# ROLLING .NA

## KEY AND INFRASTRUCTURE (V1.70)

Dr EW Lisse

2020-06-22

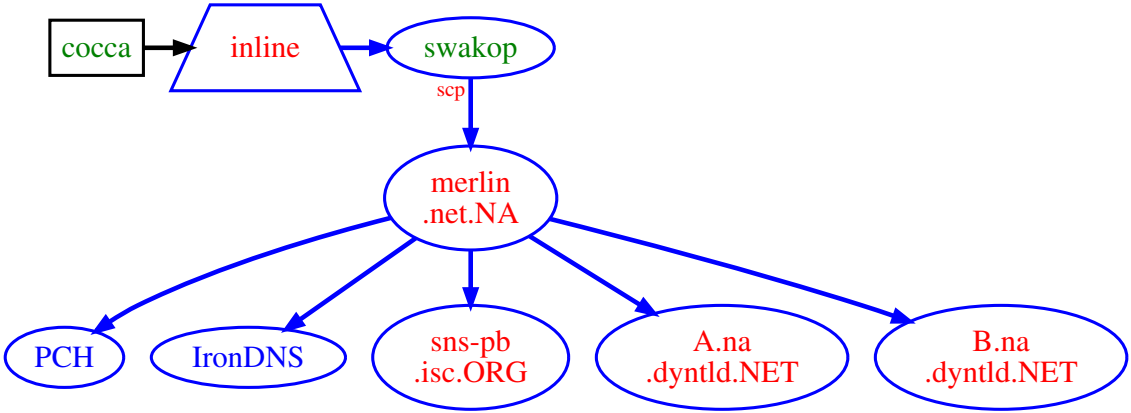
Namibian Network Information Center (Pty) Ltd

# Introduction

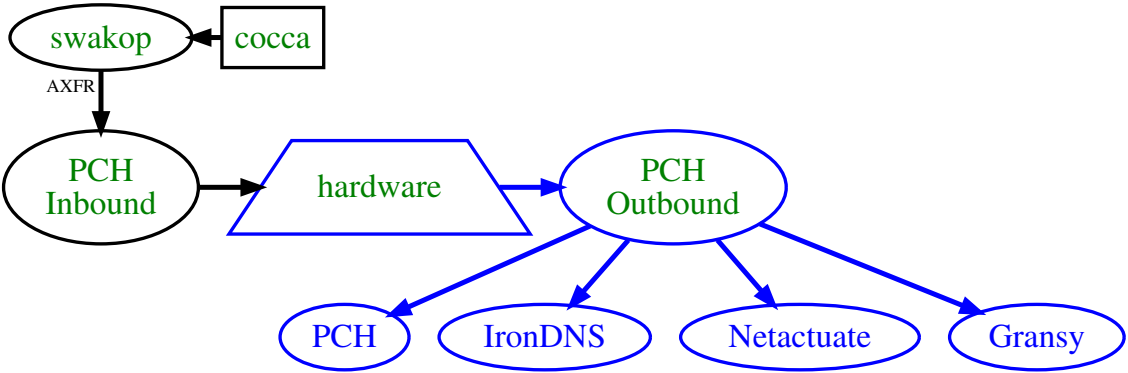
# Background

- .NA signed since 2009 (!)
  - Inline on Hidden Master
  - scp to Public Master
- SLDs signed by PCH
- .NA to be signed by PCH
  - Hardware
  - Trusted
- Added Complications
  - 4 Secondaries reached *End of Life*
    - 1 Age Related Failures (Power Supply)

# FROM HERE...

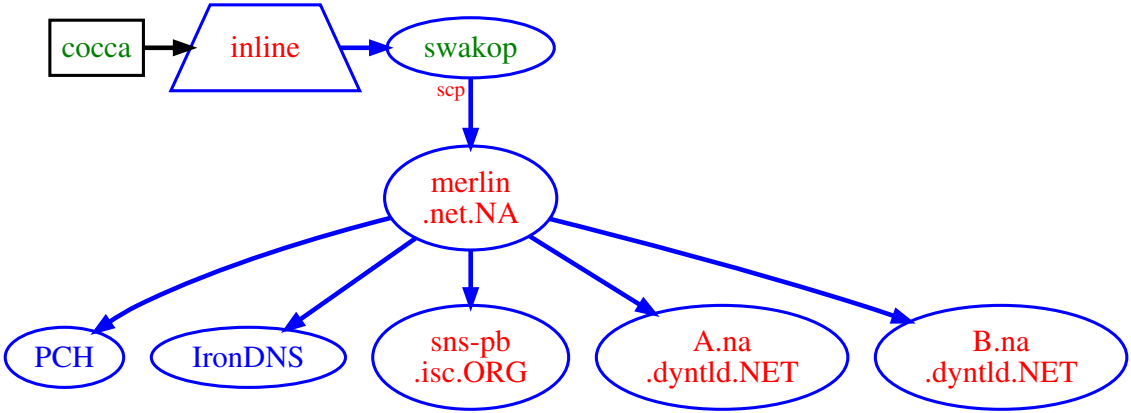

cocca
inline
swakop
scp
merlin
.net.NA
PCH
IronDNS
sns-pb
.isc.ORG
A.na
.dyntld.NET
B.na
.dyntld.NET

# ...TO THERE


swakop
cocca
AXFR
PCH
Inbound
hardware
PCH
Outbound
PCH
IronDNS
Netactuate
Gransy

# Preparatory Steps

# Point of Departure



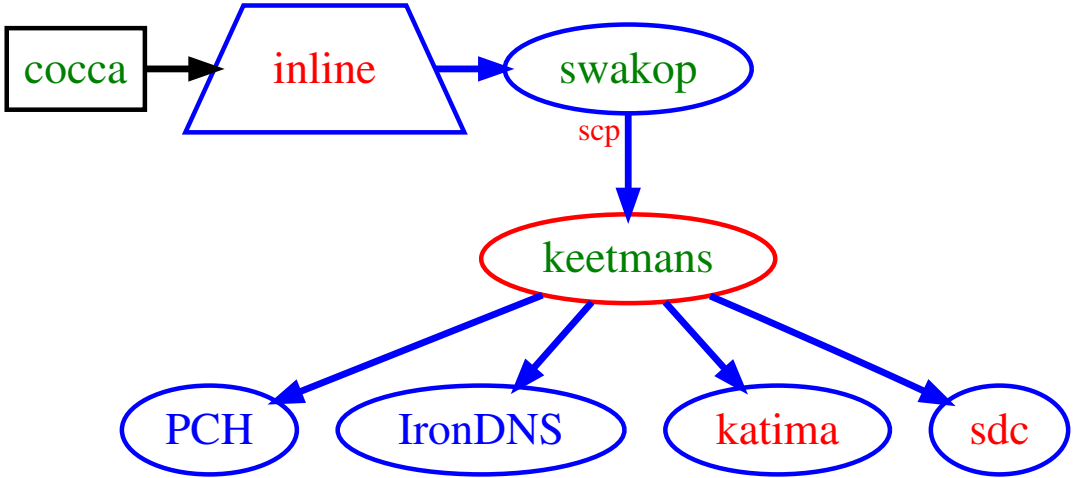
# Replace Primary

1. Add NOTIFY/AXFR on keetmans
   - 1.1 katima.omadhina.NET
   - 1.2 sdc.omadhina.co.NA
2. Modify Provision Script (on swakop)
   - 2.1 add scp signed zone to keetmans
3. Change NOTIFY/AXFR
   - 3.1 from merlin.net.NA to keetmans
     - 3.1.1 IronDNS
     - 3.1.2 PCH
   - 3.2 Allow on Firewall
4. Wait for caches to expire

# Change Secondaries

5. Root Zone Management Request
   - 5.1 Remove
     - 5.1.1 merlin.net.NA
     - 5.1.2 sns-pb.isc.ORG
     - 5.1.3 A.na.dyntld.NET
     - 5.1.4 B.na.dyntld.NET
   - 5.2 Add
     - 5.2.1 katima
     - 5.2.2 sdc
6. Wait for caches to expire
7. Modify Provision Script (on swakop)

# Intermediate Position

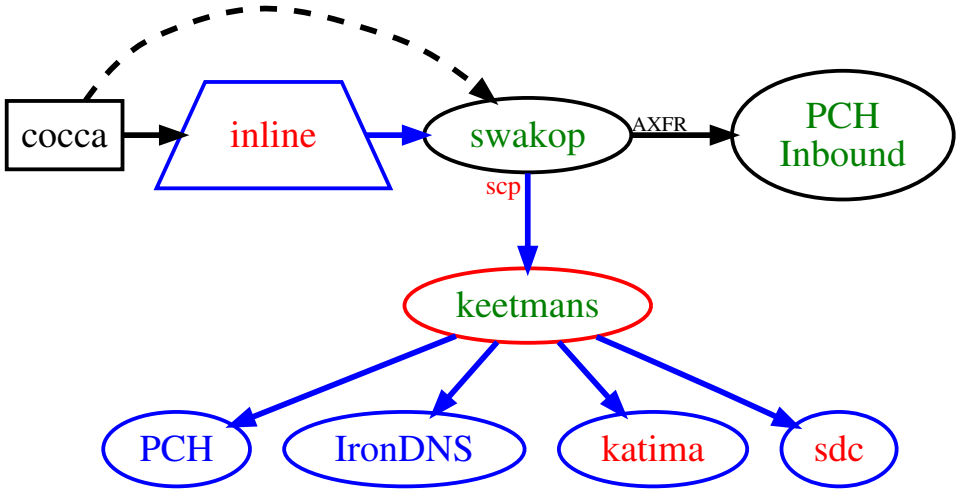


# KEYROLL

# Provision Signed & Unsigned

8. On CoCCA (swakop)
   - 8.1 Add old key to **unsigned** zone
9. Firewall (swakop)
   - 9.1 Add PCH **Unsigned** Inbound's IP
10. Modify Provision Script (swakop)
    - 10.1 NOTIFY/AXFR **unsigned** zone
      - 10.1.1 to PCH **unsigned** Inbound
      - 10.1.2 separate TSIGs
    - 10.2 Continue to scp signed zone
      - 10.2.1 to keetmans

# Position Signed & Unsigned



# Position Signed & Unsigned

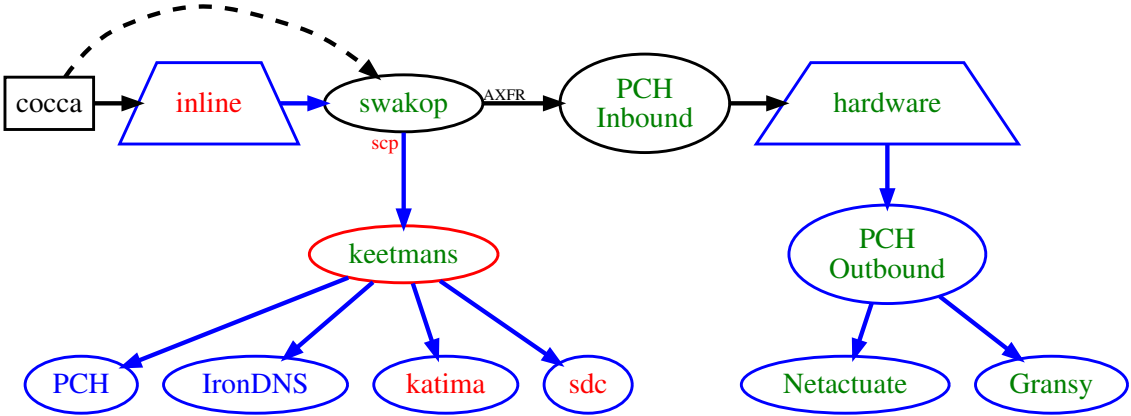
Hidden Master (swakop)

- provisions signed & unsigned zone
- to **two** different Inbounds
- using **two** different methods
- in **one** process
- in **one** Bind instance

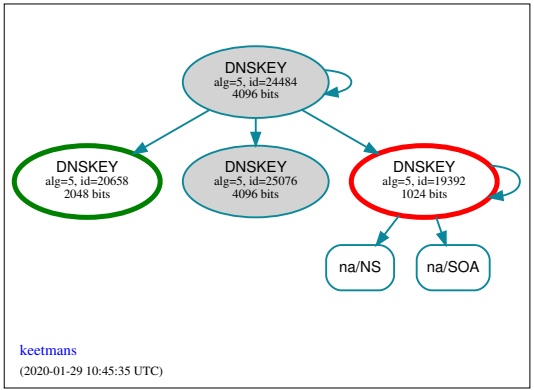
# Packet Clearing House

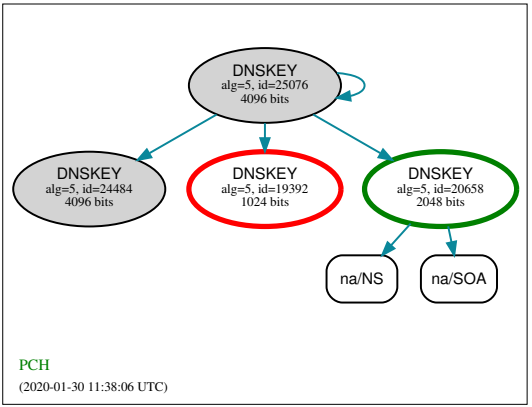
11. .NA Key Ceremony
    - 11.1 Generates new DNSKEYS
12. Add new DNSKEYS to (signed) zone
13. PCH Publishes signed zone
    - 13.1 Netactuate / Gransy
        - 13.1.1 signed with new key
14. keetmans Publishes signed zone
    - 14.1 PCH / IronDNS / katima / sdc
        - 14.1.1 signed with old key

# Signed & Unsigned Published



# DNSKEY

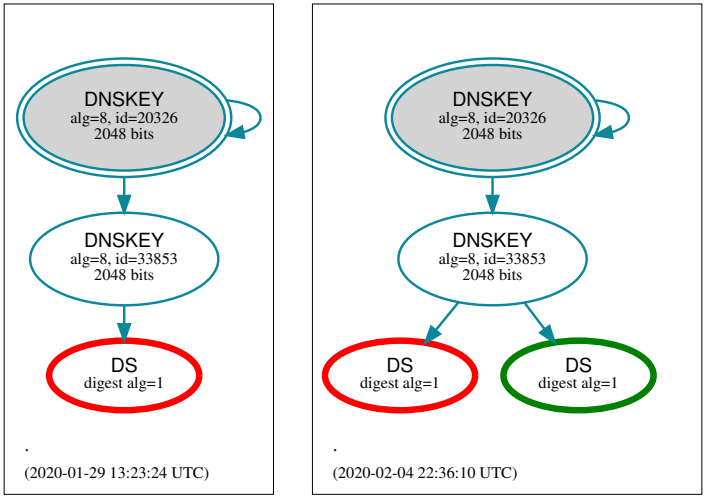

DNSKEY
alg=5, id=24484
4096 bits
DNSKEY
alg=5, id=20658
2048 bits
DNSKEY
alg=5, id=25076
4096 bits
DNSKEY
alg=5, id=19392
1024 bits
na/NS
na/SOA
keetmans
(2020-01-29 10:45:35 UTC)


DNSKEY
alg=5, id=25076
4096 bits
DNSKEY
alg=5, id=24484
4096 bits
DNSKEY
alg=5, id=19392
1024 bits
DNSKEY
alg=5, id=20658
2048 bits
na/NS
na/SOA
PCH
(2020-01-30 11:38:06 UTC)

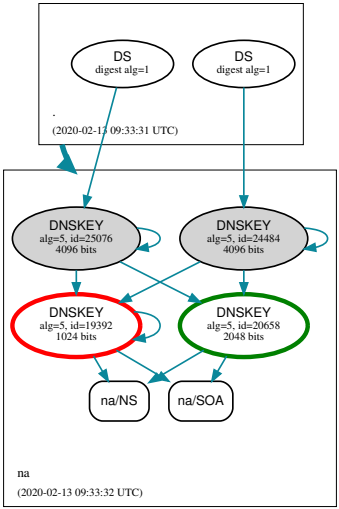
# RZM Request

15. Add new DS Record to root zone
16. Look for approval requests
    - 16.1 Should arrive within the hour
        - 16.1.1 Spam Folder
    - 16.2 Admin Contact
    - 16.3 Tech Contact
17. Wait for caches to expire

# Trust Anchors



# Ready to Roll…



# Synchronize

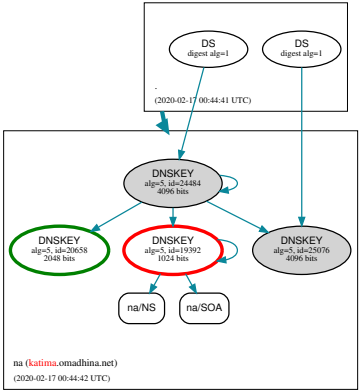
18. IronDNS
    - 18.1 change NOTIFY/AXFR
        - 18.1.1 from keetmans to PCH
19. PCH Outbound
    - 19.1 Change from old to new zone
        - 19.1.1 Internally

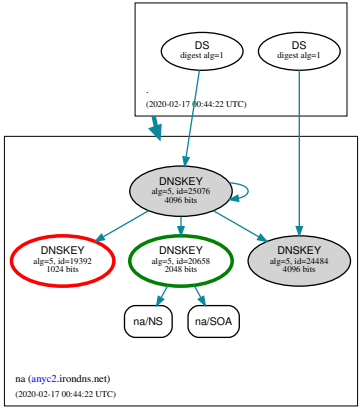
- katima & sdc temporarily serve
    - Same zone content
    - Same SOA
    - Still signed with old key

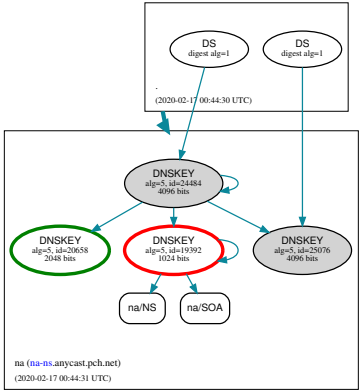
# Almost There

20. Test SOA Synchronicity
    - 20.1 Netactuate
    - 20.2 Gransy
    - 20.3 IronDNS
    - 20.4 PCH Outbound
21. On CoCCA
    - 21.1 Shorten SOA values
    - 21.2 Update authoritative NS set
22. Wait for caches to expire

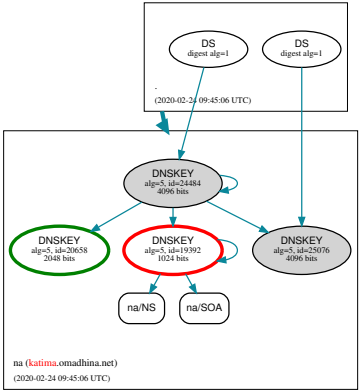
# Are we in Sync?

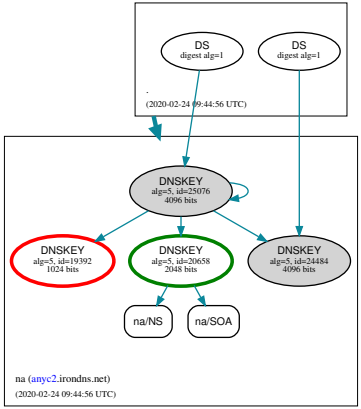


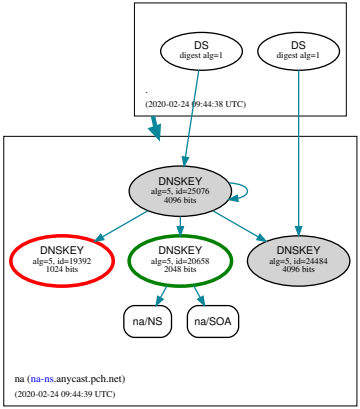



# We are in Sync!



# We are in Sync!

NA

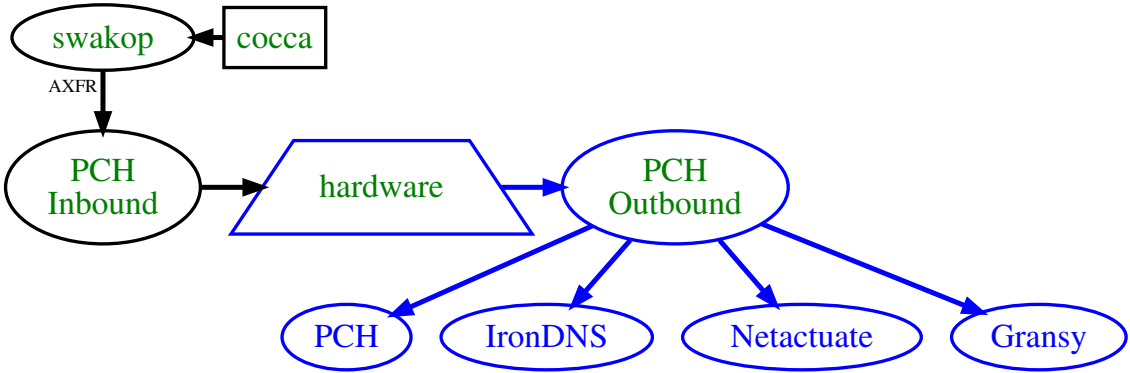
2020-02-24 11:44

| Time Stamp | Name Server | Serial | ZSK |
|---|---|---|---|
| 1582537479 | sdc.omadhina.co.na/ | 2020022411 | 19392 |
| 1582537496 | katima.omadhina.net | 2020022411 | 19392 |
| 1582537470 | na-ns.anycast.pch.net | 2020022411 | 20658 |
| 1582537489 | anyc2.irondns.net | 2020022411 | 20658 |
| 1582537506 | etld-1.anycast.net | 2020022411 | 20658 |
| 1582537529 | na.anycastdns.cz | 2020022411 | 20658 |
| 1582537554 | dnssec-01.pao.pch.net | 2020022411 | 20658 |

# RZM Requests

23. Remove
    - 23.1 katima
    - 23.2 sdc
24. Add
    - 24.1 Netactuate
    - 24.2 Gransy
25. Wait for caches to expire
26. Remove old DS Record

# Final Outcome



# Tidy Up

27. On CoCCA (swakop)
    - 27.1 Remove old key from **unsigned** zone
28. Unconfigure bind
    - 28.1 keetmans
    - 28.2 sdc / katima
29. Close Firewall
    - 29.1 keetmans
30. Reset SOA values
    - 30.1 CoCCA
31. Document Setup in Handbook

# Lessons Learned

# Lessons Learned

- Write a Plan
  - **Test** the plan (lisse.NA)
- Follow the Plan
  - **ONE** item at a time
    - Document **every** modification
- Take your time
  - Communicate!
    - Details matter
- Emergency Contacts
  - Different Time Zones
- DNSVIZ is your friend

# Thanks

- PCH
- Gransy
- NetActuate
- IronDNS/Knipp
- ISC
- DYN/Oracle

# Questions?