

DNSSEC Validation

as part of

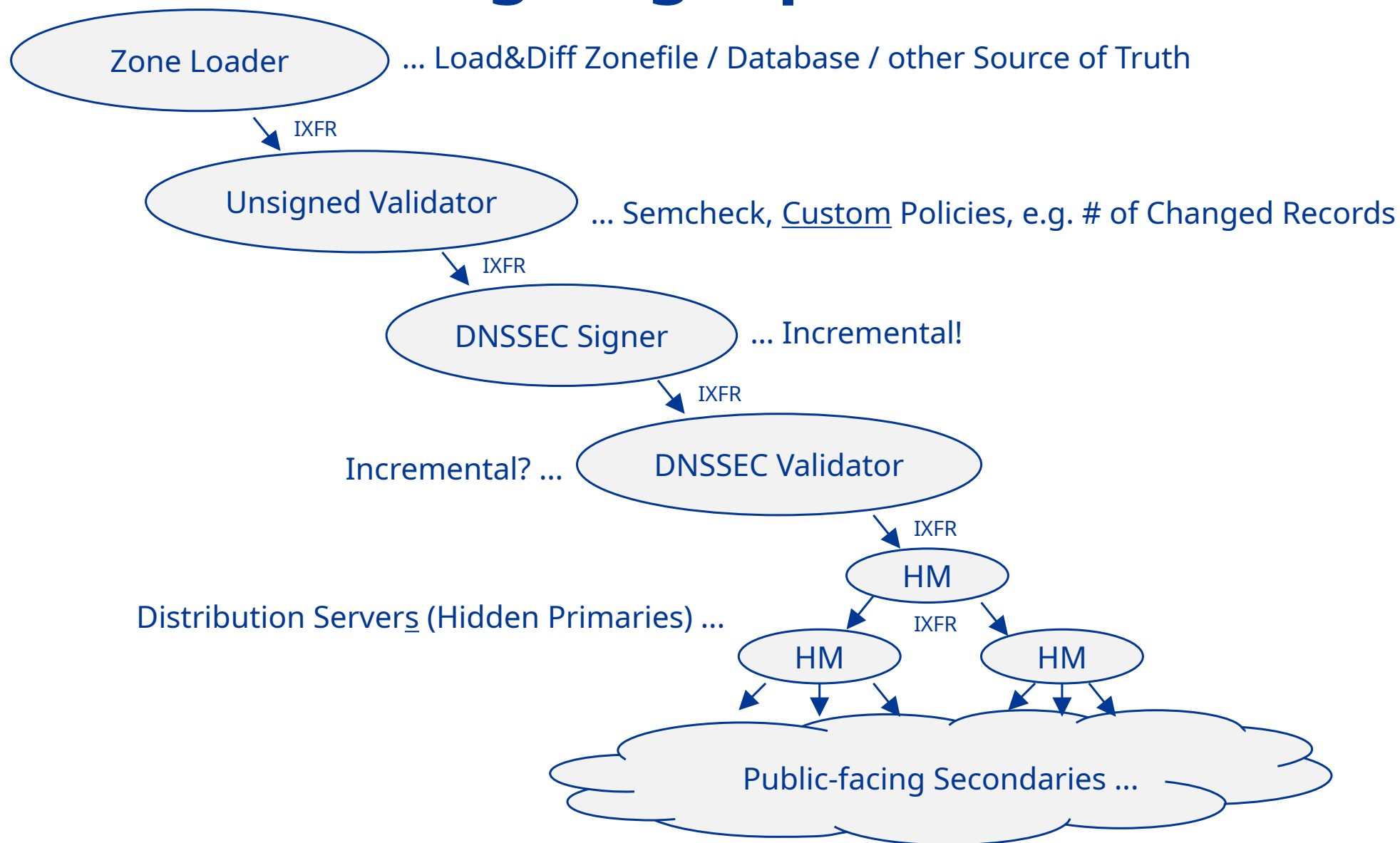
Signing Pipeline

Libor Peltan

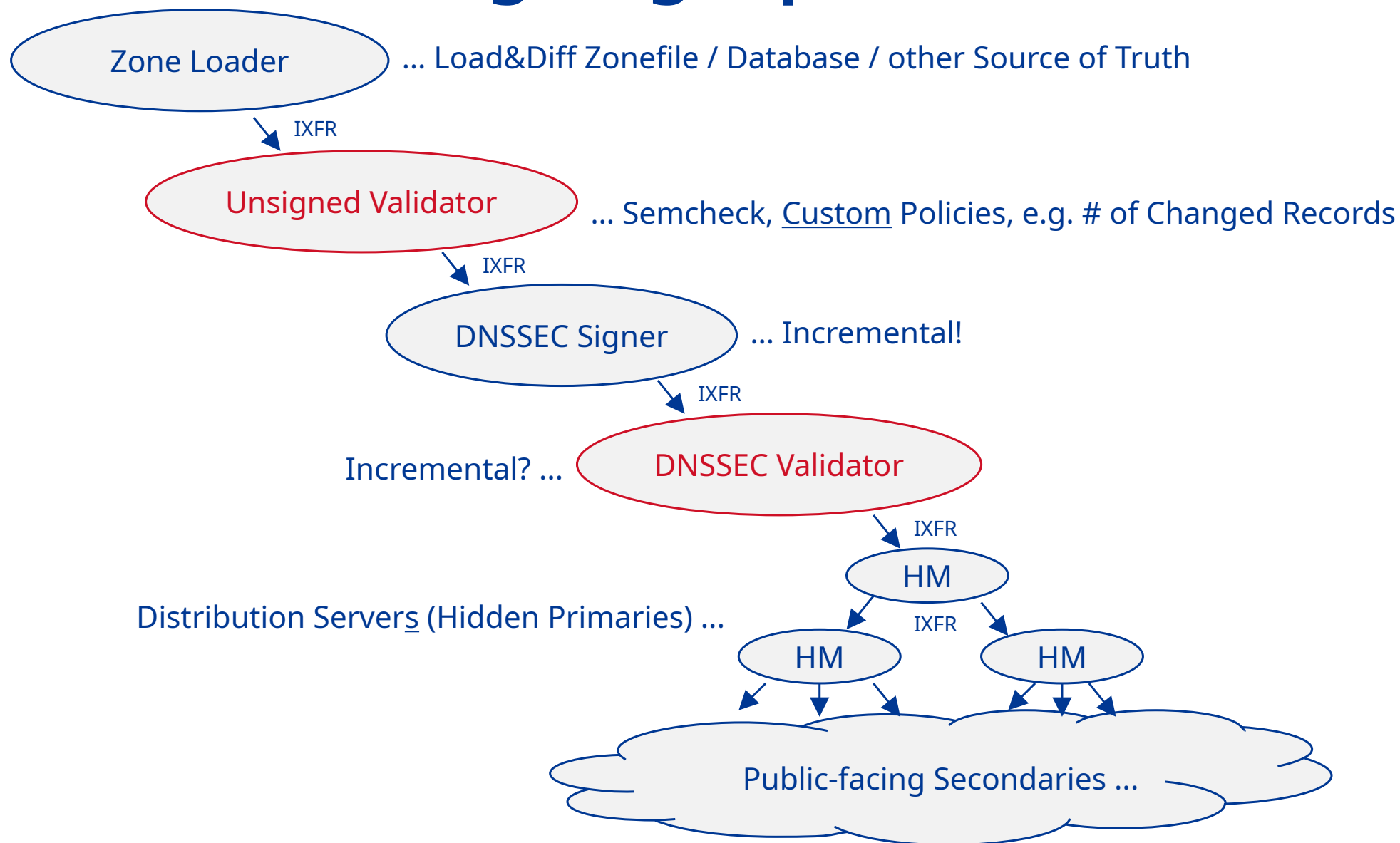
• 7. 10. 2025

- Small zone operation – 1 server
 - Zonefile load, DNSSEC signing, answering queries
- Big zone operation – 1 server per task
 - Or more (diversity and/or redundancy)
 - out of scope of talk
 - Zone Transfers, Incremental (IXFR)

Signing Pipeline



Signing Pipeline



Bump-in-the-Wire Validation

- Get new Version, validate, serve it
 - IXFR in, IXFR out
- Reject Failing Version
 - Send e-mail
- Continue serving Last Good Version
- Next Correct – Accept
 - How IXFR works

After-the-Fact Validation

- Example:
 - Frequently updated zone
 - Full (non-incremental) DNSSEC Validation
- Get new Version, serve it, validate
- Failure: send e-mail, panic, revert???

Problem #1

Calling External Tools from Pipeline

External Tool to Bump-in-the-Wire

- Little need of scripting
- Desired validation properties
- NSD 4.6+, previously CreDNS
 - Simple subprocess
- Knot DNS 3.5+
 - Separated daemon, sockets
- Cascade – see next presentation

NSD External Validation 1/2

- Simply system() call, outcome in ercode
- Params specification, incl. full zonefile

```
verify: enable: yes
```

```
zone:
```

```
  name: "example.com"
```

```
  verifier: drill -S -k example.com.ds @::1 -p 5432 example.com SOA
```

```
verify: enable: yes
```

```
verifier: ldns-verify-zone -V2
```

```
verifier-timeout: 10
```

```
verifier-feed-zone: yes
```

NSD External Validation 2/2

- No direct access to diff
- Validating script can IXFR from primary
- Still limited checks
 - Only new RRSIGs etc.

Knot DNS External Validation 1/2

- Need of external script
- ...and some configuration:

```
server:
    dbus-event: external-verify

external:
    - id: ldns
      timeout: 600
      dump-new-zone: /tmp/example.com.newzone

zone:
    - domain: example.com.
      master: signer
      external-validation: ldns
```

Knot DNS External Validation 2/2

- Continuously listen for specific DBus msg
- When triggered, verify
- Based on outcome, knotc commit/abort

```
gdbus monitor --system --dest cz.nic.knotd --object-path /cz/nic/knotd \  
| fgrep --line-buffered cz.nic.knotd.events.external_verify \  
| while IFS=" " read JUNK1 ZONE JUNK2; do  
    if ldns-verify-zone /tmp/${ZONE}newzone  
    then knotc zone-commit ${ZONE}  
    else knotc zone-abort ${ZONE}  
    fi  
done
```

Problem #2

How validate what

DNSSEC Validation

- Zone Scope
 - RRSIGs against DNSKEYs
 - NSEC(3) tree
- Delegation
 - DNSKEYs against DSs
 - For all NSs...
- Trust Chain
 - Useless beyond closest Delegation

DNSSEC Validation Tools

- Whole Zone Validation
 - Full & Textual (Zonefile)
 - Full
 - Incremental
- Validation by querying *something*
 - Zone Scope
 - Delegation
 - Whole Trust Chain / Complete Resolution

Full DNSSEC Validation

+ Diversity of Tools

- dnssec-verify, Idns-verify-zone, validns, ...

+ Easy to understand and believe

– Zone Scope only

– Takes much time

- Even more time r/w textual zonefile

Bump-in-the-Wire Incremental Val.

- + Fast
- + No scripting at all
- + No Problem #1
- Zone Scope only
- AFAIK only implementation: Knot DNS

zone:

```
- domain: "example.com"  
  master: signer  
  dnssec-validation: on
```

Query Val. by Validating Resolver

- + Corresponds target audience
- Poor error description
 - SERVFAIL + EDE
- Might need “fake Root”
- Useless whole Trust Chain validation

Delv

- Similar to previous
- Bind9 recursive codebase
 - Brief output

DNSViz (or Verisign's tool)

- + Beautiful error description
- + Complete delegation breakdown
 - Slightly less beautiful

kdig +validate

- + Educative (non)error description
 - Incl. NSEC(3)
- + Comprehensible dig-like output
- Zone Scope only
- No care about Delegations
- Not yet released
- <https://kdig-validate.nic.cz/>

Proposed Delegation-validation tool

- + Focus on single Delegation
- + Query all parent & child NSs
- + Versatile options (zonefile instead NS...)
- + Uncluttered & complete output
- ? Do you know such
- ? Would you like such

DNSSEC Validation Overview

- All-in-one bump-in-the-wire: Knot DNS
- Easy iface to zonefile check utils: NSD
- Custom scripting:
 - NSD or Knot DNS or other iface
 - Full (slow) or incomplete validation
 - Prettiness of output matters

Thank you for attention