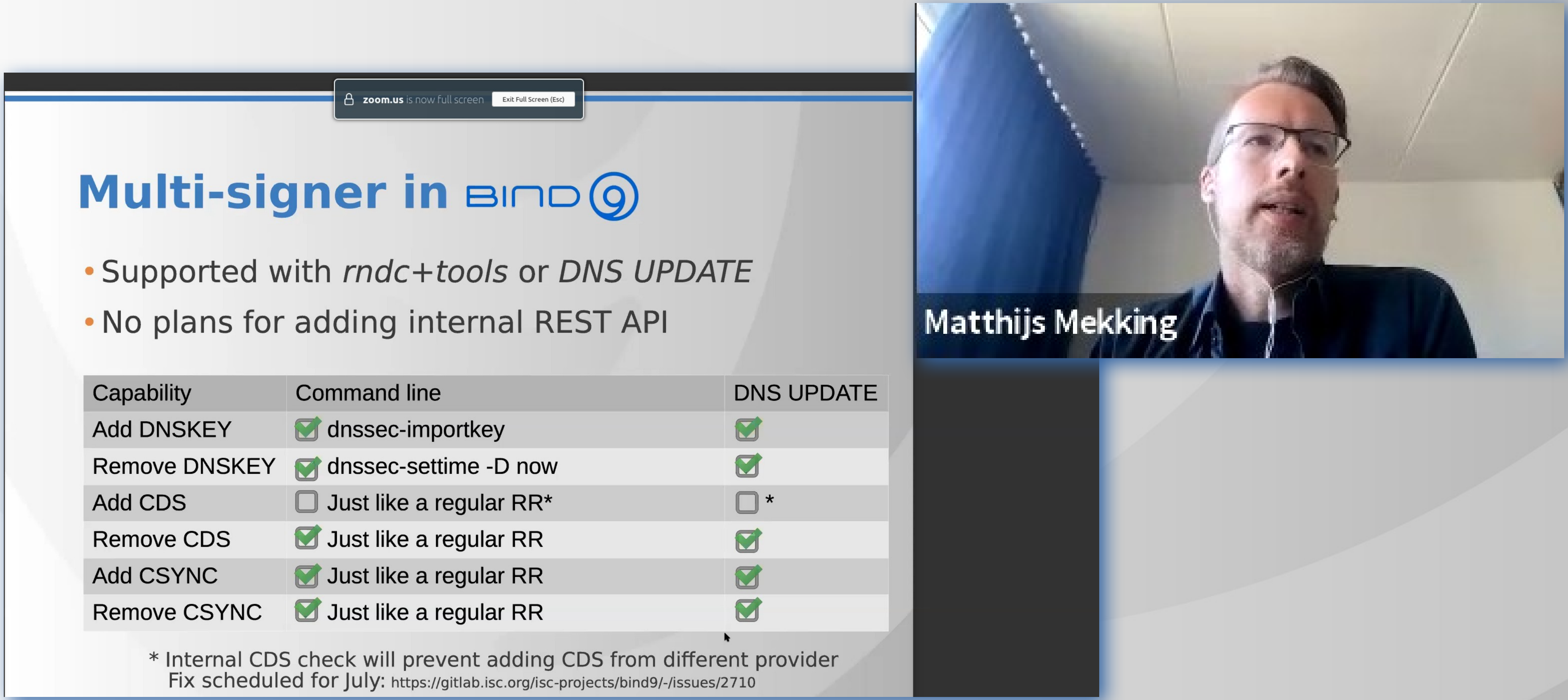
DNSSEC Multi-Signer Model in BIND 9

Matthijs Mekking, ISC
RIPE86, DNS-WG

Once upon a time (June 2021)



Multi-signer in BIND 9

- Supported with *rndc+tools* or *DNS UPDATE*
- No plans for adding internal REST API

Capability	Command line	DNS UPDATE
Add DNSKEY	☑ dnssec-importkey	☑
Remove DNSKEY	☑ dnssec-settime -D now	☑
Add CDS	□ Just like a regular RR*	□ *
Remove CDS	☑ Just like a regular RR	☑
Add CSYNC	☑ Just like a regular RR	☑
Remove CSYNC	☑ Just like a regular RR	☑

* Internal CDS check will prevent adding CDS from different provider
Fix scheduled for July: https://gitlab.isc.org/isc-projects/bind9/-/issues/2710

This is not a “DNSSEC is hard” story

- I’ll be describing some weird scenarios where things can go wrong
- But for the majority of setups, **dnssec-policy** just works
- Multi-Signer is not a common setup (at least at the moment)

Multi-Signer Model

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

Multi-Signer Model

- Model 1
  - Common KSK, unique ZSK
  - Not possible with BIND 9 today
    - Requires loading of pre-signed DNSKEY RRset
    - Need to add support for offline KSK
- Model 2
  - Unique KSK and ZSK per provider
  - Works best for BIND 9

Multi-Signer Model

- Current BIND 9 documentation says
  - *Such a setup requires some coordination between providers when it comes to key rollovers, and may be better suited to be configured with **auto-dnssec allow;***
  - *Still requires the creation of key files for other provider's keys with **dnssec-importkey***
  - ***auto-dnssec** is marked deprecated*

Required server capabilities

Capability	Command line	DNS UPDATE
Add DNSKEY	☑ dnssec-importkey	☑
Remove DNSKEY	☑ dnssec-settime -D now	☑
Add CDS/CDNSKEY	☑ Just like a regular RR	☑
Remove CDS/CDNSKEY	☑ Just like a regular RR	☑
Add CSYNC	☑ Just like a regular RR	☑
Remove CSYNC	☑ Just like a regular RR	☑

In practice

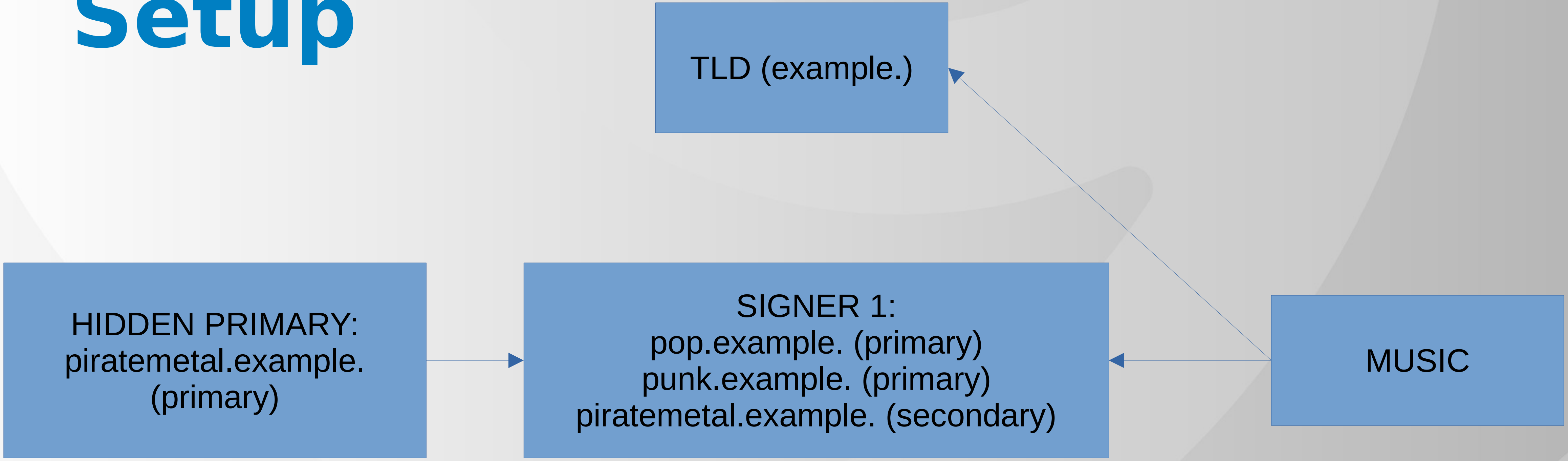
- Use cases described in draft-ietf-dnsop-dnssec-automation
  - Signer joins a multi-signer group
  - Signer leaves a multi-signer group
  - Signer performs ZSK rollover
  - Signer performs KSK rollover (or CSK)
  - Algorithm rollover

MUSIC

- Multi-signer controller
- Proof of concept implementation of draft-ietf-dnsop-dnssec-automation
  - Signer joins a multi-signer group
  - Signer leaves a multi-signer group
  - Key rollover scenarios not yet implemented

Zwarte Cross

Setup



TLD (example.)

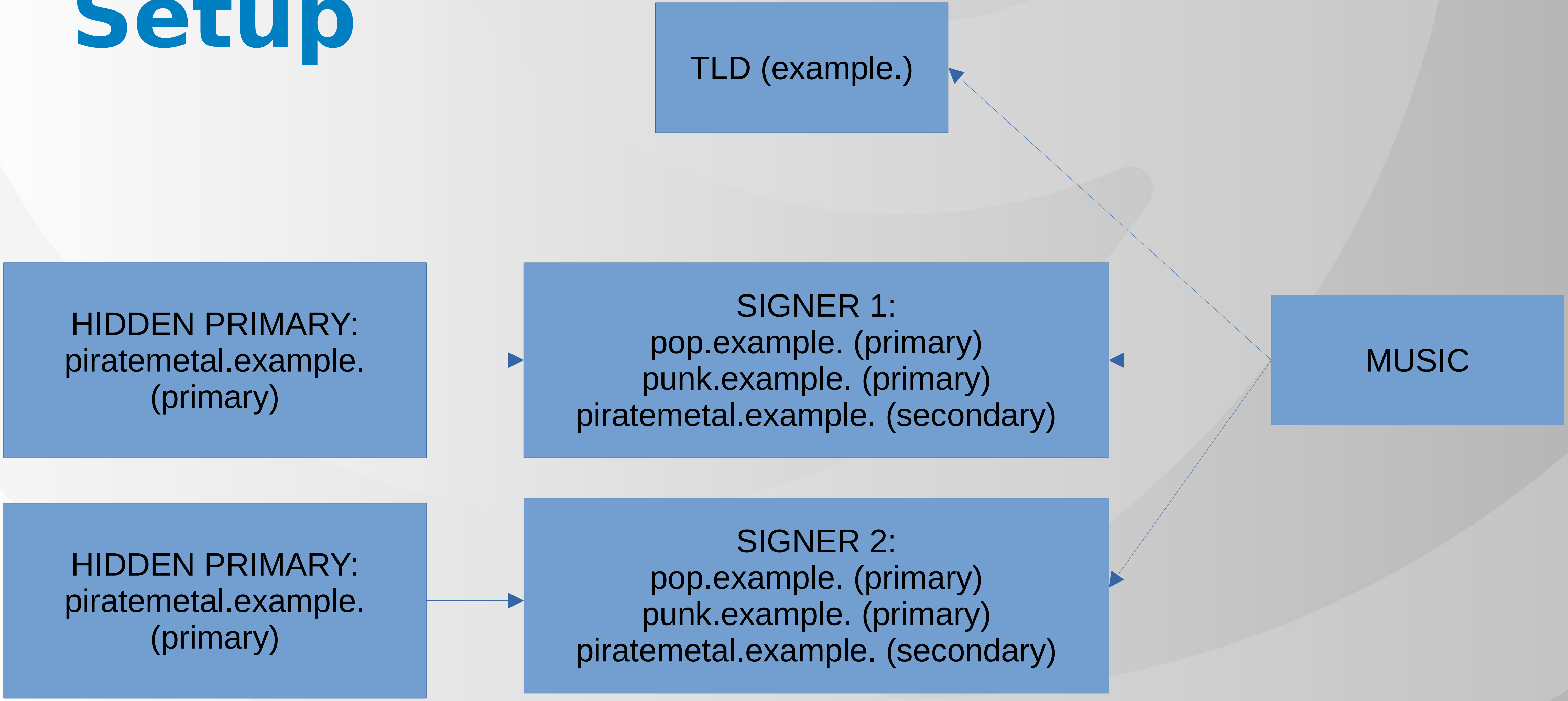
HIDDEN PRIMARY:
piratemetal.example.
(primary)

SIGNER 1:
pop.example. (primary)
punk.example. (primary)
piratemetal.example. (secondary)

MUSIC

- pop.example: primary, dnssec-policy
- punk.example: primary, dnssec-policy, inline-signing
- piratemetal.example: bump in the wire (secondary, d-p+i-s)

Setup



TLD (example.)

HIDDEN PRIMARY:
piratemetal.example.
(primary)

SIGNER 1:
pop.example. (primary)
punk.example. (primary)
piratemetal.example. (secondary)

MUSIC

HIDDEN PRIMARY:
piratemetal.example.
(primary)

SIGNER 2:
pop.example. (primary)
punk.example. (primary)
piratemetal.example. (secondary)

Let’s dance

SIGNER:
pop (primary)

pop:
SOA **+ RRSIG**
NS **+ RRSIG**
A **+ RRSIG**
AAAA **+ RRSIG**
DNSKEY + RRSIG
NSEC + RRSIG
CDS + RRSIG
CDNSKEY + RRSIG

Duncan Laurence

Singer joins a MUSIC group

- Confirm signer meets prerequisites
- Establish a trust mechanism (TSIG)
- Add ZSK for each signer to all signers
- Publish CDS/CDNSKEY RRset
- Wait for parent to publish the DS RRset
- Remove CDS/CDNSKEY RRset
- Wait DS-Wait-Time and DNSKEY-Wait-Time
- Compile NS RRset and publish
- Publish CSYNC record on all signers
- Wait for parent to publish NS RRset
- Remove CSYNC records

Singer joins a MUSIC group

```
$ music-cli zone step-fsm -z pop.example
Zone pop.example. transitioned from 'signers-unsynced' to 'dnskeys-synced'
$ music-cli zone step-fsm -z pop.example
Zone pop.example. transitioned from 'dnskeys-synced' to 'cds-added'
$ music-cli zone step-fsm -z pop.example
Zone pop.example. transitioned from 'cds-added' to 'parent-ds-synced'
$ music-cli zone step-fsm -z pop.example
pop.example.: PreCondition for 'nses-synced' failed. Current stop reason: Largest TTL found was
3600, waiting until 2023-05-17 10:33:06.728013291 +0200 CEST m=+76014.551034185 (4.999996303s)
$ music-cli zone step-fsm -z pop.example
Zone pop.example. transitioned from 'parent-ds-synced' to 'nses-synced'
$ music-cli zone step-fsm -z pop.example
Zone pop.example. transitioned from 'nses-synced' to 'csync-added'
$ music-cli zone step-fsm -z pop.example
Zone pop.example. transitioned from 'csync-added' to 'parent-ns-synced'
$ music-cli zone step-fsm -z pop.example
Zone pop.example. transitioned from 'parent-ns-synced' to 'stop'
```

Singer joins a MUSIC group

- Yay! It works! But there are some quirks...

Issue #1: It works, sort of

- Yay! It works! But there are some quirks...
- BIND 9 expects key files for DNSKEYs
- But will ignore signing with keys if the key files are not found
- This only works because there are already keys that can sign the zone
- **FIX:** Existence of key files determines which are the signing keys

```
10.53.0.1#51016/key ns2: updating zone 'pop.example/IN': update section prescan OK
10.53.0.1#51016/key ns2: updating zone 'pop.example/IN': prerequisites are OK
10.53.0.1#51016/key ns2: updating zone 'pop.example/IN': adding an RR at 'pop.example' DNSKEY 257...
10.53.0.1#51016/key ns2: updating zone 'pop.example/IN': adding an RR at 'pop.example' DNSKEY 256...
10.53.0.1#51016/key ns2: updating zone 'pop.example/IN': checking for NSEC3PARAM changes
dns_dnssec_findzonekeys2: error reading dnssec/Kpop.example.+013+58516.private: file not found
dns_dnssec_findzonekeys2: error reading dnssec/Kpop.example.+013+15496.private: file not found
```

Issue #2: Auto CDS/CDNSKEY

- Some time later keymgr is executed, CDS and CDNSKEY are put back
- Only for our KSK
- And this is problematic for CDS scanners
- **WORKAROUND:** keep CDS/CDNSKEY RRset published
- **FIX:** Add options *cds-digest-types* and *cdnskey* to *dnssec-policy*
- Allows you to disable automatic CDS and CDNSKEY publication

```
$ dig @10.53.0.1 cdnskey pop.example +short
$ dig @10.53.0.1 cds pop.example +short

$ rndc loadkeys pop.example

$ dig @10.53.0.1 cdnskey pop.example +short
257 3 13 d+On8GPusydWgz4Dk9LAB3rY6CvQ7nWTSM07OM3xMmLR3an3hQ7I6vkg nv+ddNDZPwRKqSWYocKGrOfVq3gJ7g==
$ dig @10.53.0.1 cds pop.example +short
38504 13 2 E3108BBE573CF315AE19B47CEF2A981CCBBD9E56D9F507B243282F2E 9A55EF20
```

Now the fun part: inline-signing

SIGNER:
punk (primary, **inline-signing**)

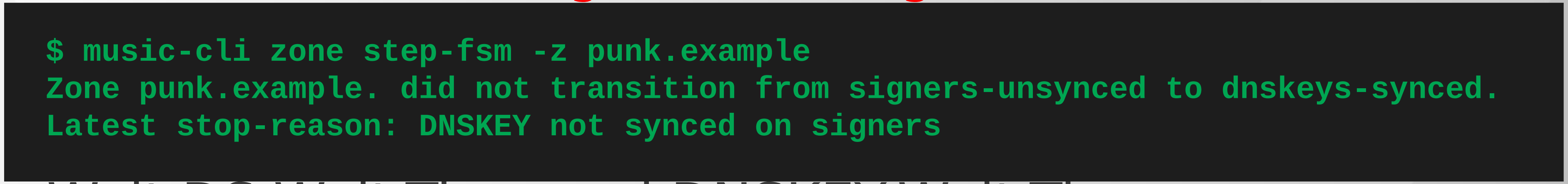
punk:
SOA
NS
A
AAAA

punk (signed):
SOA **+ RRSIG**
NS **+ RRSIG**
A **+ RRSIG**
AAAA **+ RRSIG**
DNSKEY + RRSIG
NSEC + RRSIG
CDS + RRSIG
CDNSKEY + RRSIG

Prins S. en de Geit – Wanneer punk geen muziek is

Singer joins a MUSIC group

- Confirm signer meets prerequisites
- Establish a trust mechanism (TSIG)
- Add ZSK for each signer to all signers



```
$ music-cli zone step-fsm -z punk.example
Zone punk.example. did not transition from signers-unsynced to dnskeys-synced.
Latest stop-reason: DNSKEY not synced on signers
```

- Wait DS-Wait-Time and DNSKEY-Wait-Time
- Compile NS RRset and publish
- Publish CSYNC record on all signers
- Wait for parent to publish NS RRset
- Remove CSYNC records

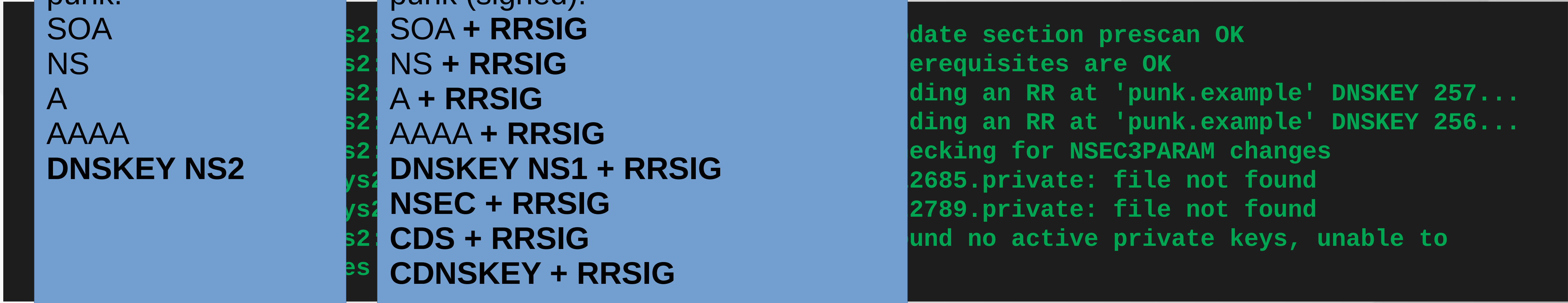
Issue #3: No signing keys found

- When adding DNSKEY records with dynamic update
- BIND 9 looks up the key files to be used for signing
- But we don’t have the key files for keys from the other provider
- With inline-signing, our DNSKEY RRs are added to the signed zone

```
10.53.0.1#33200/key ns2: updating zone 'punk.example/IN': update section prescan OK
10.53.0.1#33200/key ns2: updating zone 'punk.example/IN': prerequisites are OK
10.53.0.1#33200/key ns2: updating zone 'punk.example/IN': adding an RR at 'punk.example' DNSKEY 257...
10.53.0.1#33200/key ns2: updating zone 'punk.example/IN': adding an RR at 'punk.example' DNSKEY 256...
10.53.0.1#33200/key ns2: updating zone 'punk.example/IN': checking for NSEC3PARAM changes
dns_dnssec_findzonekeys2: error reading Kpunk.example.+013+12685.private: file not found
dns_dnssec_findzonekeys2: error reading Kpunk.example.+013+22789.private: file not found
10.53.0.1#33200/key ns2: updating zone 'punk.example/IN': found no active private keys, unable to
generate any signatures
```

Issue #3: No signing keys found

- When adding DNSKEY records with dynamic update
- BIND 9 looks up the key files to be used for signing
- But we don’t have the key files for keys from the other provider
- With inline-signing, our DNSKEY RRs are added to the signed zone



```
s2:   date section prescan OK
s2:   erequisites are OK
s2:   ding an RR at 'punk.example' DNSKEY 257...
s2:   ding an RR at 'punk.example' DNSKEY 256...
s2:   ecking for NSEC3PARAM changes
ys2   2685.private: file not found
ys2   2789.private: file not found
s2:   und no active private keys, unable to
es
```

punk:
SOA
NS
A
AAAA
DNSKEY NS2

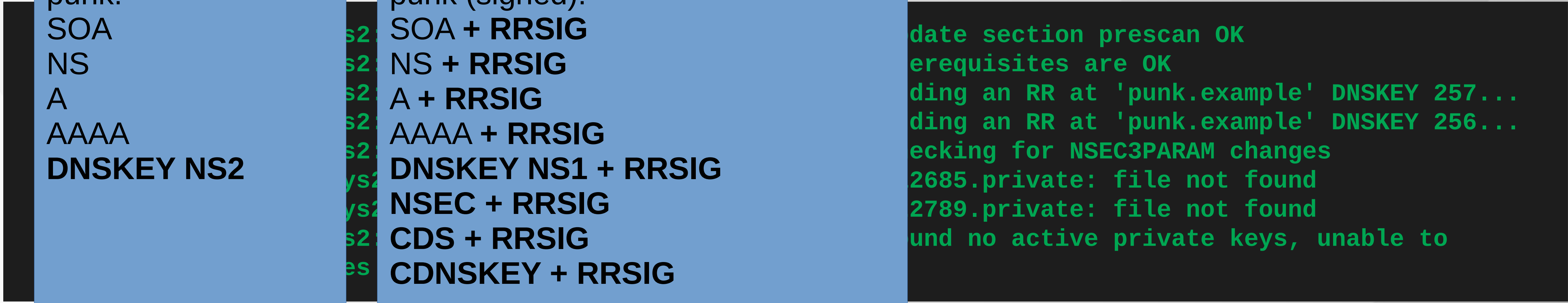
punk (signed):
SOA **+ RRSIG**
NS **+ RRSIG**
A **+ RRSIG**
AAAA **+ RRSIG**
DNSKEY NS1 + RRSIG
NSEC + RRSIG
CDS + RRSIG
CDNSKEY + RRSIG

Issue #3: No signing keys found

- When adding DNSKEY records with dynamic update
- BIND 9 looks up the key files to be used for signing
- But we don’t have the key files for keys from the other provider
- With inline-signing, our DNSKEY RRs are added to the signed zone
- **FIX:** Don’t try to sign the unsigned version of the zone

punk:
SOA
NS
A
AAAA
DNSKEY NS2

punk (signed):
SOA + **RRSIG**
NS + **RRSIG**
A + **RRSIG**
AAAA + **RRSIG**
DNSKEY NS1 + RRSIG
NSEC + RRSIG
CDS + RRSIG
CDNSKEY + RRSIG



```
s2:   date section prescan OK
s2:   erequisites are OK
s2:   ding an RR at 'punk.example' DNSKEY 257...
s2:   ding an RR at 'punk.example' DNSKEY 256...
s2:   ecking for NSEC3PARAM changes
ys2   2685.private: file not found
ys2   2789.private: file not found
s2:   und no active private keys, unable to
es
```

Issue #4: Other keys not added

- Still the same error:

```
$ music-cli zone step-fsm -z punk.example
Zone punk.example. did not transition from signers-unsynced to dnskeys-synced.
Latest stop-reason: DNSKEY not synced on signers
```

- With inline-signing, DNSSEC records are not synced between unsigned and signed zone
  - DNSKEY, CDS, CDNSKEY, RRSIG, NSEC, NSEC3
- **FIX:** Allow syncing of DNSKEY (also CDS/CDNSKEY)

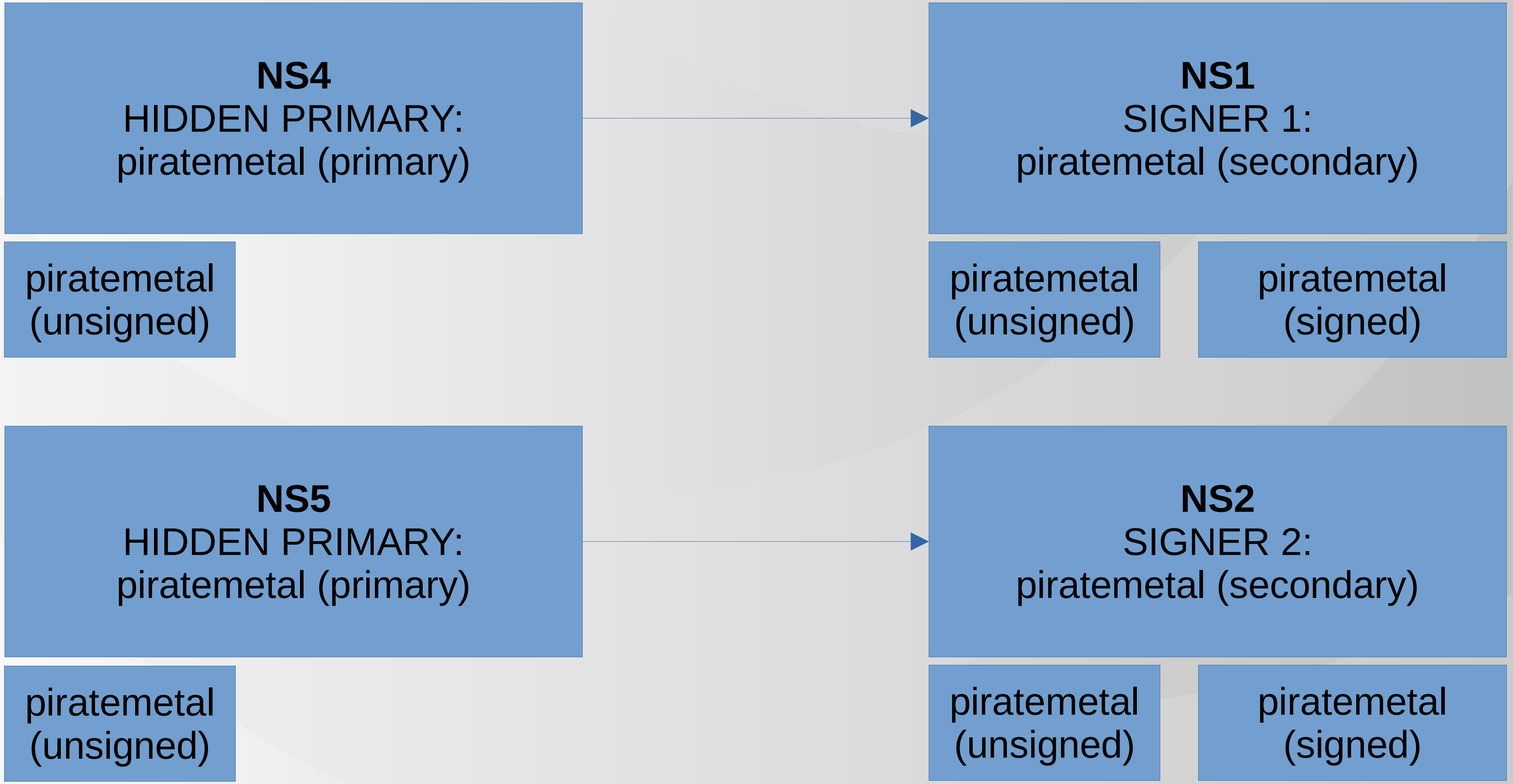
- But make sure that we don’t remove our own DNSKEY
- **FIX:** Add check if this key is in use (check key files)

Singer joins a MUSIC group

```
$ music-cli zone step-fsm -z punk.example
Zone punk.example. transitioned from 'signers-unsynced' to 'dnskeys-synced'
$ music-cli zone step-fsm -z punk.example
Zone punk.example. transitioned from 'dnskeys-synced' to 'cds-added'
$ music-cli zone step-fsm -z punk.example
Zone punk.example. transitioned from 'cds-added' to 'parent-ds-synced'
$ music-cli zone step-fsm -z punk.example
punk.example.: PreCondition for 'nses-synced' failed. Current stop reason: Largest TTL found was
3600, waiting until 2023-05-17 16:24:26.009560793 +0200 CEST m=+97093.832581692 (4.999996763s)
$ music-cli zone step-fsm -z punk.example
Zone punk.example. transitioned from 'parent-ds-synced' to 'nses-synced'
$ music-cli zone step-fsm -z punk.example
Zone punk.example. transitioned from 'nses-synced' to 'csync-added'
$ music-cli zone step-fsm -z punk.example
$ music-cli zone step-fsm -z punk.example
Zone punk.example. transitioned from 'csync-added' to 'parent-ns-synced'
$ music-cli zone step-fsm -z punk.example
Zone punk.example. transitioned from 'parent-ns-synced' to 'stop'
```

Let’s go crazy: bump in the wire

Let’s go crazy: bump in the wire



NS4
HIDDEN PRIMARY:
piratemetal (primary)

piratemetal
(unsigned)

NS1
SIGNER 1:
piratemetal (secondary)

piratemetal
(unsigned)

piratemetal
(signed)

NS5
HIDDEN PRIMARY:
piratemetal (primary)

piratemetal
(unsigned)

NS2
SIGNER 2:
piratemetal (secondary)

piratemetal
(unsigned)

piratemetal
(signed)

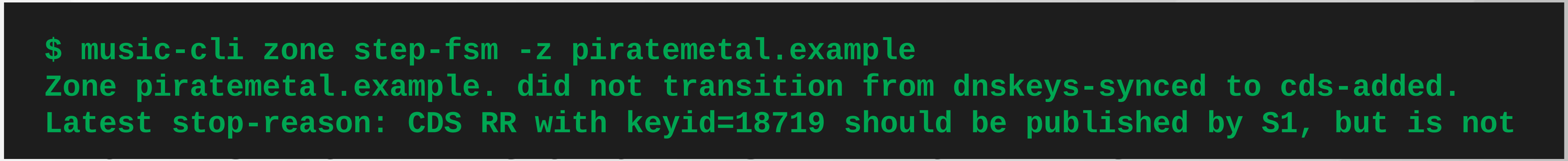
Let’s go crazy: bump in the wire

```
zone "piratemetal.example." {
        type primary;
        file "db/piratemetal.example.db";
        allow-update { ns1; };
        also-notify { 10.53.0.1; };
};
```

```
zone "piratemetal.example." {
        type secondary;
        primaries { 10.53.0.4; };
        file "db/piratemetal.example.db";
        dnssec-policy music;
        inline-signing yes;
        allow-update-forwarding { ns1; };
};
```

Singer joins a MUSIC group

- Confirm signer meets prerequisites
- Establish a trust mechanism (TSIG)
- Add ZSK for each signer to all signers
- Publish CDS/CDNSKEY RRset



```
$ music-cli zone step-fsm -z piratemetal.example
Zone piratemetal.example. did not transition from dnskeys-synced to cds-added.
Latest stop-reason: CDS RR with keyid=18719 should be published by S1, but is not
```

- Compile NS RRset and publish
- Publish CSYNC record on all signers
- Wait for parent to publish NS RRset
- Remove CSYNC records

Issue #5: Bad CDS RRset

- BIND 9 does not allow CDS/CDNSKEY if there is not a good DNSKEY RR
- That is, there needs to be a DNSKEY record with the same algorithm
- But this hidden primary is not signing (remember: bump in the wire)
- **WORK AROUND:** Add own DNSKEY records to primary zone

```
10.53.0.1#39666: updating zone 'piratemetal.example/IN': update section prescan OK
10.53.0.1#39666: updating zone 'piratemetal.example/IN': prerequisites are OK
10.53.0.1#39666: updating zone 'piratemetal.example/IN': adding an RR at 'piratemetal.example' CDS 18719…
10.53.0.1#39666: updating zone 'piratemetal.example/IN': adding an RR at 'piratemetal.example' CDNSKEY…
10.53.0.1#39666: updating zone 'piratemetal.example/IN': update rejected: bad CDS RRset
```

Singer joins a MUSIC group

```
$ music-cli zone step-fsm -z piratemetal.example
Zone piratemetal.example. transitioned from 'signers-unsynced' to 'dnskeys-synced'
$ music-cli zone step-fsm -z piratemetal.example
Zone piratemetal.example. transitioned from 'dnskeys-synced' to 'cds-added'
$ music-cli zone step-fsm -z piratemetal.example
Zone piratemetal.example. transitioned from 'cds-added' to 'parent-ds-synced'
$ music-cli zone step-fsm -z piratemetal.example
piratemetal.example.: PreCondition for 'nses-synced' failed. Current stop reason: Largest TTL
found was 3600, waiting until 2023-05-17 16:24:26.009560793 +0200 CEST m=+97093.832581692
(4.999996763s)
$ music-cli zone step-fsm -z piratemetal.example
Zone piratemetal.example. transitioned from 'parent-ds-synced' to 'nses-synced'
$ music-cli zone step-fsm -z piratemetal.example
Zone piratemetal.example. transitioned from 'nses-synced' to 'csync-added'
$ music-cli zone step-fsm -z piratemetal.example
Zone piratemetal.example. transitioned from 'csync-added' to 'parent-ns-synced'
$ music-cli zone step-fsm -z piratemetal.example
Zone piratemetal.example. transitioned from 'parent-ns-synced' to 'stop'
```

Singer leaves a MUSIC group

- Remove signer’s NS records from signers
- Publish CSYNC record on all signers
- Wait for parent to update NS RRset
- Remove CSYNC records
- Wait NS-Wait-Time
- Remove zone from leaving signer
- Publish new CDS/CDNSKEY RRset
- Update DNSKEY RRset
- Wait for parent to update DS RRset
- Remove CDS/CDNSKEY RRset

```
$ music-cli signer leave -s S2 -g MUSIC
Signer S2 is in pending removal from signer group MUSIC and
therefore 3 zones entered the 'remove-signer' process.
```

Singer leaves a MUSIC group

- No issues with pop and punk
- But when the singer leaves a pirate metal band there are issues

Issue #6: NS record ownership

- Signer must be able to differentiate between NS records that are updated by itself and NS records that receive updates from other signers.
- I don’t think this is a very common property in DNS servers
- This was only an issue I ran into in a more complex setup

```
$ music-cli zone step-fsm -z piratemetal.example
piratemetal.example.: PreCondition for 'csync-added' failed. Current stop reason: NS
ns2.piratemetal.example. still exists in signer S2

Latest stop-reason: NS ns2.piratemetal.example. still exists in signer S2
```

Hold tight, almost done (recap)

- Supporting multi-signer environments is more complex than first meets the eye
- Model 2 with centralized controller
- Many fixes in BIND 9 that make the experience nicer
  - Better key management
  - More control over CDS/CDNSKEY
  - Fixes scheduled for (no promises)
    - BIND 9.18.16-S, BIND 9.19.14

Suggested configuration

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


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

Next steps

- MUSIC:
  - Reporting encountered bugs
  - Key rollover scenarios
    - ZSK rollover
    - KSK rollover
    - Algorithm rollover
- BIND 9: Testing key rollovers
- Contributing to draft-ietf-dnsop-dnssec-automation

Thank you!

- Main 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