CIRA: KSK Rock and Roll

Rolling from Algorithm 8 to 13 on .CA and on new HSMs

Leo Liang

ICANN78 DNSSEC & Security Workshop

Oct 25, 2023

What we'll cover

- Who is CIRA
- Why are we doing this
- Different trials and technique
- Lessons and mistakes
- Conclusion

Who is CIRA

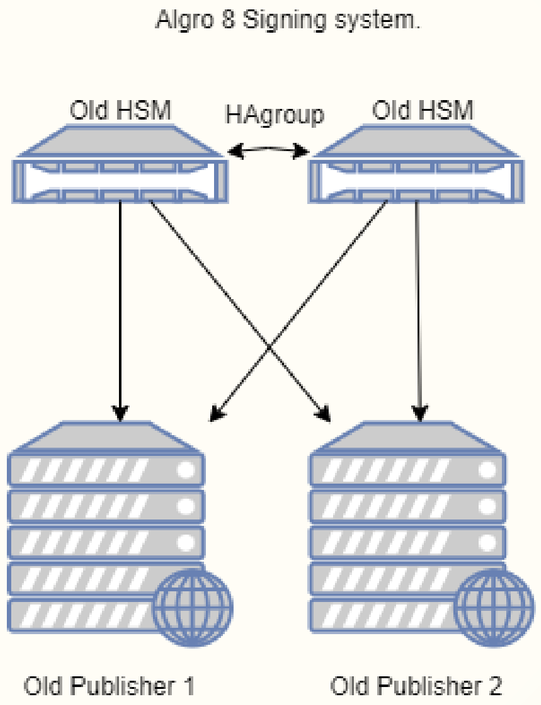
- CIRA is non-profit best known for managing the .CA ccTLD on behalf of all Canadians
- We provide hosted registry services for ccTLDs and gTLDs (.ca .kiwi, .eco, .sx, etc.)
- We provide registry platform to third parties (.nz and .ie)
- We are an EBERO provider for ICANN
- Anycast DNS and CIRA Canadian Shield

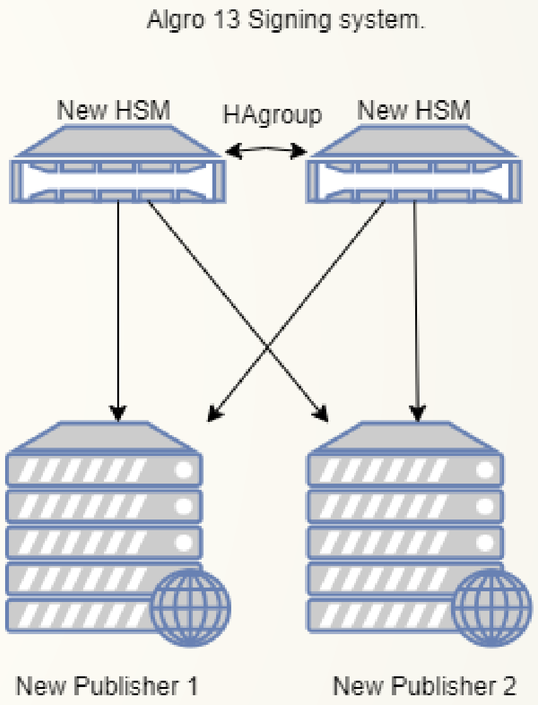
Why are we doing this.

- Our old HSMs is getting out of support
- We want to switch to operating with algorithm 13
- We do annual KSK rolls
- We are trying to do all 3 at the same time

Trial #1 on Aug 1, 2023:

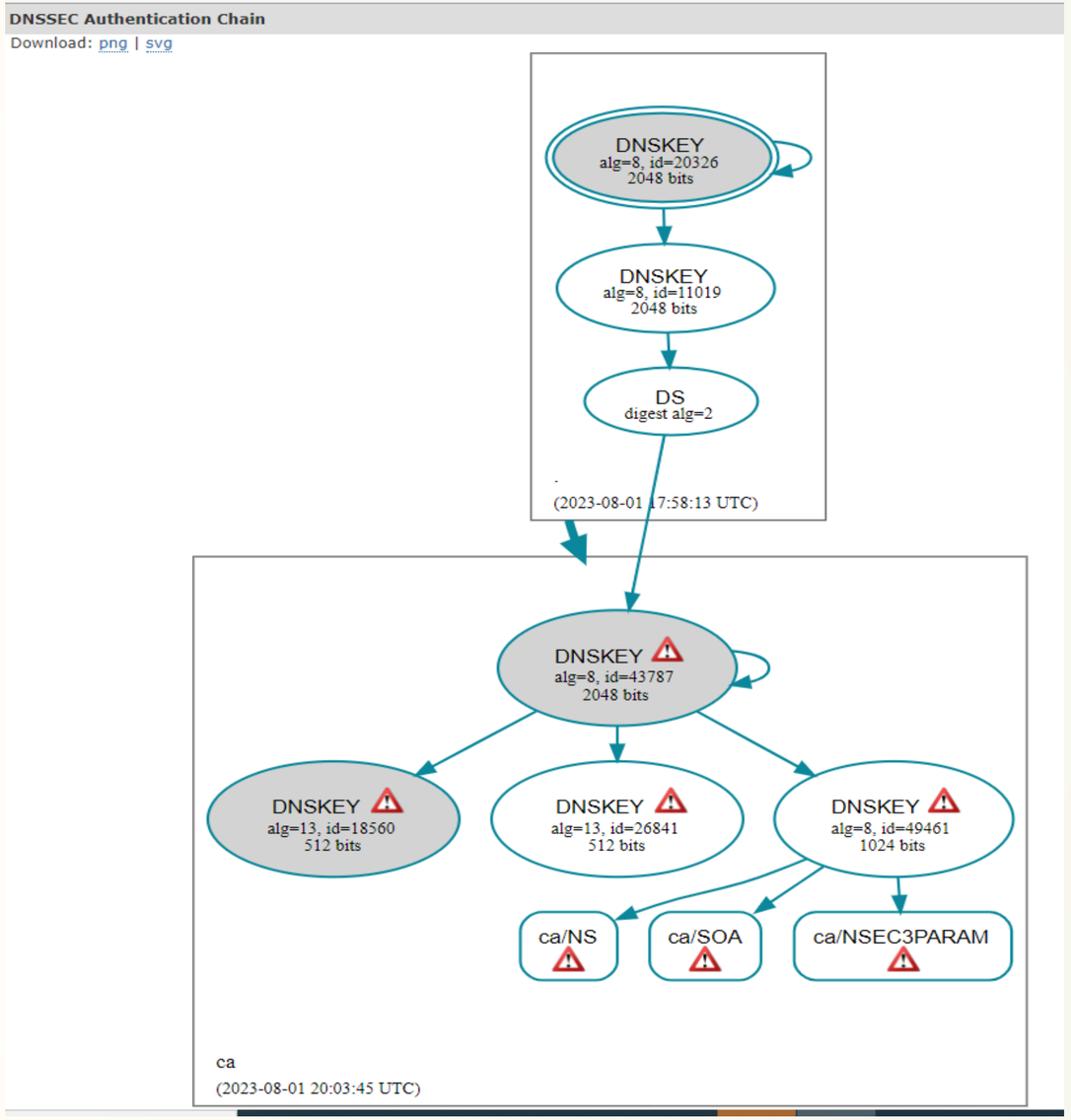
- Simulate to DNS operator take over
- Insert algorithm 13 keys into old system, and vice versa





Trial #1 on Aug 1, 2023:

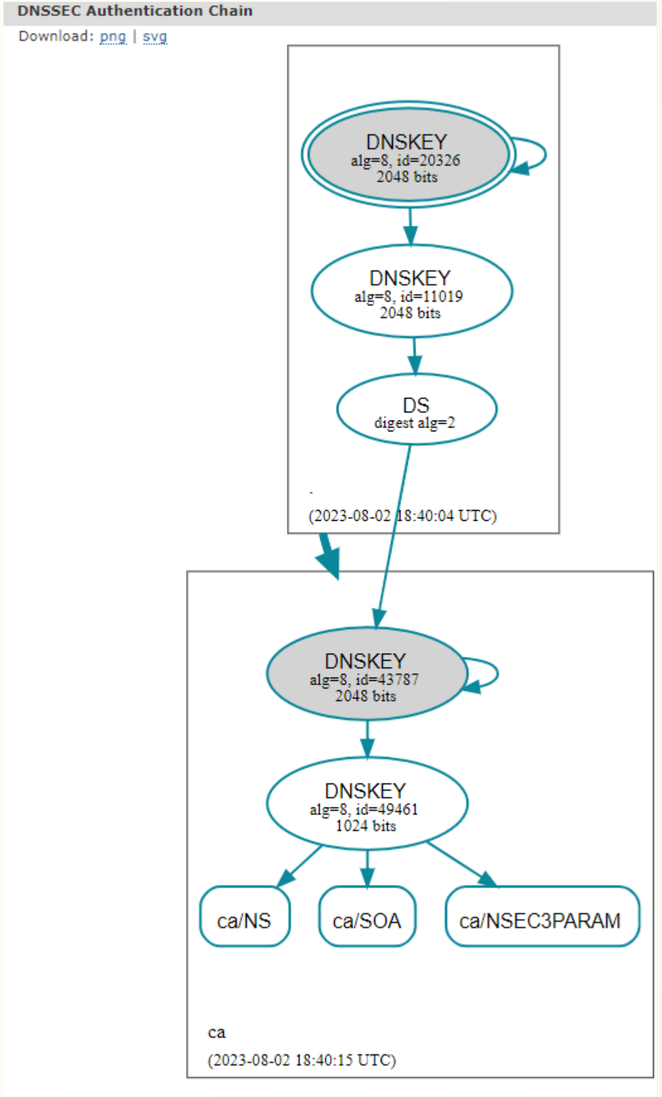
- Caused ERROR on DNSVIZ and Zonemaster warning
- Reach out to DNS community
- Missing the DNSKEY RRSET RRSIGs for the new keys
    - The intended KSK has not signed the DNSKEY RRSet. not a SEP
    - The intended ZSK has not signed any of the zone's RRSets,
- Thanks to Viktor Dukhovni, Paul Wouters, Steve Crocker, Peter Thomassen for their advice, assistance, and ideas



https://dnsviz.net/d/ca/ZMlllQ/dnssec/

Trial #1 on Aug 2, 2023: Rollback

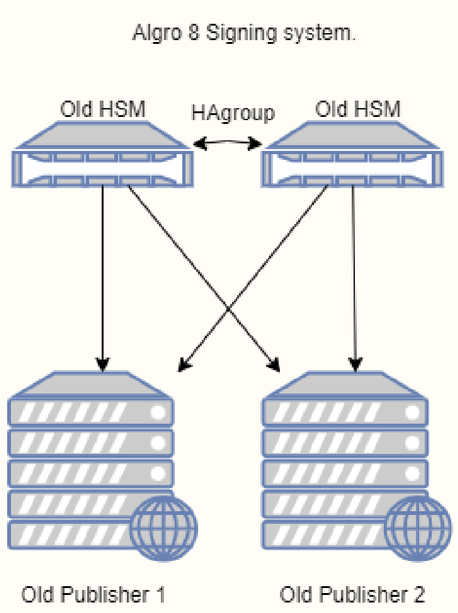
- Remove the inserted DNS Keys from the zone template
- Wait for the next zone publish.
- Check everything went back to normal

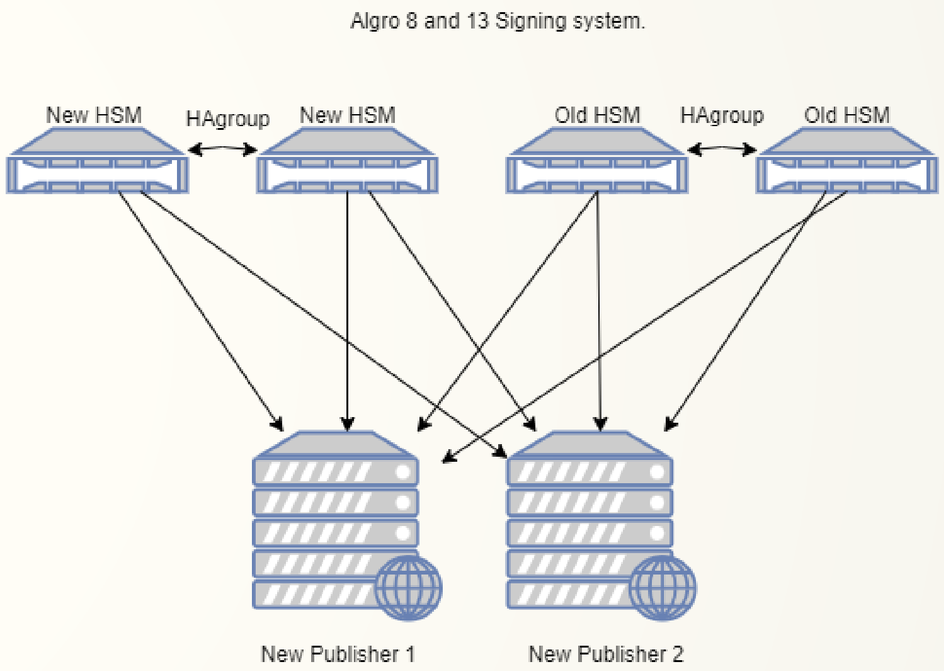


https://dnsviz.net/d/ca/ZMqjDw/dnssec/

Trial #2 on Sep 13, 2023:

- Use OpenDNSSEC software for algorithm rollover
- The new publishers communicated with both sets of HSMs
- Double signing the zone file with both algorithm 8 and 13





Trial #2 configuration :

Specially thanks to Berry van Halderen from NLnet Labs who guide us through the process

1. Setup additional 'repository' in OpenDNSSEC config.xml
2. Import new keys to OpenDNSSEC
   - Using ods cli commands
   - Using database queries
3. Setup kasp.xml to deal with the double signing

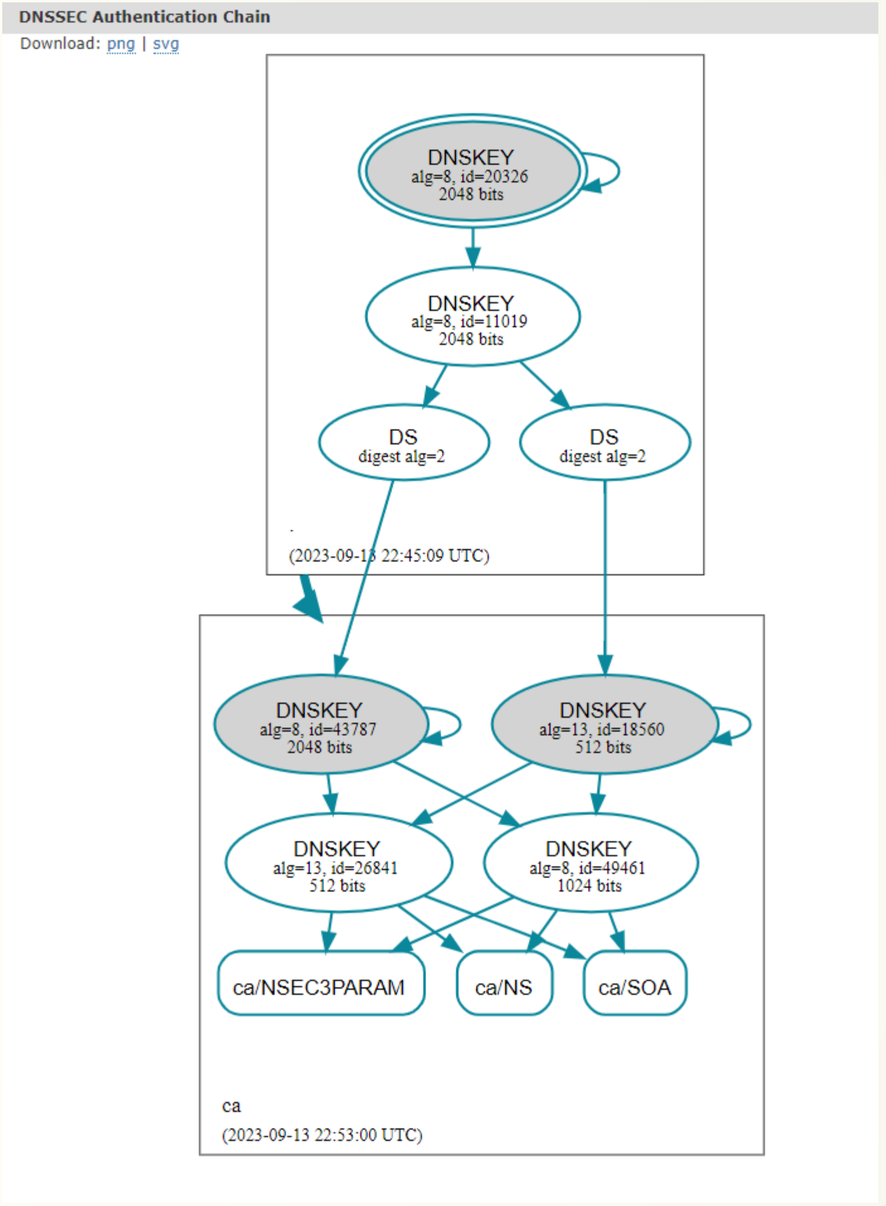
```
<Repository name="HSM-ca">
        <Module>/usr/lib/libCryptoki2_64.so</Module>
        <TokenLabel>GROUP-dotCA-OLD</TokenLabel>
        <PIN>xxxxx</PIN>
</Repository>

<Repository name="HSM-ca-new">
        <Module>/usr/lib/libCryptoki2_64.so</Module>
        <TokenLabel>GROUP-dotCA</TokenLabel>
        <PIN>xxzxx</PIN>
</Repository>
```

```
<KSK>
        <Algorithm length="256">13</Algorithm>
        <Lifetime>P14M</Lifetime>
        <Repository>HSM-ca-new</Repository>
</KSK>
<!-- Parameters for ZSK only -->
<ZSK>
        <Algorithm length="256">13</Algorithm>
        <Lifetime>P30D</Lifetime>
        <Repository>HSM-ca-new</Repository>
</ZSK>
```


cira

Trial #2 Sep 13, 2023 :

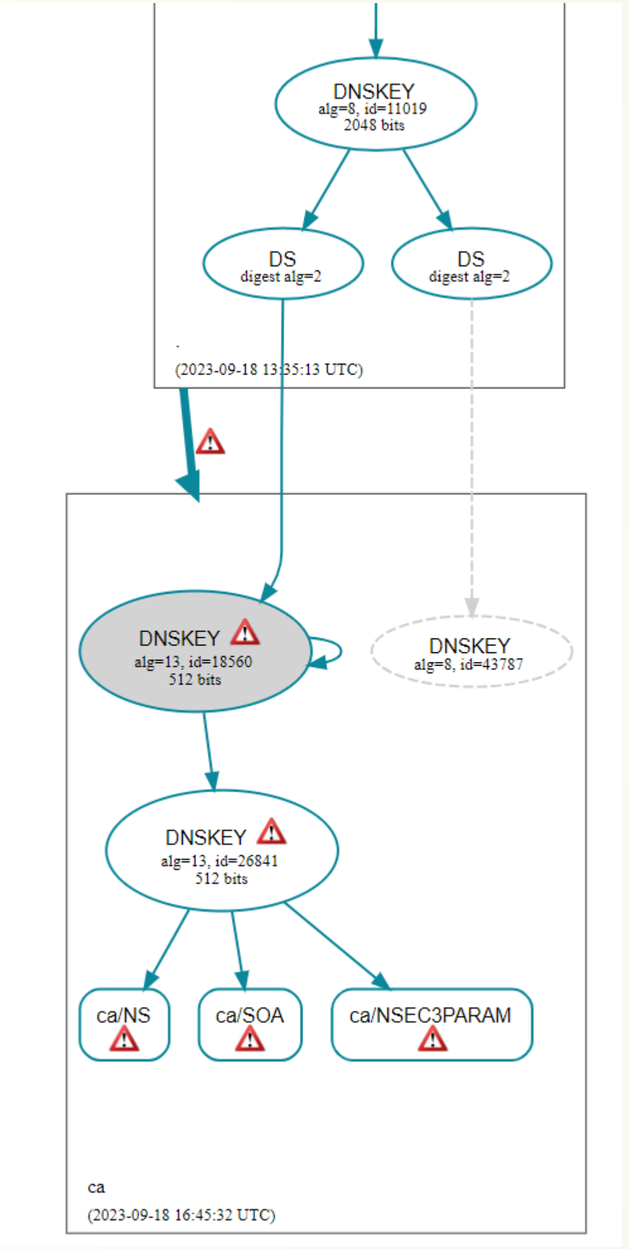
- Cutover to new system
- Add DS record to IANA
- Double signing with both algorithm



https://dnsviz.net/d/ca/ZQI9TA/dnssec/

Trial #2 mistakes: Sep 18, 2023

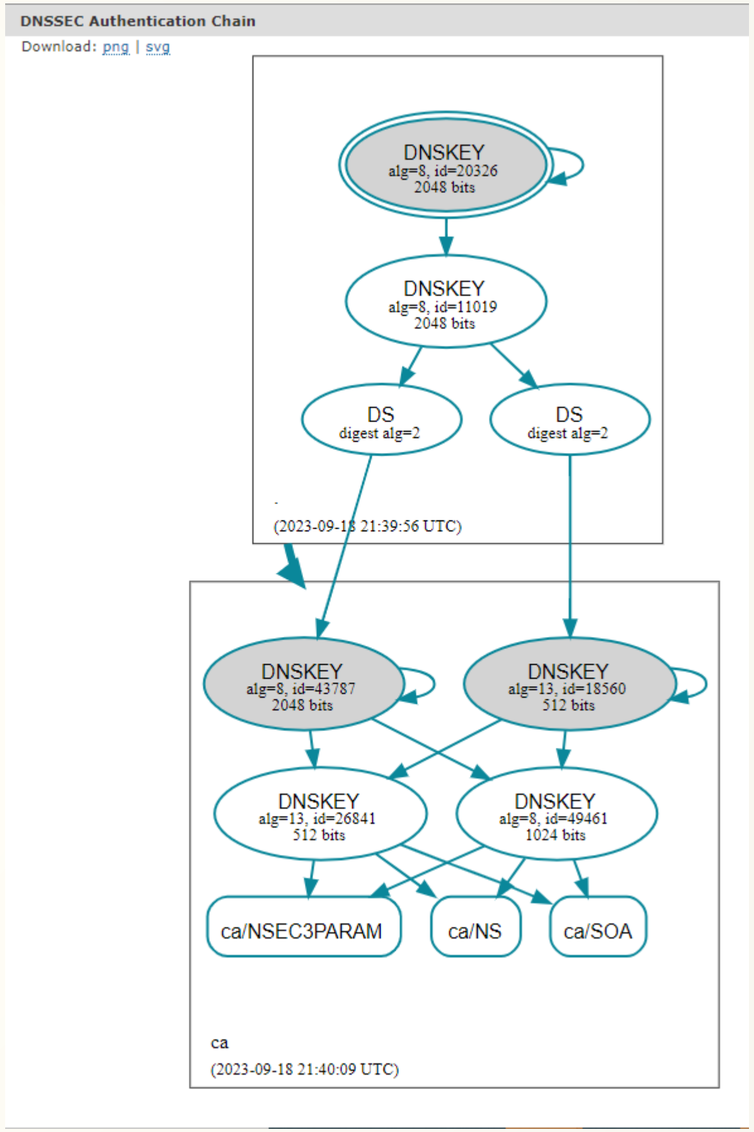
- Remove algorithm 8 DNSKEYs before removing the DS record from IANA
- ds-seen and ds-gone were issued at the same time
  - During Algorithm roll, ds-gone will need to be issued after the ds record is removing from IANA portal



https://dnsviz.net/d/ca/ZQiMfQ/dnssec/

Trial #2 mistakes: Sep 18, 2023 rollback

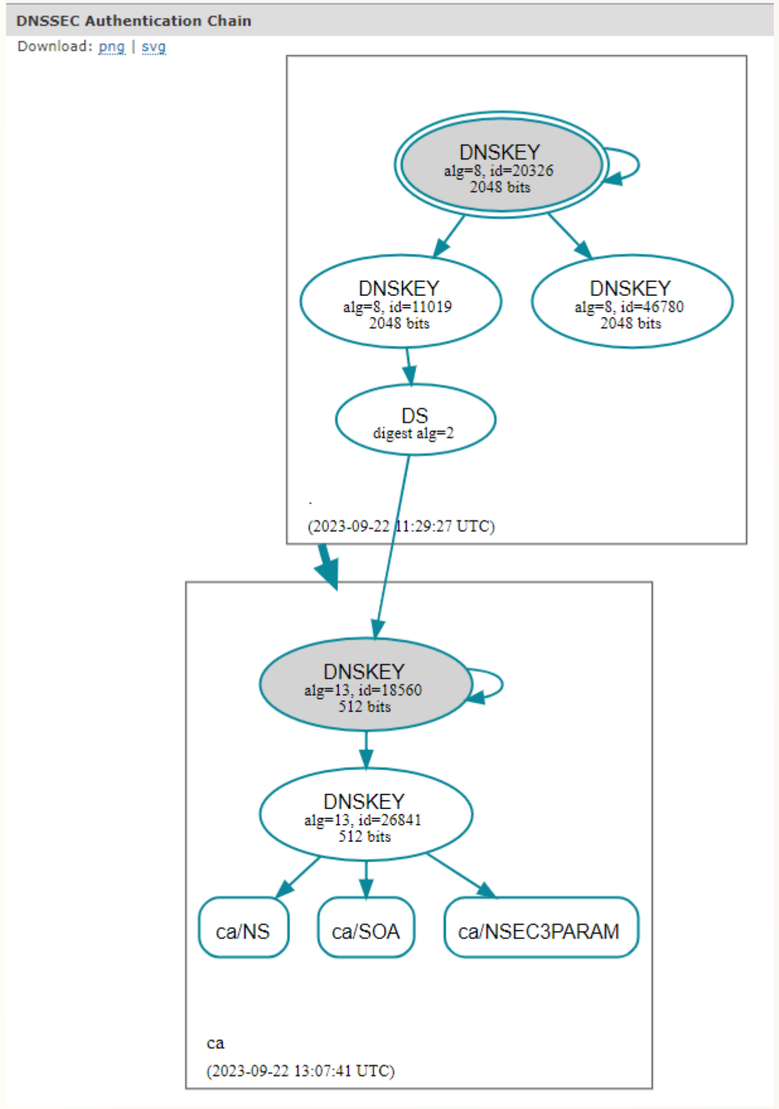
- Restore OpenDNSSEC to the backup taken before the ds-seen and ds-gone commands were issue
- Republish the zone
- Everything back to normal with double signing.



https://dnsviz.net/d/ca/ZQjDuQ/dnssec/

Trial #2 completed: Sep 22, 2023

- After remove DS record from IANA
- Then removed algorithm 8 from the Publishers
- Completed the cutover



https://dnsviz.net/d/ca/ZQ4hSw/dnssec/

Lessons and Mistakes

- When trying to switch HSM with Algorithm rollover, it’s better to not using the DNS operator takeover approach. Conservative approach to roll the algorithm within the same publisher would be a safer.
- any DS records in the root zone must have a corresponding DNSKEY KSK with SEP flag (257), and each KSK signs each KSKs and ZSK. The zone content (opt-in) must be signed by all ZSKs present

Future Suggestions:

- Human intervention needs to be minimized during Algorithm and KSK rolling process – end to end
- Tools need to better support automation
- ICANN IANA should support automation mechanism
  - RZM API integration with CDS/CDNSKEY automation
    - Changes created automatically in RZM when a CDS is present
      - Manual authorization as-is
      - Logic and integrity test done automatic
- Algorithm rollover with DNS operator take over – relaxing the requirements for double signing when different Algorithm involves

Questions