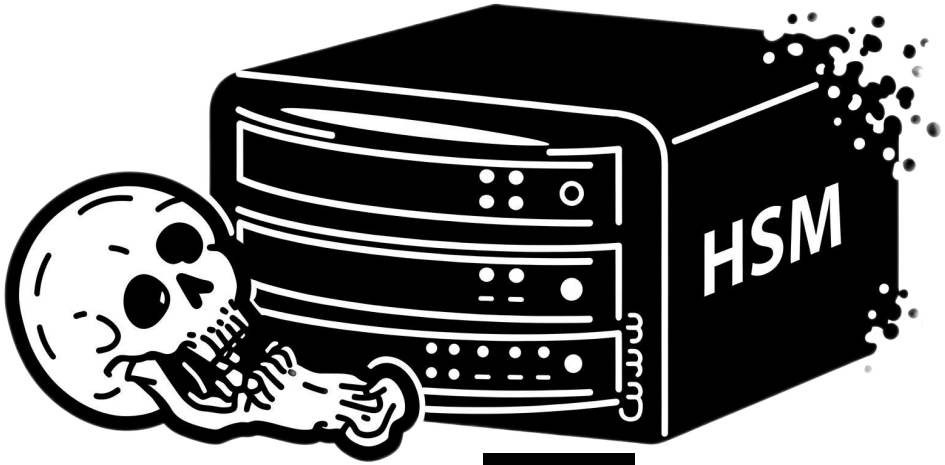
Sketch from a re-design of a multi-signer environment

ICANN DNSSEC & Security Workshop
June 2025

Felipe Agnelli Barbosa
InternetNZ

The demand



EOL

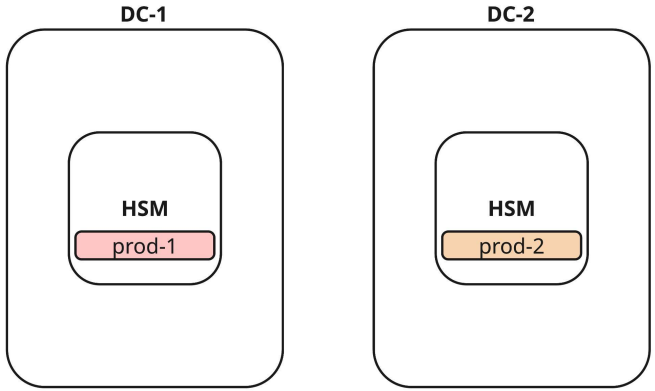
Work to do

- HSMs replacement
- Signers from scratch
- ~~Primaries from scratch~~

Current design

HSMs

- AEP Keyper Plus
- 10 years old
- ECC alg support(~950 tps)
  (ECDSA, ECDH)
- 2 standby HSMs
- Different key for each zone in each site



Signers

- OpenDNSSEC 1.4.14
- Ubuntu 14.04
- Bind 9.10.8
- Perl and Shell scripts
- 1 VM and 1 Server
- Manual key rollovers
- Documentation?

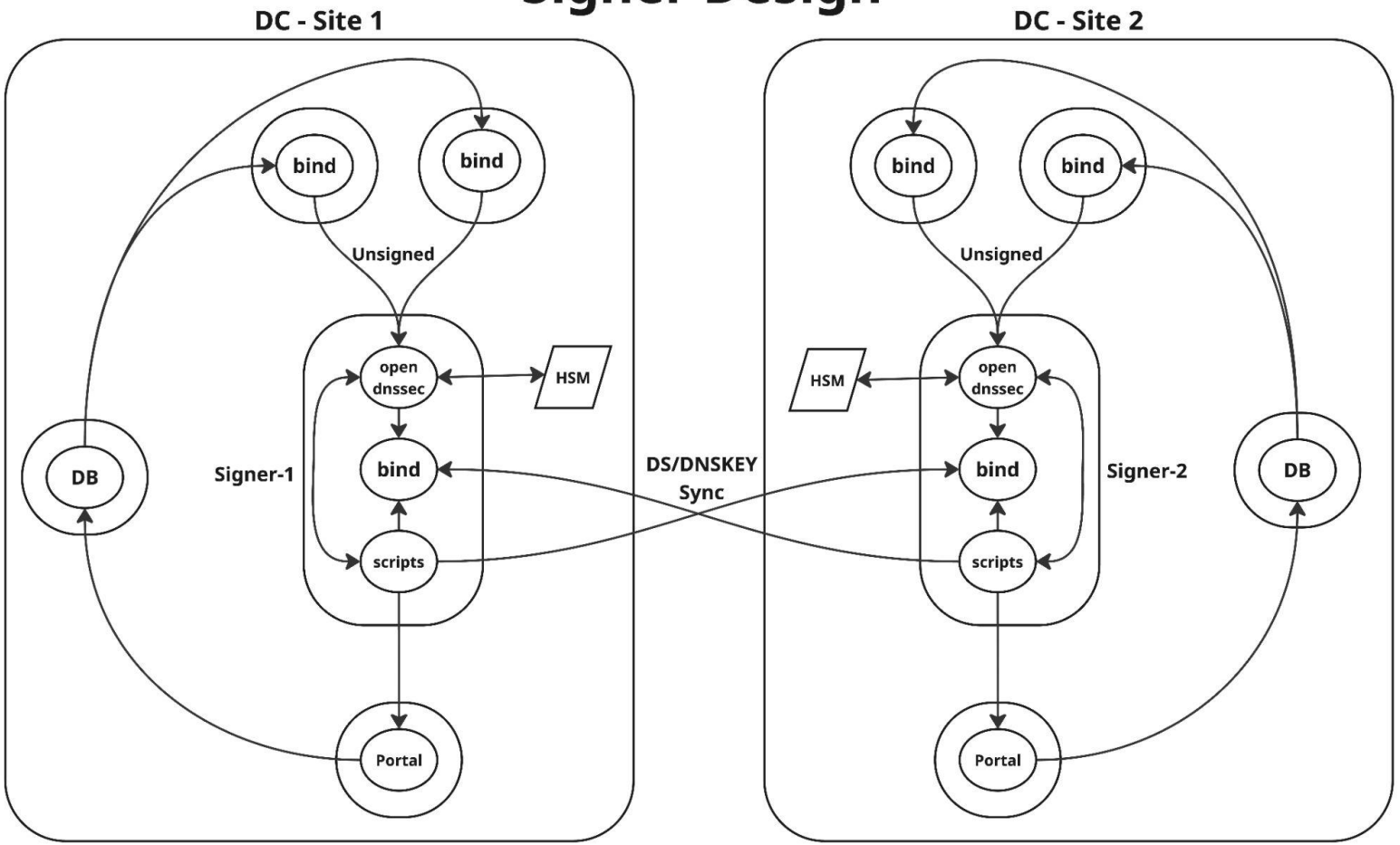
Multi-signer operations

- DS and DNSKEY synchronization
- DS and DNSKEY injection/removal
- Monitoring(Naemon + FakeRoot + Thousand eyes + Ripe atlas)
- SOPs
  - Backup/Restore
  - Key Rollovers
  - Signer Site Switch
- Stage and Prod environments(in different locations)
- Manual key rollovers(ZSK and KSK)

Multi-signer operations

- Sync(DS and DNSKEY) every 5 minutes
  - Shell script collects DS/DNSKEY from OpenDNSSEC
    - Creates DNS zones with that data
    - The other Signer does the same and keep it in a cycle
  - Perl script collect DS/DNSKEY data from Bind
    - Build a file with all that records on both signers
    - This file is used as source of truth for injection/removal/monitoring

Signer Design



New design

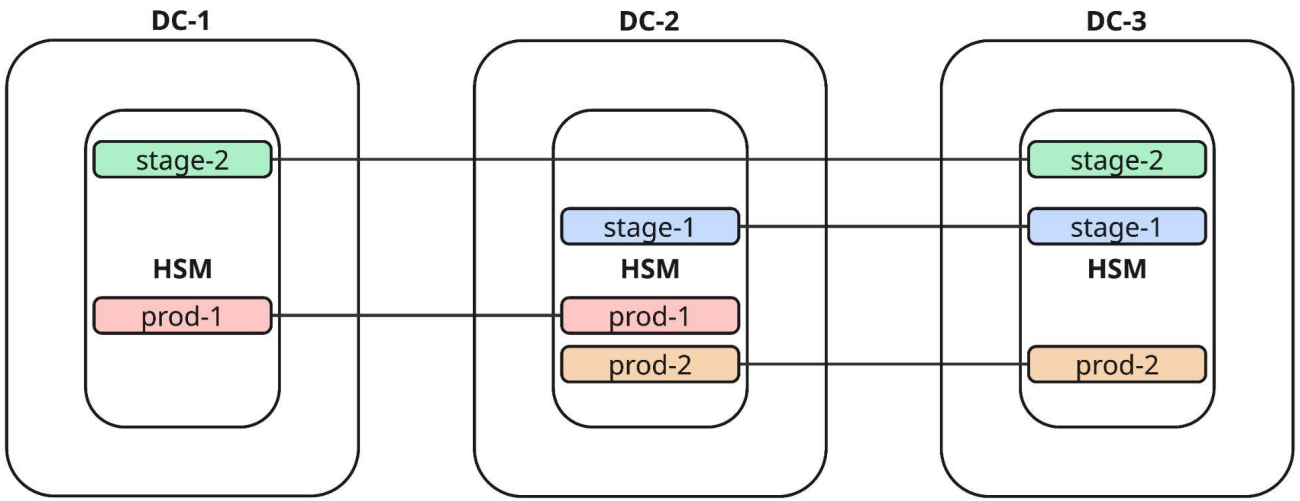
Community-driven insights

SIDN, Internetstiftelsen, DENIC and a few others

HSMs

- Thales Luna 7 S750
- ECC alg support(~10k tps)

  (ECDSA, ED25519, ECDH, ECIES)
- Backup devices
- Remote access devices
- High-Availability Groups
- Partition per environment
- Break glass access


DC-1
DC-2
DC-3
stage-2
HSM
prod-1
stage-1
HSM
prod-1
prod-2
stage-2
stage-1
HSM
prod-2

Premises

- Split the "signer" work into more processes
- Ability to operate without registry DB
- Remove interaction between signer and portal
- Increase troubleshooting capacity
- Increase validation capacity (unsigned and signed)
- Ease the management of signed zones for primaries
- Ability to store signed zones for auditing/forensics
- Automatic key rollovers (ZSK and KSK)

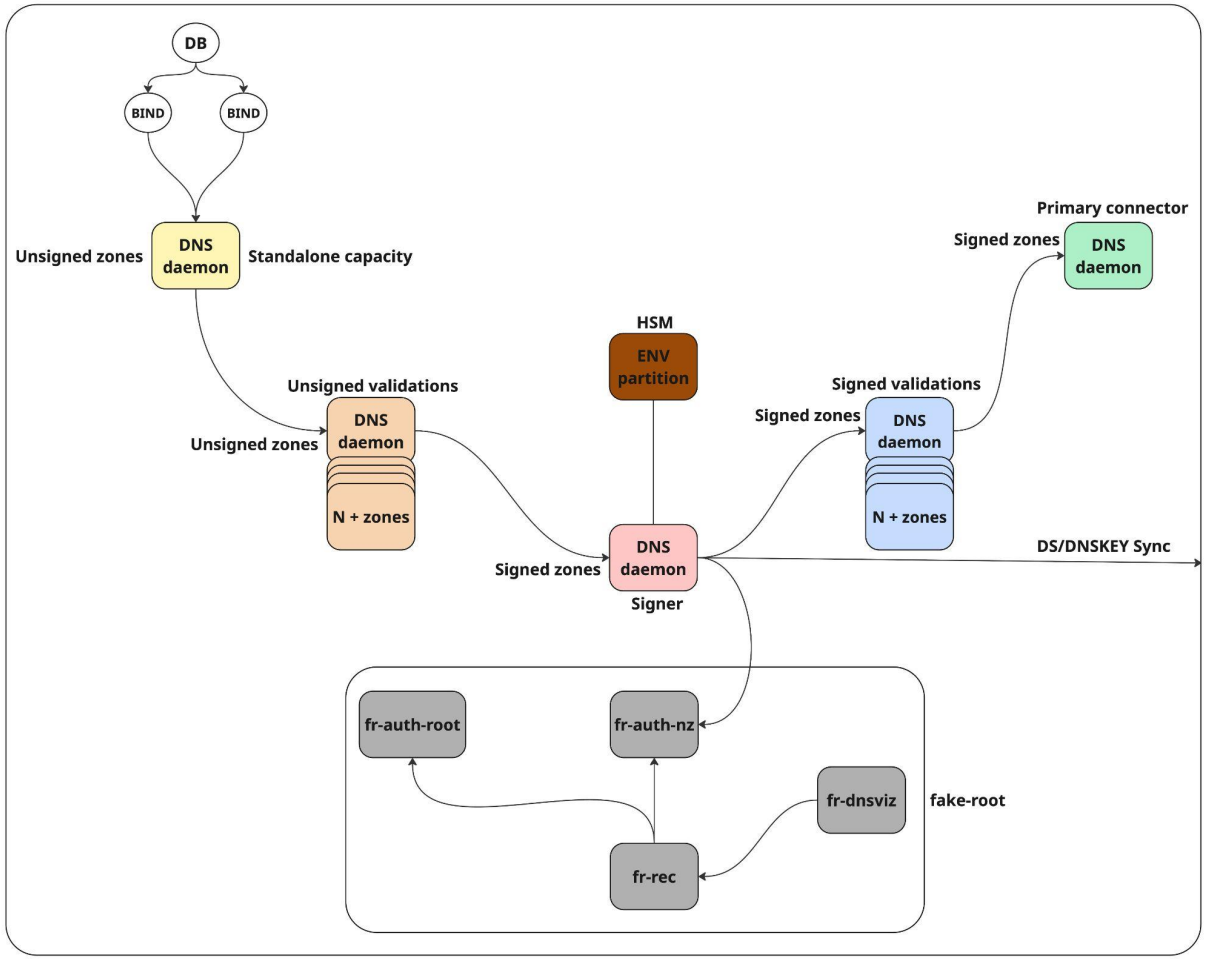
Requirements

- CI/CD tool
  - Self-hosted
  - Open source
  - Repository mirroring
  - Independent secret management
  - Container registry
  - Local users

Requirements

- Signer software
  - CDS/CDNSKEY
  - DDNS
  - DNSKEY Sync
  - Keytag conflict avoidance
  - DS submission
  - *Offline KSK*
  - *SKR/KSR*
  - *Go insecure safely*
  - ZoneMD

DC - Site ?
(Environment ?)



The route to be taken

Work ongoing

- ADRs and PoCs
  - Signer software
  - CI/CD tool
  - Pipelines
  - Workflow

ADR - Architecture Decision Records
PoC - Proof of Concept

What we aim to achieve

- Modernise and update
- Algorithm rollover
    - Zone size + Packet size
    - Key rollover frequency
- High availability
- Fault tolerance
- Reproducibility
- Reliability

Any Pātai(Questions)?

Gemini **generated all the Orc pictures and the HSM one**