SALOTTINO

May 24, **2022**

An opinionated review of RPKI validators

and the state of their Debian packaging

Marco d'Itri

Network Manager Seeweb

An opinionated review of RPKI validators

and the state of their Debian packaging

Marco d'Itri
`<md@seeweb.it>`
@rfc1036

Seeweb s.r.l.

Salottino del MIX - 24 maggio 2022

Content

1. A review of RPKI validators

2. The state of RPKI software in Debian

Content

1. A review of RPKI validators

2. The state of RPKI software in Debian

The software (1)

Validators

- Routinator
- OpenBSD's rpki-client
- ~~RIPE NCC RPKI Validator~~ (discontinued)
- OctoRPKI (not actively developed)
- FORT Validator (not actively developed)
- Prover

The software (2)

OctoRPKI and rpki-client do not implement the RPKI-to-router (RTR) protocol themselves, but use an external daemon.

RTR servers

- ~~gortr~~ (abandoned)
- stayrtr

stayrtr is an actively maintained fork of gortr and it looks like it will replace it.

Usage of validation software

Routinator	69.98%
rpki-client	19.30%
RIPE NCC Validator	4.37%
OctoRPKI	3.53%
FORT Validator	3.23%
rpki-prover	0.52%

This data was gathered by Job Snijders by counting the unique IPs accessing a RRDP web server.

Routinator

Pros

- Actively developed, support contracts available.
- Well documented.

Cons

- Impossible to package by distributions.

Developed in Rust by NLnet Labs.

rpki-client

Pros

- Actively developed by network operators.
- Simple and essential.
- Separation of privileges in multiple processes.

Cons

- Needs a third party RTR daemon.

Developed in C by the OpenBSD project.

RIPE NCC Validator

Pros

- Nothing else was available at the time?

Cons

- Written in Java.
- RIPE NCC stopped development.
- End of support in June 2021: **nobody should use it anymore!**

Developed in Java by RIPE NCC.

OctoRPKI

Pros

- Simple and essential.

Cons

- Not developed anymore except for security fixes since the original author left Cloudflare.
- Needs a third party RTR daemon.

Developed in Go by Cloudflare.

FORT Validator

Pros

- Used to be actively developed.
- Well documented.
- Good middle ground of features and complexity.

Cons

- Has lost funding, future unclear.

Developed in C by LACNIC and NIC.MX.

rpki-prover

Pros

- ?

Cons

- ?
- Very few networks use it.

Developed in Haskell by Mikhail Puzanov.

Should I package it?

My suggestions

Use two of:

- Routinator
- FORT Validator
- rpki-client + stayrtr

They are all good and have different tradeoffs.

Using software packaged by a Linux distribution significantly reduces the system administration effort and allows to adopt diverse implementations.

Content

1. A review of RPKI validators

2. The state of RPKI software in Debian

Debian for network operators

Debian GNU/Linux is the one stop shop for all your RPKI validation needs.

My goals

- Packages with sane defaults which just work after being installed.
- Common management of TALs in the `rpki-trust-anchors` package.
- State of the art security with systemd sandboxing.

Issues

- The RPKI ecosystem is still young and fast moving for a stable distribution.
- Routinator cannot be packaged.

seeweb

The issue with Routinator

The Rust development ecosystem is broken and hostile to distributions

- APIs are not stable and there is no dynamic linking.
- Hence it is common for Rust software to depend on specific versions of libraries.
- General *vendoring* of dependencies is not acceptable to the Debian security team.
- Maintaining multiple versions of libraries in the distribution is too much time consuming (and not appreciated either...).
- Rust programs would depend on different versions of the same library.
- **There is no practical way to package complex Rust projects.**

The Routinator developers publish a Debian package which nowadays is good enough, but it does not use `rpki-trust-anchors`.

The state of Debian RPKI packages

Package	Debian 11	Debian testing	Ubuntu 22.04
`routinator`	✗	✗	✗
`rpki-client`	(old)	✓	✓(7.6)
`cfrpki`	✓	✓	✓
`fort-validator`	✓	✓	✓
`gortr`	✓	✓	✓
`stayrtr`	✗	✓	✓
`rpki-trust-anchors`	✓	✓	✓

`rpki-client` could not be updated in stable because it depends on `libretls`.
`stayrtr` is not in Debian 11, but `gortr` still works fine.

Ubuntu 22.04 LTS is good right now but the packages will probably not be updated over its life.

Backports to Debian/stable

Backported packages of `rpki-client` will be maintained in the official Debian backports archive until the release of Debian 12.

```
echo 'deb http://deb.debian.org/debian bullseye-backports main' \
  > /etc/apt/sources.list.d/bullseye-backports.list
apt update
apt install rpki-client/bullseye-backports
```

I plan to backport other RPKI-related packages too if and when it will be needed.

Any questions?

`https://www.linux.it/~md/text/rpki-validators-mix2022.pdf`

(Google . . . Marco d'Itri . . . I feel lucky)