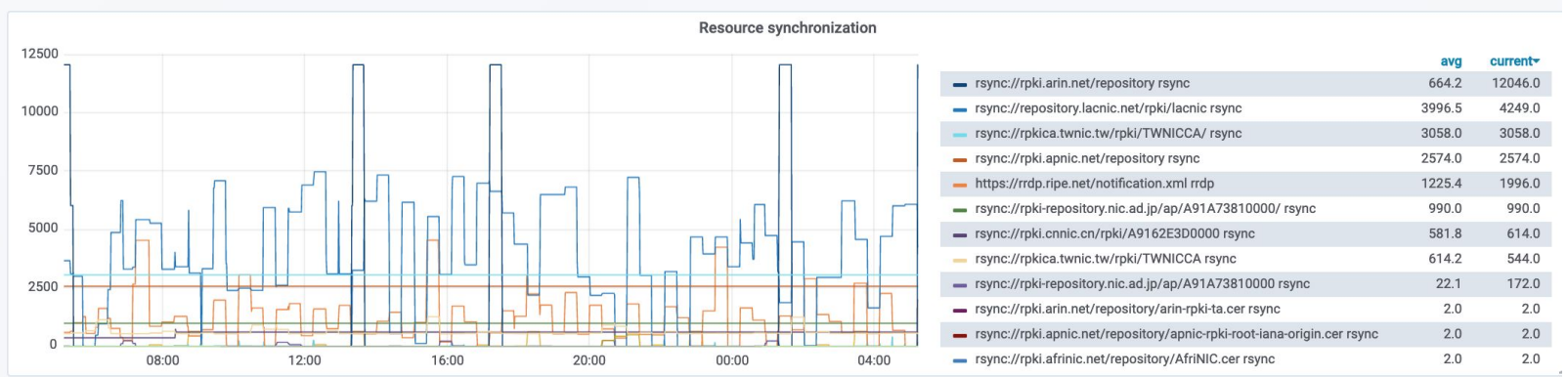


avg

rpk-benchmark-octorpi	428 MB
rpk-benchmark-ripe	906 MB
rpk-benchmark-routinator	511 MB

OctoRPKI v1.1.3
RIPE Validator v2.25
Routinator v3.3.0

Monitoring



```

INFO[0002] Rsync sync rsync://rpki.arin.net/repository/arin-rpki-ta.cer
INFO[0002] Rsync sync rsync://rpki.ripe.net/ta/ripe-ncc-ta.cer
INFO[0004] Rsync sync rsync://repository.lacnic.net/rpki/lacnic/rta-lacnic-rpki.cer
INFO[0007] Rsync sync rsync://rpki.afrinic.net/repository/AfriNIC.cer
ERRO[0012] Error exploring file: open cache/rpki.afrinic.net/repository/04E8B0D80F4D11E0B657D8931367AE7D/6ZgPOPXWxxu0sQa4vQZYUBLaMb
Y.mft: no such file or directory
ERRO[0012] Error exploring file: open cache/rpki.apnic.net/repository/838DB214166511E2B38C286172FD1FFZ/CSzKkN0Neo3ZmsZIX_g2EA3t6I.
mft: no such file or directory
ERRO[0012] Error exploring file: open cache/rpki.arin.net/repository/arin-rpki-ta/arin-rpki-ta.mft: no such file or directory
ERRO[0012] Error exploring file: open cache/repository.lacnic.net/rpki/lacnic/rta-lacnic-rpki.mft: no such file or directory
ERRO[0012] Error exploring file: open cache/rpki.ripe.net/repository/ripe-ncc-ta.mft: no such file or directory
INFO[0012] Still exploring. Revalidating now
INFO[0012] RRDp sync https://rrdp.apnic.net/notification.xml
INFO[0012] RRDp: Downloading root notification https://rrdp.apnic.net/notification.xml
INFO[0014] RRDp: https://rrdp.apnic.net/notification.xml Downloading snapshot at: https://rrdp.apnic.net/fa64523b-7381-4fda-9eb9-b1
233b30f503/83968/snapshot.xml
INFO[0064] RRDp sync https://rrdp.ripe.net/notification.xml
INFO[0064] RRDp: Downloading root notification https://rrdp.ripe.net/notification.xml
INFO[0064] RRDp: https://rrdp.ripe.net/notification.xml Downloading snapshot at: https://rrdp.ripe.net/8ab7553b-b124-4717-b20c-105a
da07476c/866/snapshot.xml
INFO[0177] Rsync sync rsync://repository.lacnic.net/rpki/lacnic
INFO[0241] Rsync sync rsync://rpki.arin.net/repository
INFO[0298] Rsync sync rsync://rpki.afrinic.net/repository
INFO[0309] Rsync sync rsync://rpki.apnic.net/repository
    
```

Validator

```

127.0.0.1:8080/infos
127.0.0.1:8080/output.json
127.0.0.1:8080/infos
[{"uri": "rsync://repository.lacnic.net/rpki/lacnic/rta-lacnic-rpki.cer",
  "file-count": 1,
  "iteration": 1,
  "errors": 0,
  "duration": 2.9613296,
  "last-fetch": 1550342002
},
{
  "uri": "rsync://rpki.afrinic.net/repository/AfriNIC.cer",
  "file-count": 1,
  "iteration": 1,
  "errors": 0,
  "duration": 4.3905323,
  "last-fetch": 1550342006
}
],
{
  "siana-rrdp": [
    {
      "uri": "https://rrdp.apnic.net/notification.xml",
      "file-count": 6734,
      "iteration": 1,
      "errors": 0,
      "duration": 52.0518939,
      "last-fetch": 15503420590,
      "rrdp-serial": 83968,
      "rrdp-sessionid": "fa64523b-7381-4fda-9eb9-b1233b30f503",
      "rrdp-last-file": "https://rrdp.apnic.net/fa64523b-7381-4fda-9eb9-
b1233b30f503/83968/snapshot.xml"
    }
  ],
  "uri": "r"
}
    
```

API

```

$ 
    
```



```

1: docker
INFO[0842] RRDP sync https://rrdp.apnic.net/notification.xml
INFO[0842] RRDP: Downloading root notification https://rrdp.apnic.net/notification.xml
INFO[0844] RRDP: https://rrdp.apnic.net/notification.xml has 0 deltas to parse (cur: 83980, last: 83980)
INFO[0844] RRDP: finished downloading https://rrdp.apnic.net/notification.xml. Last serial 83981
INFO[0844] RRDP sync https://rrdp.apnic.net/notification.xml
INFO[0844] RRDP: Downloading root notification https://rrdp.apnic.net/notification.xml
INFO[0845] RRDP: https://rrdp.apnic.net/notification.xml has -1 deltas to parse (cur: 83980, last: 83981)
INFO[0845] RRDP: finished downloading https://rrdp.apnic.net/notification.xml. Last serial 83981
INFO[0845] RRDP sync https://rrdp.ripe.net/notification.xml
INFO[0845] RRDP: Downloading root notification https://rrdp.ripe.net/notification.xml
INFO[0845] RRDP: https://rrdp.ripe.net/notification.xml has -1 deltas to parse (cur: 867, last: 868)
INFO[0845] RRDP: finished downloading https://rrdp.ripe.net/notification.xml. Last serial 868
INFO[0845] RRDP sync https://rpki.cnnic.cn/rrdp/notify.xml
INFO[0845] RRDP: Downloading root notification https://rpki.cnnic.cn/rrdp/notify.xml
INFO[0847] RRDP: https://rpki.cnnic.cn/rrdp/notify.xml has 0 deltas to parse (cur: 253274, last: 253274)
INFO[0847] RRDP: finished downloading https://rpki.cnnic.cn/rrdp/notify.xml. Last serial 253275
INFO[0847] Rsync sync rsync://rpki.arin.net/repository
INFO[0847] Rsync sync rsync://rpki.afnic.net/repository
INFO[0867] Rsync sync rsync://rpki.ripe.net/ta/ripe-ncc-ta.cer
INFO[0869] Rsync sync rsync://repository.lacnic.net/rpki/lacnic
INFO[0883] Rsync sync rsync://rpki-repository.nic.ad.jp/ap/A91A73810000
INFO[0885] Rsync sync rsync://rpki.ca.twnic.tw/rpki/TWNICCA
INFO[0885] Rsync sync rsync://rpki.cnic.cn/rrdp/notify.xml
INFO[1065] Stable state. Revalidating in 20m0s

```

```

1270.0.1:8080/output.json
1270.0.1:8080/output.json
1270.0.1:8080/metrics

{
  "counts": 76058,
  "generated": "1550346658",
  "valid": "1550346658",
  "signature": "3045022100b5db8f4bd478b418d6ef6ec55f68779ed723c63cfe705fb6e5b10db100220a27b6eae89bb8b845b481f7aa20ebf2fd2adfd04be1bcf7099522fa39e02e",
  "signatureDate": "3045022100f036e9cdf510c55ae28387a87fbdca15636f99c86f5e5af065c29514cf77e8c02202fcd4969b2c166b9e4c7cb2fb410ecad406f1c03d05024dec2ee71b9177da5",
  "roas": [
    {
      "prefix": "216.59.62.0/24",
      "maxLength": 24,
      "asn": "AS36167",
      "ta": ""
    },
    {
      "prefix": "91.204.174.0/20",
      "maxLength": 20,
      "asn": "AS197540",
      "ta": ""
    },
    {
      "prefix": "190.108.216.0/22",
      "maxLength": 24,
      "asn": "AS265751",
      "ta": ""
    },
    {
      "prefix": "186.179.112.0/20",
      "maxLength": 24,
      "asn": "AS27755",
      "ta": ""
    },
    {
      "prefix": "190.2.224.0/20",
      "maxLength": 24,
      "asn": "AS27755",
      "ta": ""
    },
    {
      "prefix": "200.3.200.0/21",
      "maxLength": 24,
      "asn": "AS27755",
      "ta": ""
    },
    {
      "prefix": "172.69.84.0/22",
      "maxLength": 22,
      "asn": "AS13335",
      "ta": ""
    },
    {
      "prefix": "77.74.76.0/24",
      "maxLength": 24,
      "asn": "AS206850",
      "ta": ""
    },
    {
      "prefix": "37.130.198.0/24",
      "maxLength": 24,
      "asn": "AS199386",
      "ta": ""
    },
    {
      "prefix": "37.130.199.0/24",
      "maxLength": 24,
      "asn": "AS199386",
      "ta": ""
    },
    {
      "prefix": "37.130.196.0/24",
      "maxLength": 24,
      "asn": "AS199386",
      "ta": ""
    },
    {
      "prefix": "37.130.197.0/24",
      "maxLength": 24,
      "asn": "AS199386",
      "ta": ""
    },
    {
      "prefix": "2a04:dc1::/32",
      "maxLength": 32,
      "asn": "AS199386",
      "ta": ""
    },
    {
      "prefix": "2a04:dc1::/32",
      "maxLength": 32,
      "asn": "AS199386",
      "ta": ""
    },
    {
      "prefix": "220.216.104.0/23",
      "maxLength": 24,
      "asn": "AS10010",
      "ta": ""
    },
    {
      "prefix": "185.132.68.0/22",
      "maxLength": 22,
      "asn": "AS203489",
      "ta": ""
    },
    {
      "prefix": "185.214.0.0/22",
      "maxLength": 22,
      "asn": "AS203489",
      "ta": ""
    },
    {
      "prefix": "2a0b:930b::/29",
      "maxLength": 29,
      "asn": "AS203489",
      "ta": ""
    },
    {
      "prefix": "132.247.56.0/24",
      "maxLength": 24,
      "asn": "AS278",
      "ta": ""
    },
    {
      "prefix": "192.188.33.0/24",
      "maxLength": 24,
      "asn": "AS23487",
      "ta": ""
    },
    {
      "prefix": "122.129.82.0/24",
      "maxLength": 24,
      "asn": "AS38264",
      "ta": ""
    },
    {
      "prefix": "122.129.83.0/24",
      "maxLength": 24,
      "asn": "AS38264",
      "ta": ""
    },
    {
      "prefix": "203.128.15.0/24",
      "maxLength": 24,
      "asn": "AS38264",
      "ta": ""
    },
    {
      "prefix": "203.128.16.0/24",
      "maxLength": 24,
      "asn": "AS38264",
      "ta": ""
    },
    {
      "prefix": "2600:9000:1044::/48",
      "maxLength": 48,
      "asn": "AS16509",
      "ta": ""
    },
    {
      "prefix": "185.154.128.0/24",
      "asn": "AS8059",
      "ta": ""
    },
    {
      "prefix": "185.154.130.0/24",
      "asn": "AS8059",
      "ta": ""
    },
    {
      "prefix": "185.154.129.0/24",
      "asn": "AS8059",
      "ta": ""
    },
    {
      "prefix": "185.154.131.0/24",
      "asn": "AS8059",
      "ta": ""
    },
    {
      "prefix": "185.154.128.0/24",
      "asn": "AS8059",
      "ta": ""
    },
    {
      "prefix": "185.252.128.0/22",
      "maxLength": 22,
      "asn": "AS8059",
      "ta": ""
    },
    {
      "prefix": "185.252.129.0/24",
      "maxLength": 24,
      "asn": "AS8059",
      "ta": ""
    },
    {
      "prefix": "2600:9000:20d5::/48",
      "maxLength": 48,
      "asn": "AS8059",
      "ta": ""
    }
  ]
}

```

ROA list

```

"counts": 76058,
"generated": "1550346658",
"valid": "1550346658",
"signature": "3045022100b5db8f4bd478b418d6ef6ec55f68779ed723c63cfe705fb6e5b10db100220a27b6eae89bb8b845b481f7aa20ebf2fd2adfd04be1bcf7099522fa39e02e",
"signatureDate": "3045022100f036e9cdf510c55ae28387a87fbdca15636f99c86f5e5af065c29514cf77e8c02202fcd4969b2c166b9e4c7cb2fb410ecad406f1c03d05024dec2ee71b9177da5",
"roas": [
  {
    "prefix": "216.59.62.0/24",
    "maxLength": 24,
    "asn": "AS36167",
    "ta": ""
  },
  {
    "prefix": "91.204.174.0/20",
    "maxLength": 20,
    "asn": "AS197540",
    "ta": ""
  },
  {
    "prefix": "190.108.216.0/22",
    "maxLength": 24,
    "asn": "AS265751",
    "ta": ""
  },
  {
    "prefix": "186.179.112.0/20",
    "maxLength": 24,
    "asn": "AS27755",
    "ta": ""
  },
  {
    "prefix": "190.2.224.0/20",
    "maxLength": 24,
    "asn": "AS27755",
    "ta": ""
  },
  {
    "prefix": "200.3.200.0/21",
    "maxLength": 24,
    "asn": "AS27755",
    "ta": ""
  },
  {
    "prefix": "172.69.84.0/22",
    "maxLength": 22,
    "asn": "AS13335",
    "ta": ""
  },
  {
    "prefix": "77.74.76.0/24",
    "maxLength": 24,
    "asn": "AS206850",
    "ta": ""
  },
  {
    "prefix": "37.130.198.0/24",
    "maxLength": 24,
    "asn": "AS199386",
    "ta": ""
  },
  {
    "prefix": "37.130.199.0/24",
    "maxLength": 24,
    "asn": "AS199386",
    "ta": ""
  },
  {
    "prefix": "37.130.196.0/24",
    "maxLength": 24,
    "asn": "AS199386",
    "ta": ""
  },
  {
    "prefix": "37.130.197.0/24",
    "maxLength": 24,
    "asn": "AS199386",
    "ta": ""
  },
  {
    "prefix": "2a04:dc1::/32",
    "maxLength": 32,
    "asn": "AS199386",
    "ta": ""
  },
  {
    "prefix": "2a04:dc1::/32",
    "maxLength": 32,
    "asn": "AS199386",
    "ta": ""
  },
  {
    "prefix": "220.216.104.0/23",
    "maxLength": 24,
    "asn": "AS10010",
    "ta": ""
  },
  {
    "prefix": "185.132.68.0/22",
    "maxLength": 22,
    "asn": "AS203489",
    "ta": ""
  },
  {
    "prefix": "185.214.0.0/22",
    "maxLength": 22,
    "asn": "AS203489",
    "ta": ""
  },
  {
    "prefix": "2a0b:930b::/29",
    "maxLength": 29,
    "asn": "AS203489",
    "ta": ""
  },
  {
    "prefix": "132.247.56.0/24",
    "maxLength": 24,
    "asn": "AS278",
    "ta": ""
  },
  {
    "prefix": "192.188.33.0/24",
    "maxLength": 24,
    "asn": "AS23487",
    "ta": ""
  },
  {
    "prefix": "122.129.82.0/24",
    "maxLength": 24,
    "asn": "AS38264",
    "ta": ""
  },
  {
    "prefix": "122.129.83.0/24",
    "maxLength": 24,
    "asn": "AS38264",
    "ta": ""
  },
  {
    "prefix": "203.128.15.0/24",
    "maxLength": 24,
    "asn": "AS38264",
    "ta": ""
  },
  {
    "prefix": "203.128.16.0/24",
    "maxLength": 24,
    "asn": "AS38264",
    "ta": ""
  },
  {
    "prefix": "2600:9000:1044::/48",
    "maxLength": 48,
    "asn": "AS16509",
    "ta": ""
  },
  {
    "prefix": "185.154.128.0/24",
    "asn": "AS8059",
    "ta": ""
  },
  {
    "prefix": "185.154.130.0/24",
    "asn": "AS8059",
    "ta": ""
  },
  {
    "prefix": "185.154.129.0/24",
    "asn": "AS8059",
    "ta": ""
  },
  {
    "prefix": "185.154.131.0/24",
    "asn": "AS8059",
    "ta": ""
  },
  {
    "prefix": "185.154.128.0/24",
    "asn": "AS8059",
    "ta": ""
  },
  {
    "prefix": "185.252.128.0/22",
    "maxLength": 22,
    "asn": "AS8059",
    "ta": ""
  },
  {
    "prefix": "185.252.129.0/24",
    "maxLength": 24,
    "asn": "AS8059",
    "ta": ""
  },
  {
    "prefix": "2600:9000:20d5::/48",
    "maxLength": 48,
    "asn": "AS8059",
    "ta": ""
  }
]

```

```

$ cat output.json | jq '.roas | length'
76058

```

OctoRPKI - Run it yourself

```
$ docker run -ti \  
  -p 8080:8080 \  
  -v $PWD/cache:/cache \  
  -v $PWD/tals/arin.tal:/tals/arin.tal \  
  cloudflare/octorpci
```

Container image

Adding ARIN TAL

Use cache folder
on host

Open port 8080 on host

GoRTR

OctoRPKI does not embed a RTR server. Modular and independence!

Fully compatible with **GoRTR** <https://github.com/cloudflare/gortr>

Signs the prefix list to ensure a safe distribution of the file.

Can run natively on Juniper!

```
$ docker run -ti \  
  -p 8082:8082 \  
  -v $PWD/example.pub:/example.pub \  
  cloudflare/gortr \  
  -verify.key /example.pub \  
  -cache https://YOUR_ROA_URL
```


GoRTR

Only software to support **plaintext**, **SSH** and **TLS**.

Future plans:

an open RTR service

available in our 160+ PoPs

Compatibility matrix

A simple comparison between software and devices. Implementations on versions may vary.

Device/software	Plaintext	TLS	SSH	Notes
RTRdump	Yes	Yes	Yes	
Juniper	Yes	No	No	
Cisco	Yes	No	Yes	Only SSH password
Alcatel	Yes	No	No	
Arista	No	No	No	
FRRouting	Yes	No	Yes	Only SSH password
Bird	Yes	No	Yes	Only SSH key
Quagga	Yes	No	No	

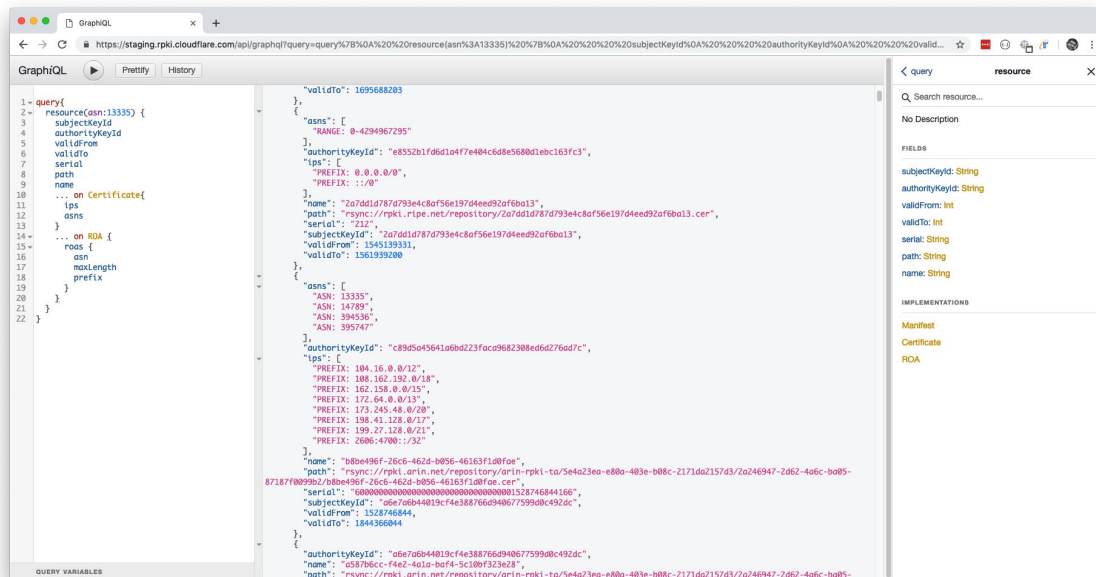
Cloudflare's Internal Version

Is providing:

<https://rpki.cloudflare.com/rpki.json>

But also a **GraphQL** API

...which powers a
dashboard



The screenshot shows a GraphQL query in a browser's developer console. The query is a complex nested query with aliases for 'Certificate', 'ROA', and 'asn'. The response is a large JSON object containing detailed information about a resource, including its ID, various keys, and lists of IP addresses and ASNs.

```
1 query {
2   resource(asn:13335) {
3     subjectKeyId
4     authorityKeyId
5     validFrom
6     validTo
7     serial
8     path
9     name
10    ... on Certificate {
11      ips
12      asns
13    }
14    ... on ROA {
15      roas {
16        asn
17        maxLength
18        prefix
19      }
20    }
21  }
22 }
```

The response JSON includes fields like 'validTo', 'asns', 'range', 'authorityKeyId', 'ips', 'name', 'path', 'serial', 'subjectKeyId', 'validFrom', 'roas', and 'asn'. It also includes a 'Manifest' section with 'Certificate' and 'ROA' entries.

Dashboard

RPKI Dashboard

TRUST ANCHOR: All KEY ID: PREFIX: 1.1.0.0/24 ASN: Enter an AS number

Resource List Hierarchical View

Showing 5 certificates and 0 ROAs

Certificates

Key	Name	Trust Anchor	ASNs
e8552b1fd6d1a4f7e404c6d8e5680d1ebc163fc3	ripe-ncc-ta	RIPE	0-429496
fc8a9cb3ed184e17d30eea1e0fa7615ce4b1af47	root trust anchor O=lacnic	LACNIC	0-429496
0b9cca90dd0d7a8a37666b19217fe0d84037b7a2	apnic-rpki-root-iana-origin	APNIC	1-429496
eb680f38f5d6c71bb4b106b8bd06585012da31b6	AfriNIC-Root-Certificate	Afrinic	0-429496

RPKI Dashboard

TRUST ANCHOR: All KEY ID: PREFIX: 1.1.0.0/32 ASN: Enter an AS number

Resource List Hierarchical View Address Space View

Found 2 ROAs and 9 certificates

ROAs

ASN	Prefix	Max Length	IP Family	Trust Anchor	Emitted	Expiration
AS13335	1.0.0.0/24	/24	IPv4	APNIC	3/16/2018	in 2 years

Name: 5aabf815-9744
Trust Anchor: APNIC
Key: aa24090e86c3bc39ee7ac345b3bf9a38cd9ff3ad
Parent Key: 68faf9dace19768cac3d4ed7bb24372bffa6d018
Path: rsync://rpki.apnic.net/member_repository/A91872ED/ED8C96901D6C11E28A38A3AD08B02CD2/797B4DEC293B11E8B187196DC4F9AE02.roa
Validity: Fri, 16 Mar 2018 17:00:05 GMT - Wed, 31 Mar 2021 00:00:00 GMT
Emitted: Fri, 16 Mar 2018 17:00:05 GMT
ASN: 13335
Prefix: 1.0.0.0/24
Max Length: /24

APNIC

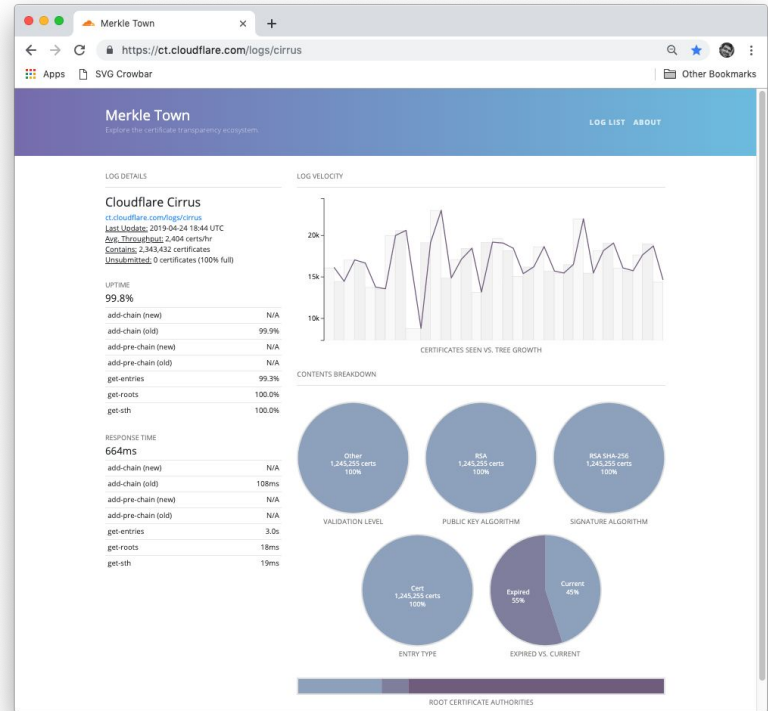
Certificate ROA

Certificate Transparency

Historical records of certificates.

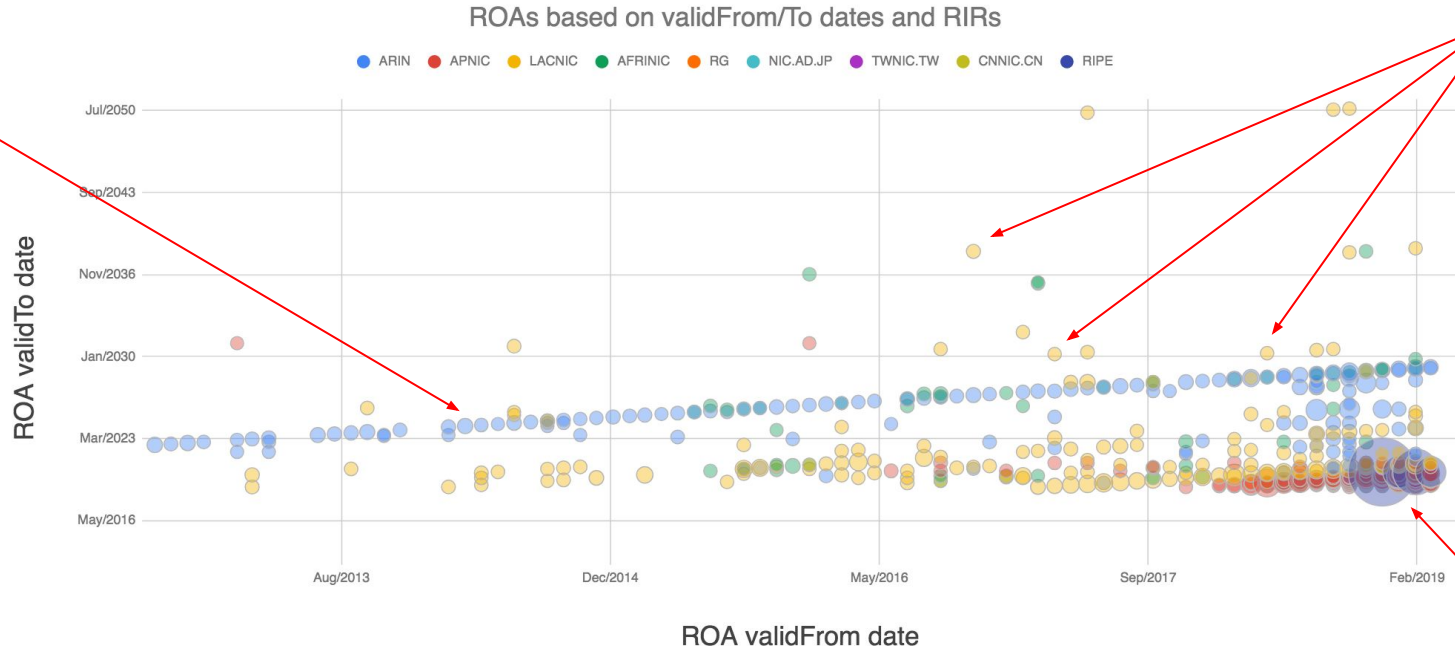
Contains a chain.

Sent by our validator.



Other data - so how fresh are those ROAs?

ARIN uses
ten year
expire



LACNIC
random
expires

RIPE regenerates
certificates!

Future projects or ideas

RPKI validation tester using our CDN:

- Using a /23 (/47 IPv4) valid and a /24 (/48 IPv6) invalid

Certificate encoder

ASPA

More toolings and visualizations around RPKI (BGP collection)

Thank you / Gracias / Obrigado

Questions?

louis@cloudflare.com
[@lpoinSIG](https://twitter.com/lpoinSIG) (twitter)

