Cascade

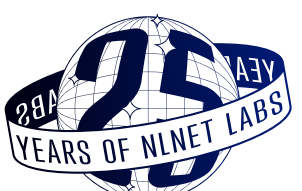
A DNSSEC signer you can trust

Maarten Aertsen NLnet Labs


Non-profit
purveyors of fine
'roads and bridges'
for the Internet
since 1899

Roads and bridges? DNS and Routing

Terms inspired by "Roads and Bridges: The Unseen Labor Behind Our Digital Infrastructure" by Nadia Eghbal



Outline

1. Introduction
2. Requirements
3. Architecture
4. What’s Next

News from NLnet *Labs*

We’re developing many new projects in Rust

Dedicated 2024 to **domain**, our Rust-based DNS library

Now we can write sophisticated DNS applications in Rust!

An end of life for OpenDNSSEC (Oct 2027)

We’ve developed OpenDNSSEC for the last 15 years

It’s served the community beyond our wildest dreams

Now, operators are telling us that they need more

So we interviewed them…

Surveyed: How do operators feel?

- Signers are uncommunicative
- Can’t trust them to do anything
- Even daily routines are a hassle
- Things could fall apart at any time

Introducing Cascade

Introducing Cascade

Purpose-built DNSSEC signer, written in Rust

Built from scratch with the same expertise

Tailored for today's DNS operators – you!

Earlier this month at DNS-OARC:

Released an alpha version of Cascade

Production-ready release in the first half of 2026

End-of-life for OpenDNSSEC announced on Oct 3rd

Designing Cascade

Designing Cascade

Prime Directive: Listen to the users!

How do operators feel?

- Signers are uncommunicative
- Can’t trust them to do anything
- Even daily routines are a hassle
- Things could fall apart at any time

Building something you can trust

Building something you can trust

Cascade

Communicates how it's doing

Detailed, per-zone status output

Doesn't assume your feelings

Review zones before publishing

Is open to your needs

Manually control every step

Helps you with chores

Good support for MS, HA setups

… and so much more

Easy to interact with

CLI, REST API; Web UI coming soon

Good at doing the right thing

Well-tested defaults at every level

Flexible enough to fit you

Systemd, Prometheus, containerization

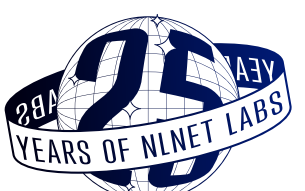
Backed with professional support

Contracts under SLA for operators of critical infrastructure.

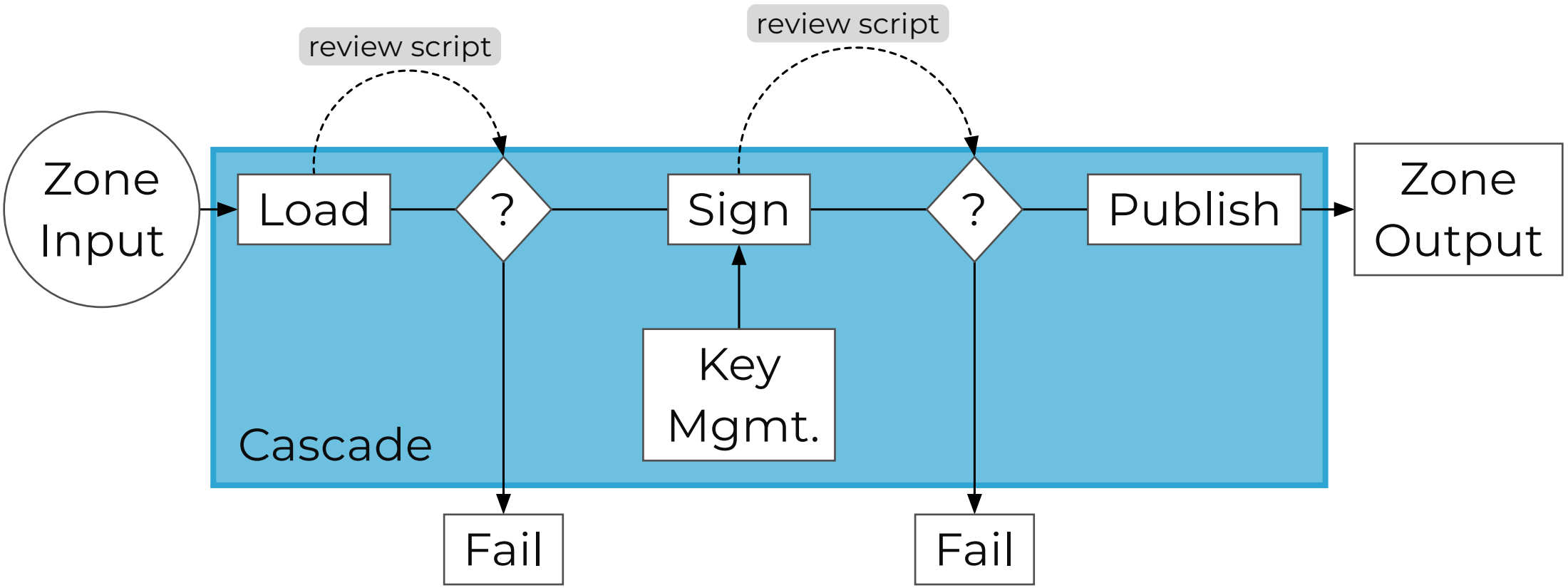
So what did we build?

So what did we build?

- A DNSSEC signer and key manager
- First-class support for zone review / approval
- An HTTP API for controlling every component
- An architecture around the signing pipeline
- Comprehensive status output via the CLI/API



So what did we build?



Cascade's per-zone pipeline.

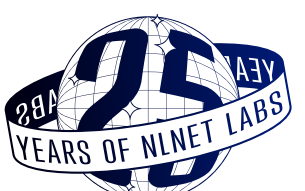
What's next?

What do you think? How can we support you better?

Come talk to us, so we can understand your needs

Expect a production-ready release in early 2026

But first, a quick detour...



But first, a quick detour...

Help us to help you replace OpenDNSSEC

Fund sustainable long-term open source development

NLnet *Labs* is a non-profit

Support contracts sustain our projects

Large up-front investment ahead of Cascade's production release

Initial investment from our reserves

Strategic but non-sustainable investment to replace OpenDNSSEC

Actively looking for initial co-funding

We are talking to STA, Nominet, but could use more help

Thank you!

We’re in touch about Cascade with about 20 of you

… but there’s many more running OpenDNSSEC today.

Let us know what your TLD needs.

Follow development

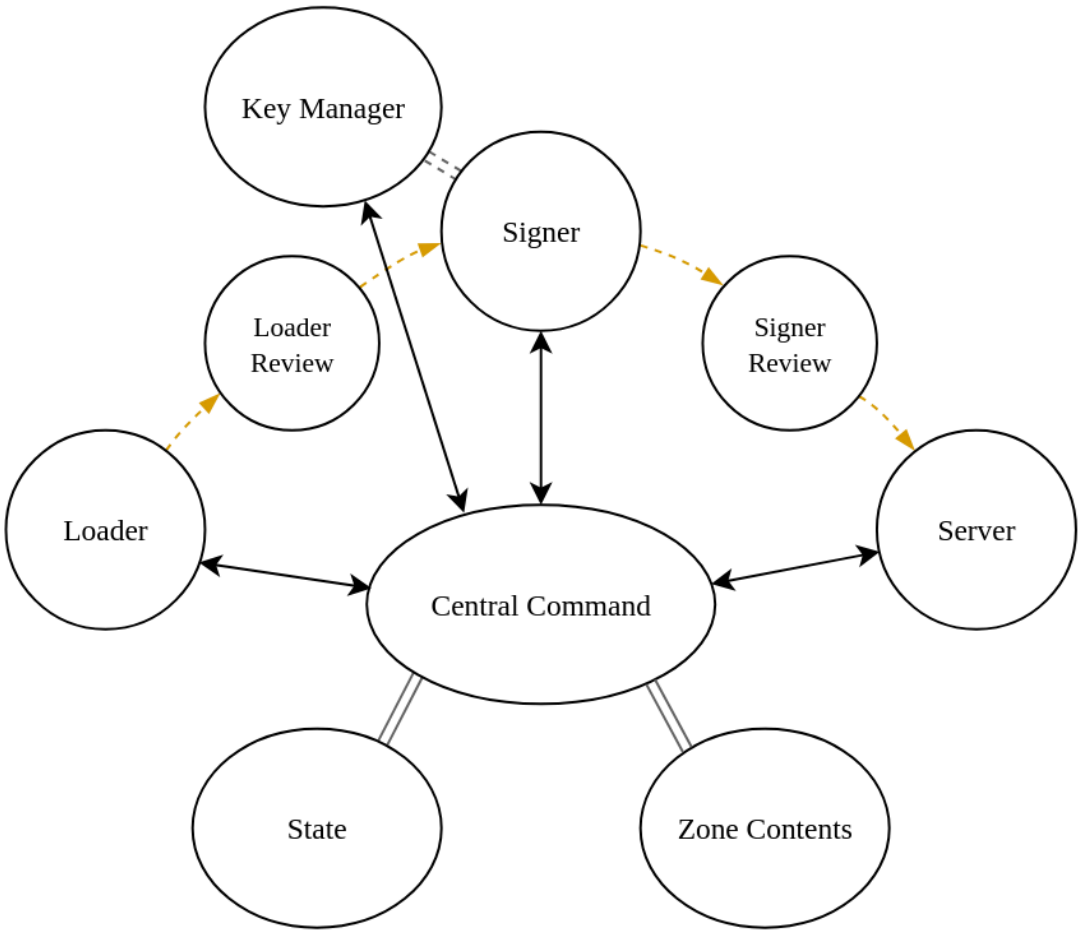
vision
blog.nlnetlabs.nl/cascade

source (Github)
NLnetLabs/cascade

docs
cascade.docs.nlnetlabs.nl

cascade@nlnetlabs.nl

Auxiliary slides



Cascade’s overall architecture.

Cascade tells you what it’s doing

Load

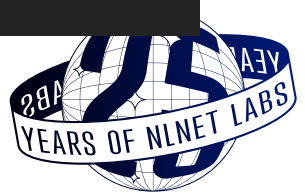
```
jannik@rusty:/srv/cascade$ ./bin/cascade zone status cascade.nlnetlabs.nl
Status report for zone 'cascade.nlnetlabs.nl' using policy 'cascade'
✔ Waited for a new version of the cascade.nlnetlabs.nl zone
✔ Loaded version 3
  Loaded at 2025-10-14T14:49:15+00:00 (6days 21h 39m 3s ago)
  Loaded 290 B and 5 records from the filesystem in 0 seconds
✔ Waited for approval to sign version 3
```

Review hooks

```
#!/usr/bin/env sh

set -e

logger -p daemon.notice -t cascade "Validating ${CASCADE_ZONE} of serial ${CASCADE_SERIAL} from ${CASCADE_SERVER}"

# Using `validns` to check the unsigned zone
# and `dnssec-verify` to check the signed zone
# Unfortunately, dig logs some errors on standard output... Nothing to do there
dig @${CASCADE_SERVER_IP} -p ${CASCADE_SERVER_PORT} "${CASCADE_ZONE}" AXFR | \
    if [ "$1" = "unsigned" ]; then
        # validns does not handle Ed25519
        validns -z "${CASCADE_ZONE}" -p all -
    else
        dnssec-verify -q -o "${CASCADE_ZONE}" /dev/stdin
    fi
```

Sign

```
✔ Approval received to sign version 3, signing requested
✔ Signed version 3 as version 2025101401
  Signing requested at 2025-10-14T14:49:16+00:00 (6days 21h 39m 3s ago)
  Signing started at 2025-10-14T14:49:16+00:00 (6days 21h 39m 3s ago)
  Signing finished at 2025-10-14T14:49:16+00:00 (6days 21h 39m 3s ago)
  Collected 5 records in 0s, sorted in 0s
  Generated 4 NSEC(3) records in 0s
  Generated 6 signatures in 0s (6 sig/s)
  Inserted signatures in 0s (6 sig/s)
  Took 0s in total, using 1 threads
  Current action: Finished
✔ Waited for approval to publish version 2025101401
```



Publish

```
✔ Published version 2025101401
  Published zone available on 127.0.0.1:1053
```

Key usage?

```
jannik@rusty:/srv/cascade$ ./bin/cascade zone status --detailed cascade.nlnetlabs.nl
Status report for zone 'cascade.nlnetlabs.nl' using policy 'cascade'
```

```
DNSSEC keys:
  ZSK tagged 64727:
    Reference: kmip://softhsm/keys/2AF59DCEEBEF088702837E66613F875F5026D5A9_pub?algorithm=13&flags=256
    Actively used for signing
  KSK tagged 4215:
    Reference: kmip://softhsm/keys/1B938AF32D4CD4AD7EFC4532F54828FBC38B5781_pub?algorithm=13&flags=257
    Actively used for signing
  Details:
    key kmip://softhsm/keys/2AF59DCEEBEF088702837E66613F875F5026D5A9_pub?algorithm=13&flags=256 expires at 2025-11-06T14:52:11Z
    key kmip://softhsm/keys/1B938AF32D4CD4AD7EFC4532F54828FBC38B5781_pub?algorithm=13&flags=257 expires at 2026-10-07T14:52:11Z
```