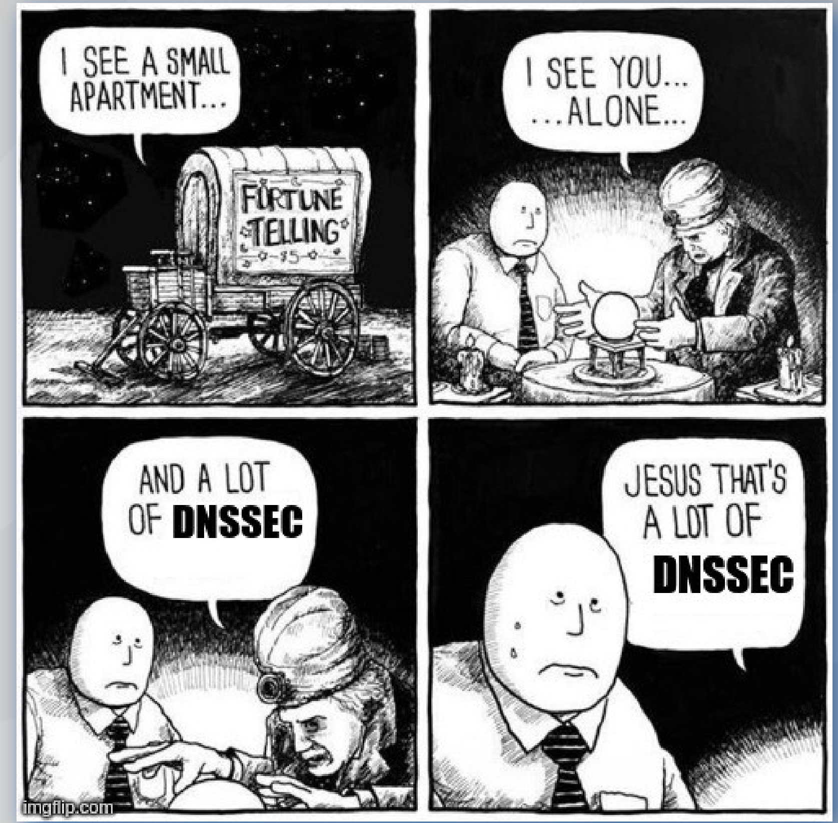
DNSSEC Multi-Signer Model

Matthijs Mekking, ISC

Who am I?

- **Matthijs Mekking**
- **DNS** software developer for 15+ years
- Working for **ISC** since December 2018
- Working on **BIND 9**
- Previously: *Dyn, OpenDNSSEC, NLnet Labs*



Multi-Signer Model

- Multiple DNS providers, for high reliability
- Signing the same zone independently
  - When regular XFR doesn’t work
  - Or online signing
- RFC 8901: Multi-Signer DNSSEC Models

Multi-Signer Model

- Which model should I use for my zone?
  - **Model 1: Common KSK, unique ZSK**
    - *“The zone owner is responsible for signing the DNSKEY RRset”*
    - Same characteristics as Offline KSK
  - **Model 2: Unique KSK and ZSK per provider**
    - More alike regular DNSSEC signing
    - CSK is possible
    - Easier to adopt with existing (open-source) software (currently)
      - So far only *knot dns* has model 1 support

Multi-Signer Model Support

- What does supporting multi-signer mean?
  1) Being capable of publishing other signer’s DNSSEC records
  2) Being aware of other signers in the multi-signer group

Multi-Signer Model Support

- Implicit assumptions of a single-signer model
  - An unsigned zone shall not contain any DNSSEC records
  - If there are DNSKEY rrs, there must be associated private keys
  - CDS/CDNSKEY rrs are tightly coupled to signing keys
  - I control all NS records in the zone

Multi-Signer Model “BCP”

- Use the same DNSSEC Policy on all signers/providers
  - MUST have same key algorithm (Req. RFC 4035, Section 2.2)
  - Same NSEC(3) algorithm (for aggressive NSEC(3) caching)
  - Differences in durations and TTL should have little to no impact

Multi-Signer Model “BCP”

- Avoid keytag collisions
  - Think KeyTrap
  - Mitigation: Allow up to n (failed) attempts
  - Key generation race condition? ZSK Pre-publication becomes a transaction

Multi-Signer Key Rollovers

- ZSK Rollovers
  - Model 1
    - Little change required because ZSKs are pregenerated
  - Model 2
    - When publishing ZSK, it should be published to all providers
    - And same for when removing the old ZSK
    - How to ensure that the new key is published/withdrawn?
      - Query DNSKEY RRset at each provider (each NS?)
      - Rollback mechanisms?

Multi-Signer Key Rollovers

- KSK Rollovers
  - Model 1
    - Same as before
  - Model 2:
    - Need to publish CDS/CDNSKEY records to all providers
    - Keep CDS/CDNSKEY RRset in sync or remove after rollover?
    - Double-KSK vs Double-DS rollover method

Multi-Signer Algorithm Rollover

- All signers should introduce the new algorithm at the same time
- Wait until signers have signed all data with the new algorithm
- Add new ZSK of each signer to all other signers/providers
- All providers publish the new CDS/CDNSKEY RRset
- Wait until DS RRset is published (and wait some more)
- Remove all DNSKEY and RRSIG records from the old algorithm
- Update the CDS/CDNSKEY RRset

- **This requires more coordination than regular key rollover**

Multi-Signer Automation [wip]

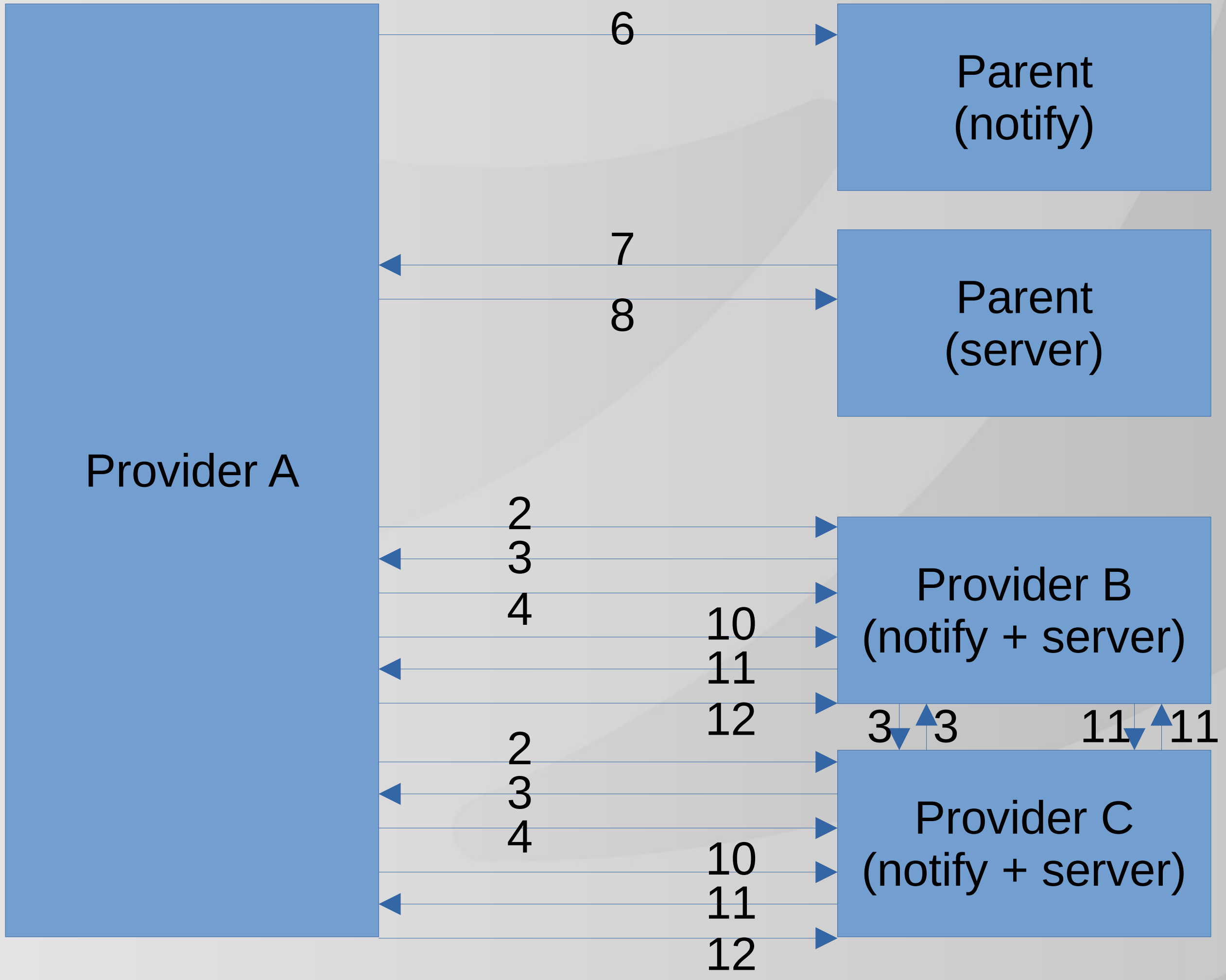
- MUSIC, a tool to control signers in a multi-signer model
  - Based on **draft-ietf-dnsop-dnssec-automation**
  - Single controller updating all the signers/providers
  - Good for testing if your software is multi-signer proof
  - Centralized vs. Distributed multi-signer environment
- Generalized DNS Notifications + DS/DNSKEY polling
  - **draft-ietf-dnsop-generalized-notify**
  - NOTIFY(CDS), NOTIFY(DNSKEY)

Multi-Signer Automation

1. Publish new CSK
2. NOTIFY(DNSKEY)
3. Providers query DNSKEY
4. DNSKEY polling

5. Update CDS/CDNSKEY
6. NOTIFY(CDS)
7. Parent queries CDS
8. DS polling

9. Remove old CSK
10. NOTIFY(DNSKEY)
11. Providers query DNSKEY
12. DNSKEY polling



Multi-Signer tldr

- Multiple DNS providers, for high reliability
- Model 1 if you already do Offline KSK
- Model 2 otherwise
- BCP: Use the same DNSSEC policy on all providers
- Especially key algorithm and NSEC algorithm
- Beware of keytag collisions
- Key rollovers now require transactions on DNSKEY publications
- Algorithm rollover requires even more coordination
- Efforts to automate multi-signer (MUSIC, dnssec-automation draft)
- Generalized DNS Notifications would help
- BIND 9 is multi-signer model 2 proof (9.18-S, upcoming 9.20)
- Model 1 (Offline KSK) and multi-signer awareness are WIP

Suggested BIND 9 configuration

```
dnssec-policy music {
        keys {
                ksk key-directory lifetime unlimited algorithm 8;
                zsk key-directory lifetime unlimited algorithm 8;
                //ksk key-directory lifetime unlimited algorithm 13;
                //zsk key-directory lifetime unlimited algorithm 13;
        };
        cdnskey no;
        cds-digest-types { };

        publish-safety 5d;
        retire-safety 5d;
};

zone "example.nl" {
        type primary;
        file "db/pop.example.db";
        dnssec-policy music;
        inline-signing no;
        update-policy {
                grant provider-b. name example.nl. DNSKEY CDS CDNSKEY CSYNC NS;
                grant provider-c. name example.nl. DNSKEY CDS CDNSKEY CSYNC NS;
        };
};
```

References

- ISC website: https://www.isc.org
- Software downloads: https://www.isc.org/download
- Presentations: https://www.isc.org/presentations
- GitLab: https://gitlab.isc.org

- Multi-Signer Project: https://github.com/DNSSEC-Provisioning/Multi-signer
- MUSIC: https://github.com/DNSSEC-Provisioning/music
- Generalized DNS Notifications: https://datatracker.ietf.org/doc/draft-thomassen-dnsop-generalized-dns-notify/