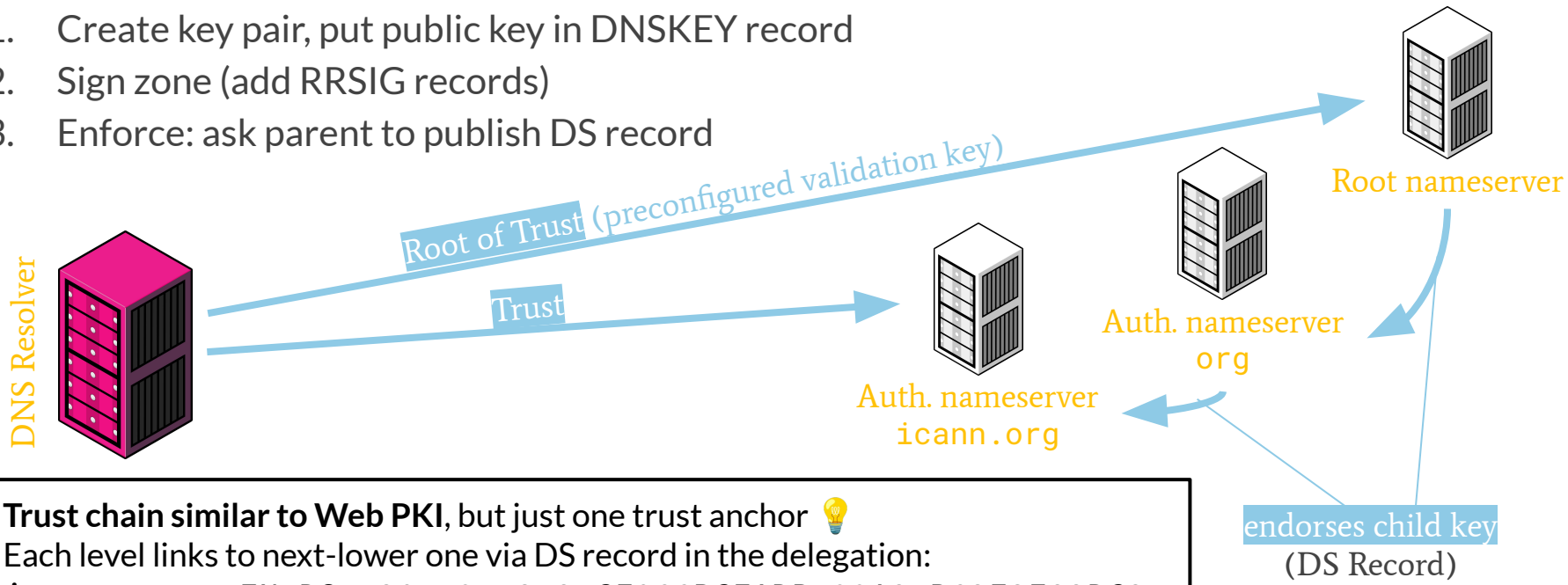
Multi-signer DNSSEC: What's coming

Peter Thomassen <peter@desec.io>

ICANN82 – Tech Day
March 10, 2025

Reminder: Typical DNSSEC setup

1. Create key pair, put public key in DNSKEY record
2. Sign zone (add RRSIG records)
3. Enforce: ask parent to publish DS record



Trust chain similar to Web PKI, but just one trust anchor 💡
Each level links to next-lower one via DS record in the delegation:

```
icann.org.  IN DS  20149 13 2 CF066BCEADB799A27B62E3E82DC2…
```

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**

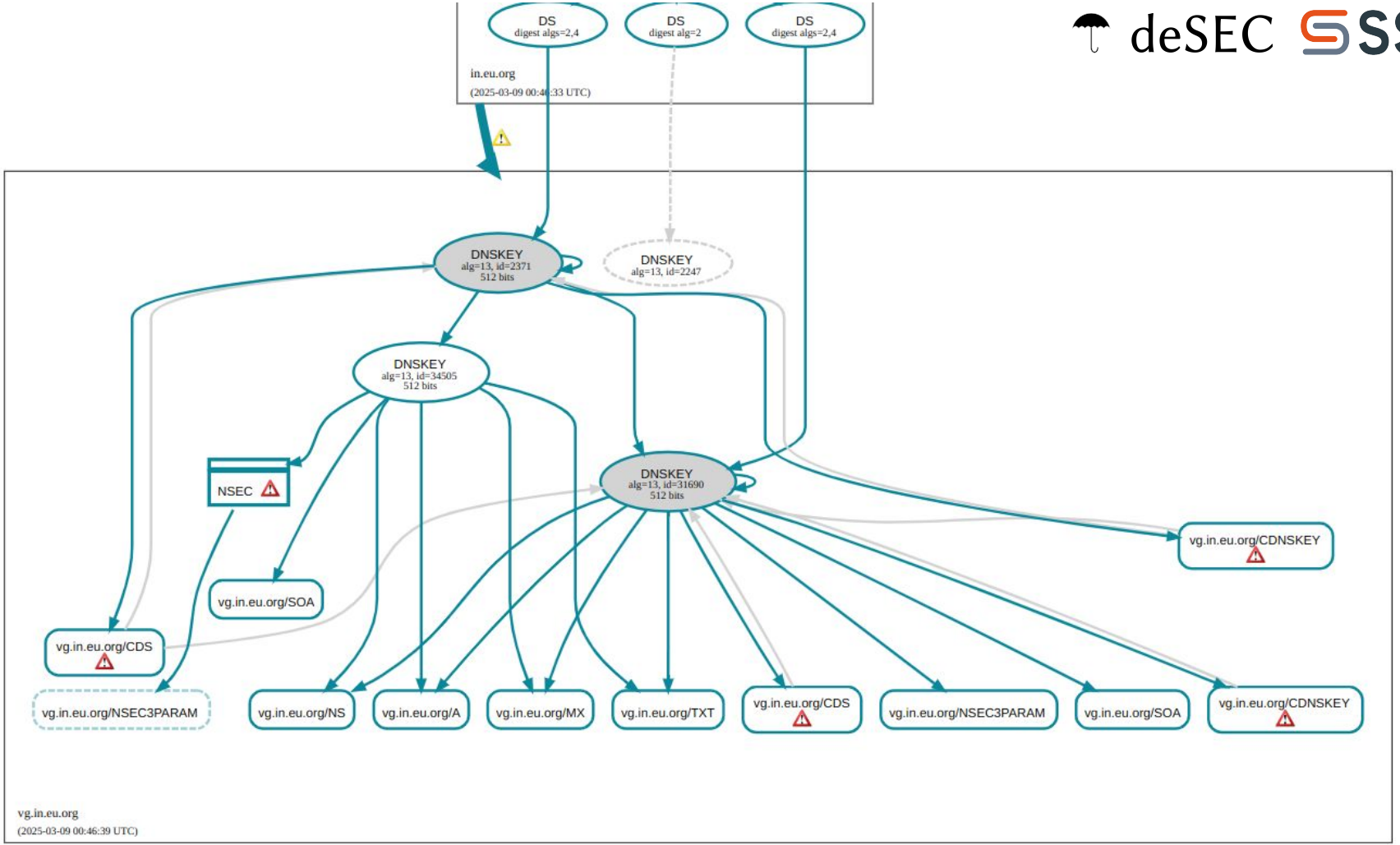
The Multi-Signer Complication

– – –

- 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

deSEC SSE


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)

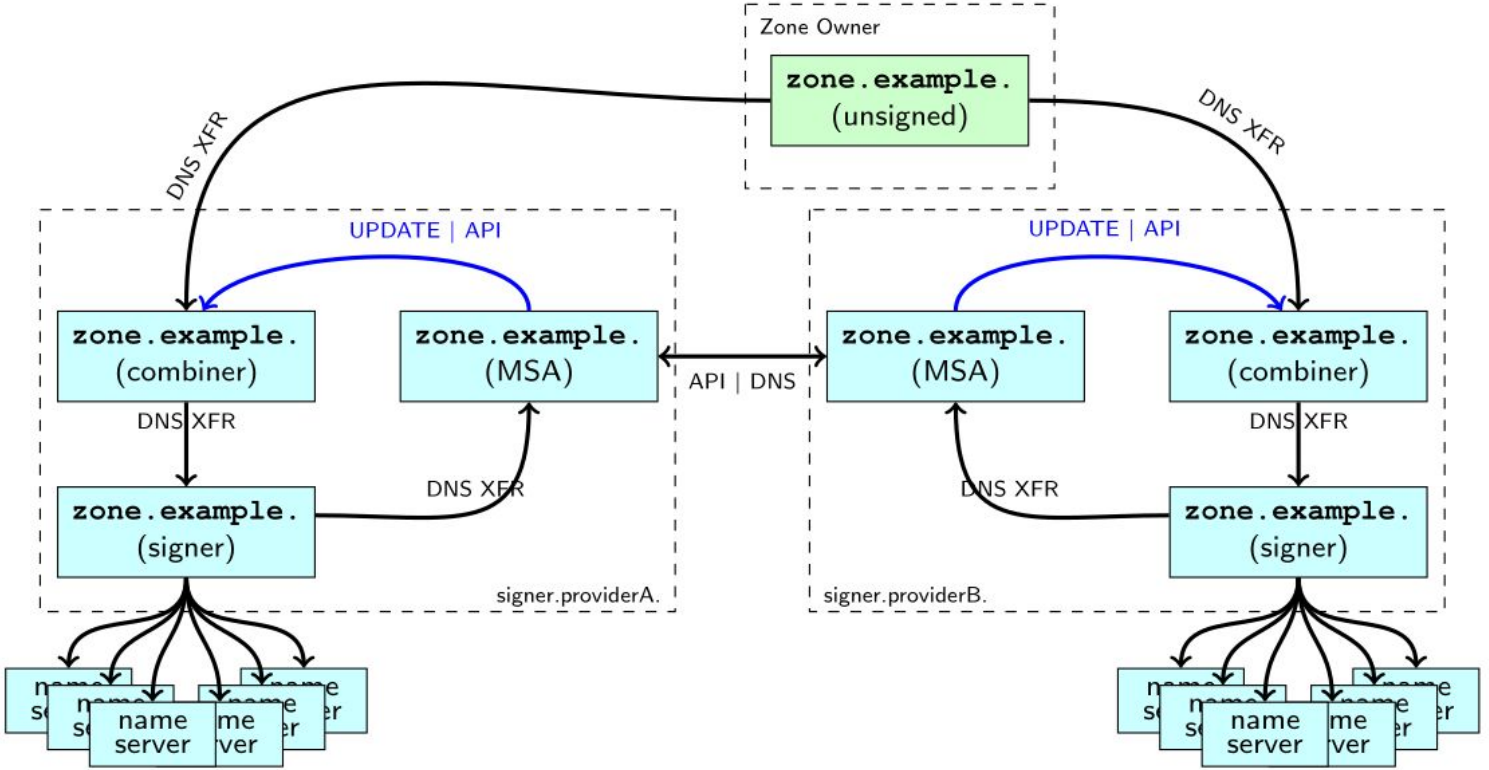


Diagram credits:
Johan Stenstam

Status & Testing

- Prototype being developed
  - Both combiner and Multi-Signer Agent (MSA) components
  - MSA actions configurable through HSYNC record
    → DNSSEC Workshop (Wednesday)
- Looking for parties interested in testing
- Also encompasses DS automation
  - Without DS automation, no multi-signer
  - Standards and implementations available
  - RFC 7344, RFC 9615; draft-ietf-dnsop-generalized-notify
- Interested? Reach out!

Thank you!

Questions?