A Proposed Framework for Distributed Multi-Signer

ICANN 82 – DNSSEC Workshop
March 12, 2025

Johan Stenstam
Peter Thomassen

DNSSEC supports multiple keys

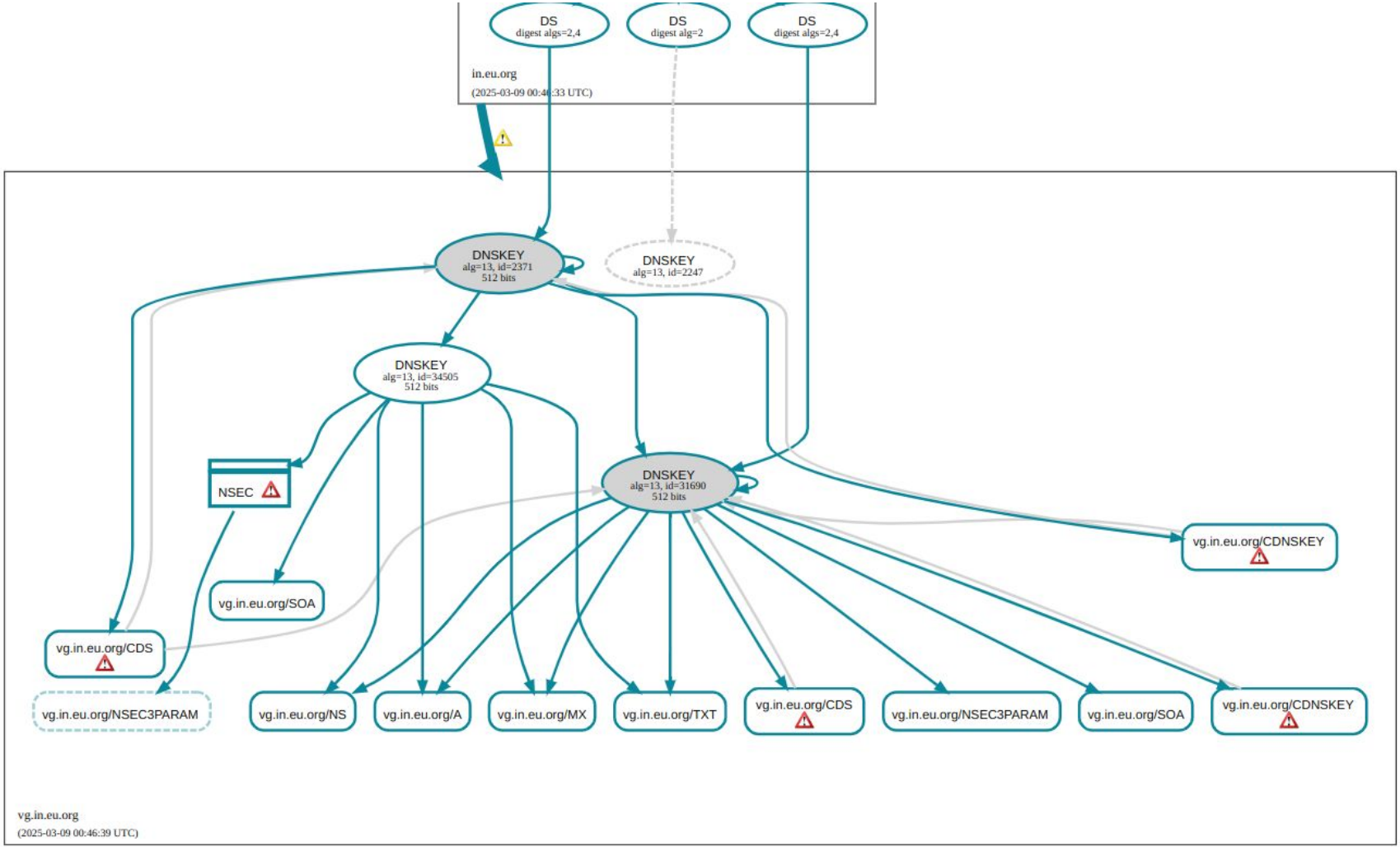
- You can **sign a single zone with multiple keys**
  - Just add more DNSKEY & DS, signatures etc. ... but there are many rules to observe
- There are good reasons to do that:
  - Transition period while changing keys
  - Pre-publishing a backup key
  - Exercise an additional experimental algorithm
  - **Transition period during provider change** ← “temporary multi-signer”
  - **Parallel operations by several signing providers** ← “permanent multi-signer”
- Nothing new (was always allowed by the specs)
  - From resolver perspective, **all looks like multi-key**

The Multi-Signer Complication

– – –

- Delegations have several nameservers → some queries go here, some go there
- **Critical constraint:** Coordinate so that data from different NS fits together
- Example: Fetch and validate an A/AAAA records
  1. **Fetch DNSKEY record** from **ns1.providerA**
  2. **Fetch A record** from **ns1.providerA**
  3. **Fetch AAAA record** from **ns-a.other-providerB**

  → **DNSKEY providers MUST import each other's public keys** (RFC 8901) to allow validating *any* signature, regardless of DNSKEY source


DS
digest algs=2,4
DS
digest alg=2
DS
digest algs=2,4
in.eu.org
(2025-03-09 00:46:33 UTC)
DNSKEY
alg=13, id=2371
512 bits
DNSKEY
alg=13, id=2247
DNSKEY
alg=13, id=34505
512 bits
NSEC
DNSKEY
alg=13, id=31690
512 bits
vg.in.eu.org/CDNSKEY
vg.in.eu.org/SOA
vg.in.eu.org/CDS
vg.in.eu.org/NSEC3PARAM
vg.in.eu.org/NS
vg.in.eu.org/A
vg.in.eu.org/MX
vg.in.eu.org/TXT
vg.in.eu.org/CDS
vg.in.eu.org/NSEC3PARAM
vg.in.eu.org/SOA
vg.in.eu.org/CDNSKEY
vg.in.eu.org
(2025-03-09 00:46:39 UTC)

Multi-Signer Coordination Requirements

– – –

Signers' collaboration …

- must be sufficiently robust to deal with **on- and offboarding of signers**
- must include **automated management of shared records** (NS, DNSKEY, DS, …)
- must be able to **manage parent-side delegation data** (if authorized by owner)

… across multiple organizations.

No (reliable) way to get this right without automation.

Q: Where does it live?

Decentralized Architecture Overview (Proposal from .SE)

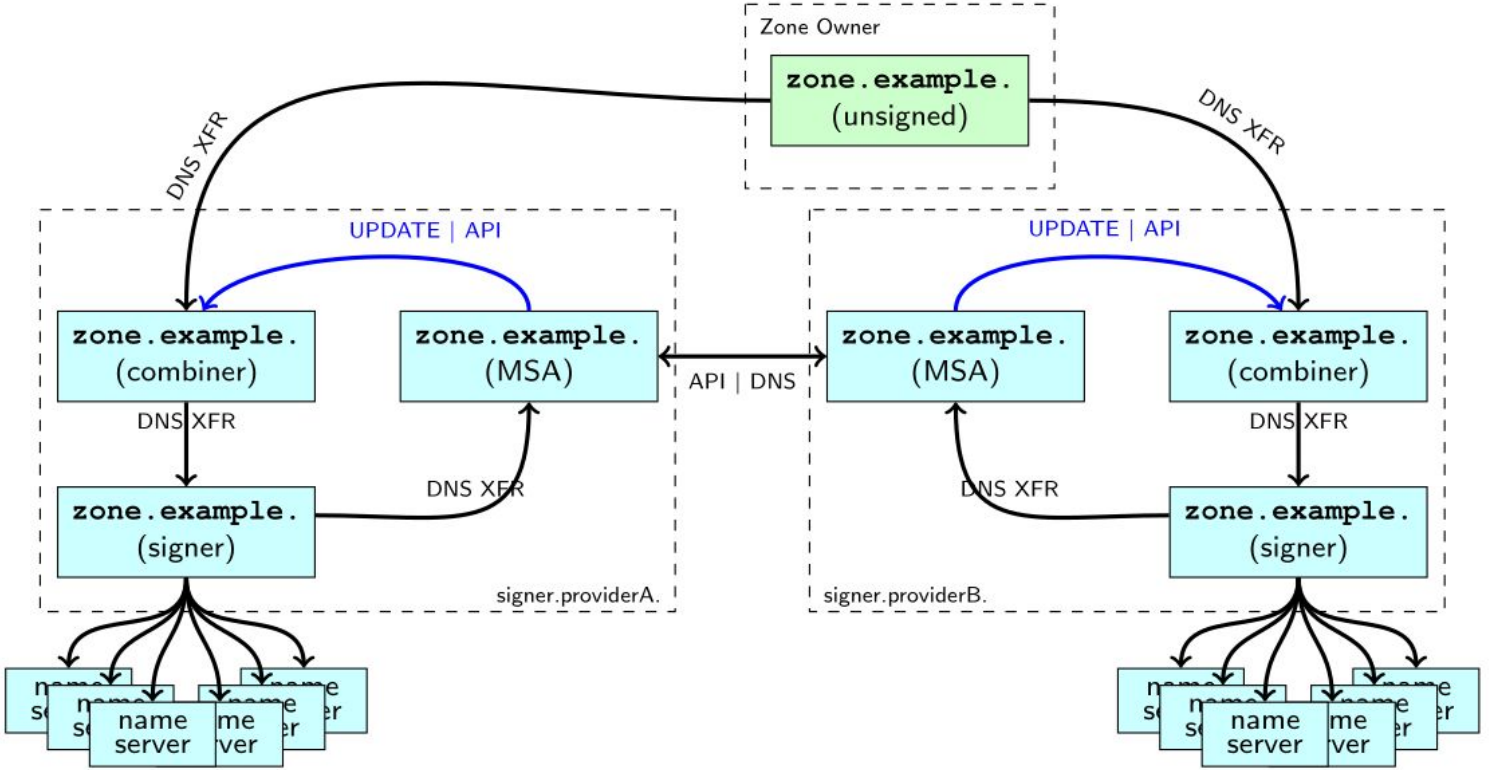


Diagram credits:
Johan Stenstam

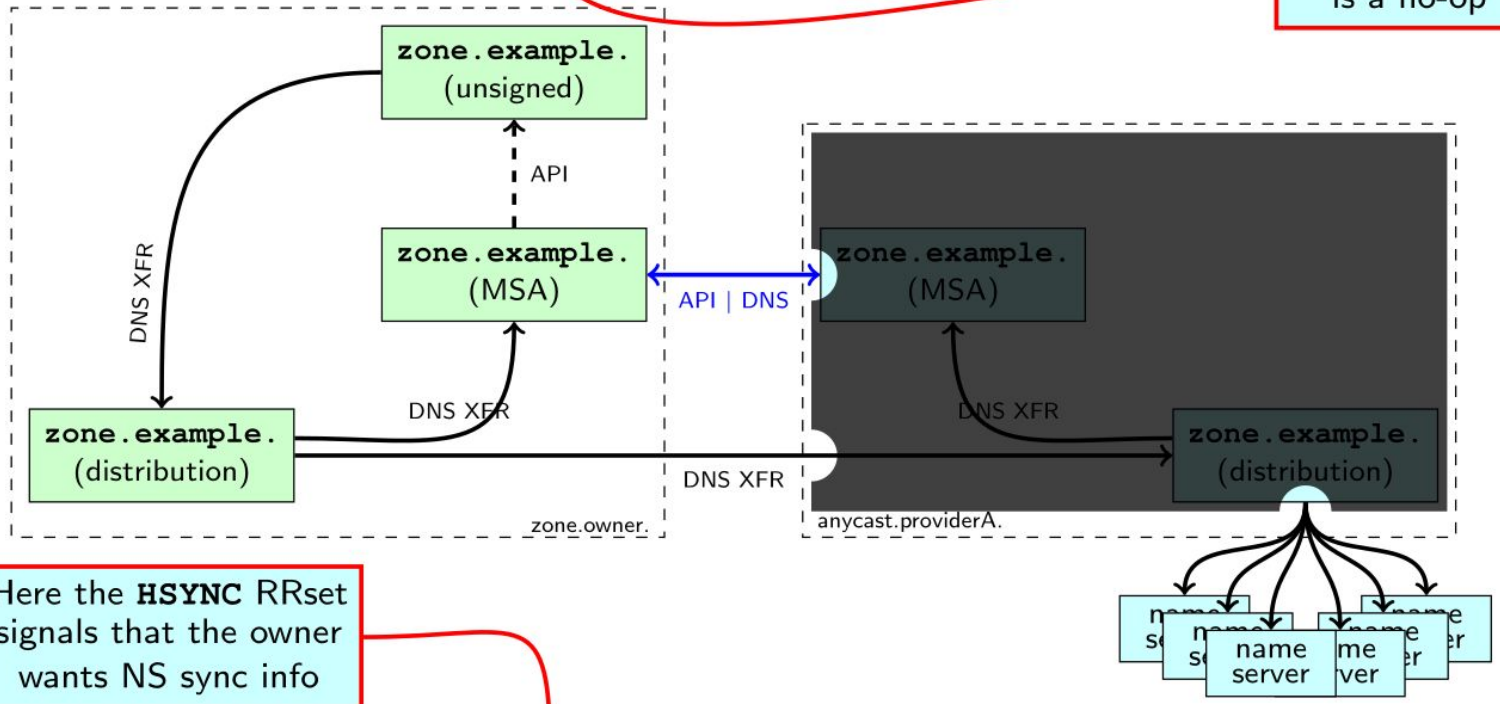
MSA Configuration: The HSYNC Record

- Five fields:
  - `STATE` ON/OFF: whether this DNS provider is onboarded/offboarded (target state)
  - `NSMGMT` OWNER/AGENT: whether parent-side NS are manual or automatic (CSYNC)
  - `SIGN` SIGN/NOSIGN: whether this DNS provider is a signer
  - `PROVIDER` domain name that identifies this DNS provider
  - `UPSTREAM` upstream DNS provider from which to ingest zone data (or "." for manual)
- Skeleton structure in a child zone:

```
zone.example. IN HSYNC {STATE} {NSMGMT} {SIGN} identity.providerA. UPSTREAM
zone.example. IN HSYNC {STATE} {NSMGMT} {SIGN} identity.providerB. UPSTREAM
zone.example. IN HSYNC {STATE} {NSMGMT} {SIGN} identity.providerC. UPSTREAM
```

```
zone.example. IN HSYNC ON OWNER NOSIGN  msa.anycast.providerA.  msa.zone.owner.
zone.example. IN HSYNC ON OWNER NOSIGN  msa.zone.owner.         .
```

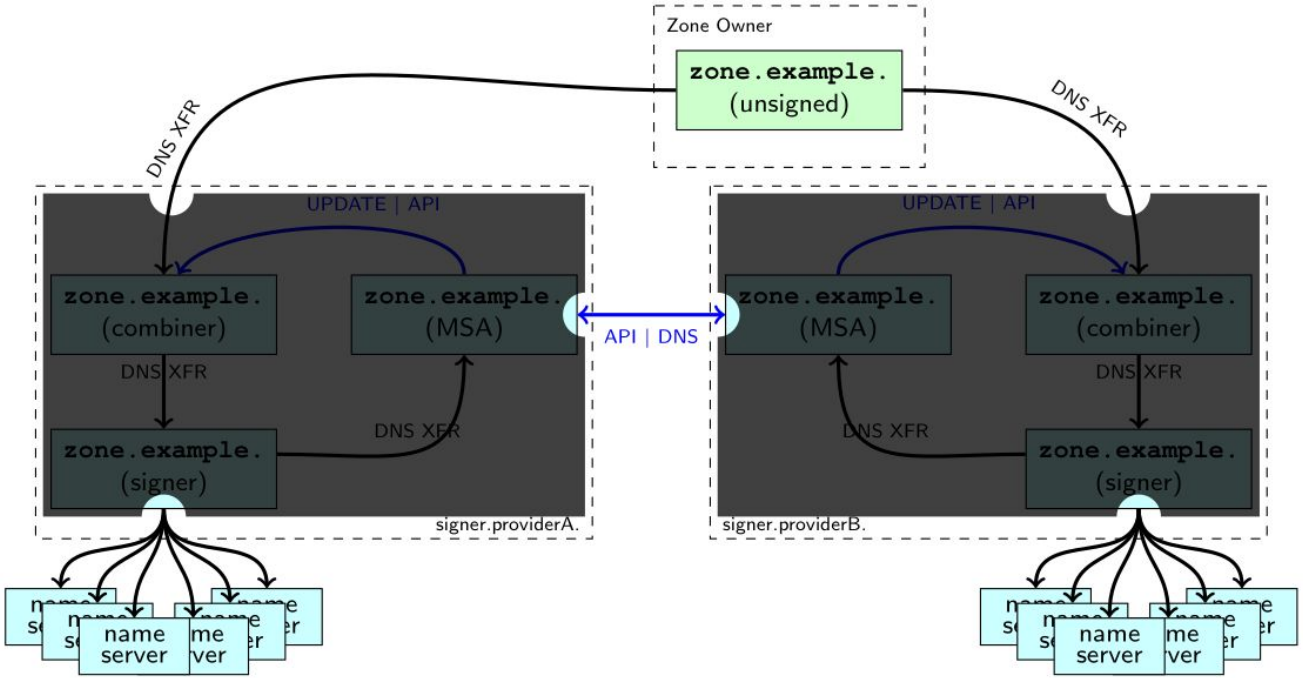
In this case the **HSYNC** RRset is a no-op



Here the **HSYNC** RRset signals that the owner wants NS sync info

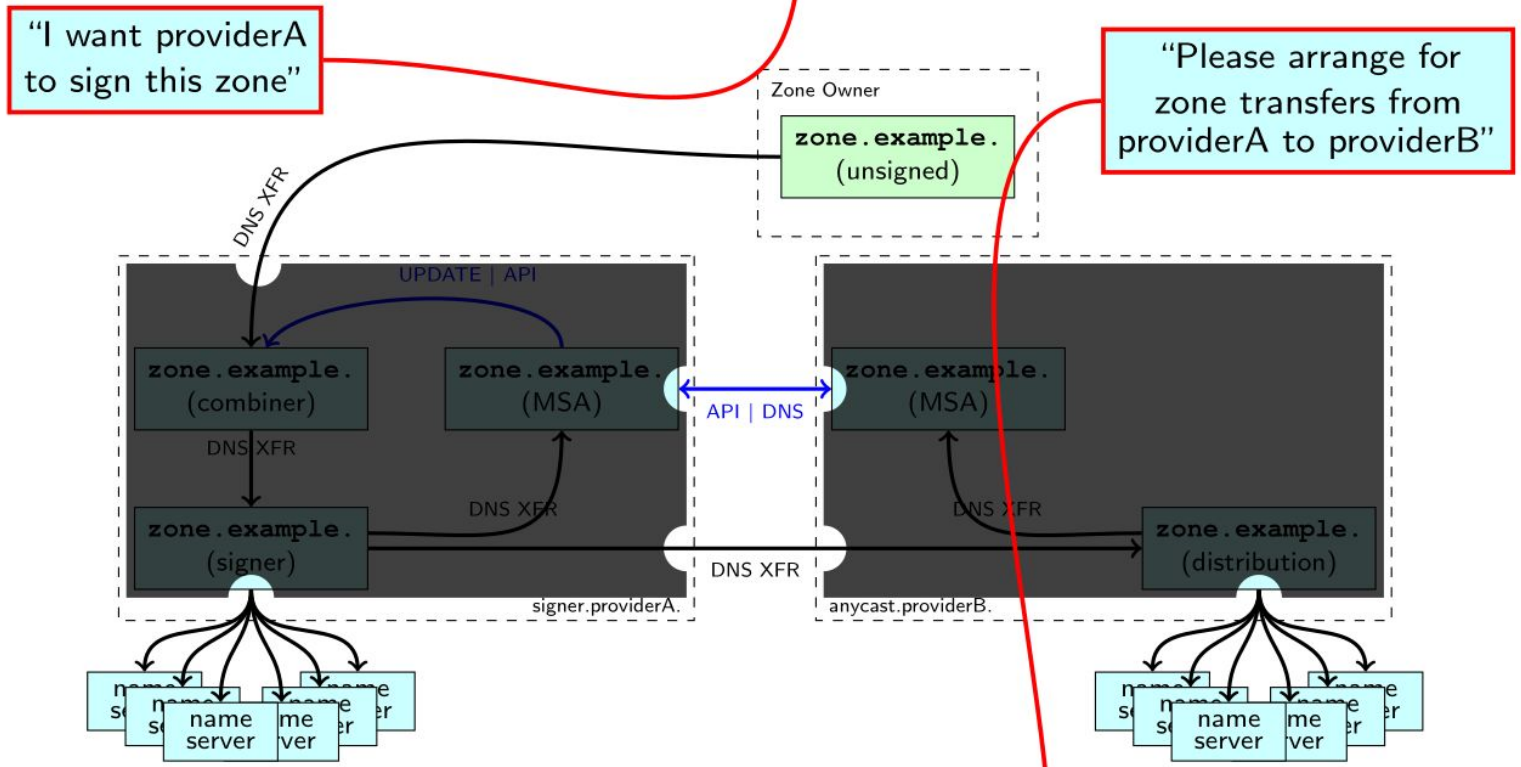
```
zone.example. IN HSYNC ON AGENT NOSIGN  msa.anycast.providerA.  msa.zone.owner.
zone.example. IN HSYNC ON AGENT NOSIGN  msa.zone.owner.         .
```

```
zone.example.   IN HSYNC ON OWNER SIGN  msa.signer.providerA.  .
zone.example.   IN HSYNC ON OWNER SIGN  msa.signer.providerB.  .
```




```
zone.example.   IN HSYNC ON AGENT SIGN  msa.signer.providerA.  .
zone.example.   IN HSYNC ON AGENT SIGN  msa.signer.providerB.  .
```

```
zone.example.   IN HSYNC ON OWNER  SIGN     msa.signer.providerA.  .
zone.example.   IN HSYNC ON OWNER  NOSIGN   msa.anycast.providerB. msa.signer.providerA.
```




```
zone.example.   IN HSYNC ON AGENT  SIGN     msa.signer.providerA.  .
zone.example.   IN HSYNC ON AGENT  NOSIGN   msa.anycast.providerB.  msa.signer.providerA.
```

Let's Discuss

– – –

- HSYNC records describes
  - each provider's role (gaining/losing? is this provider a signer?)
  - zone transfer relationships
  - whether the zone owner wishes to use CSYNC

Questions:

- Are these things best described in one structure?
- Are these things best described within the child zone?
- …?