NLnet *Labs*

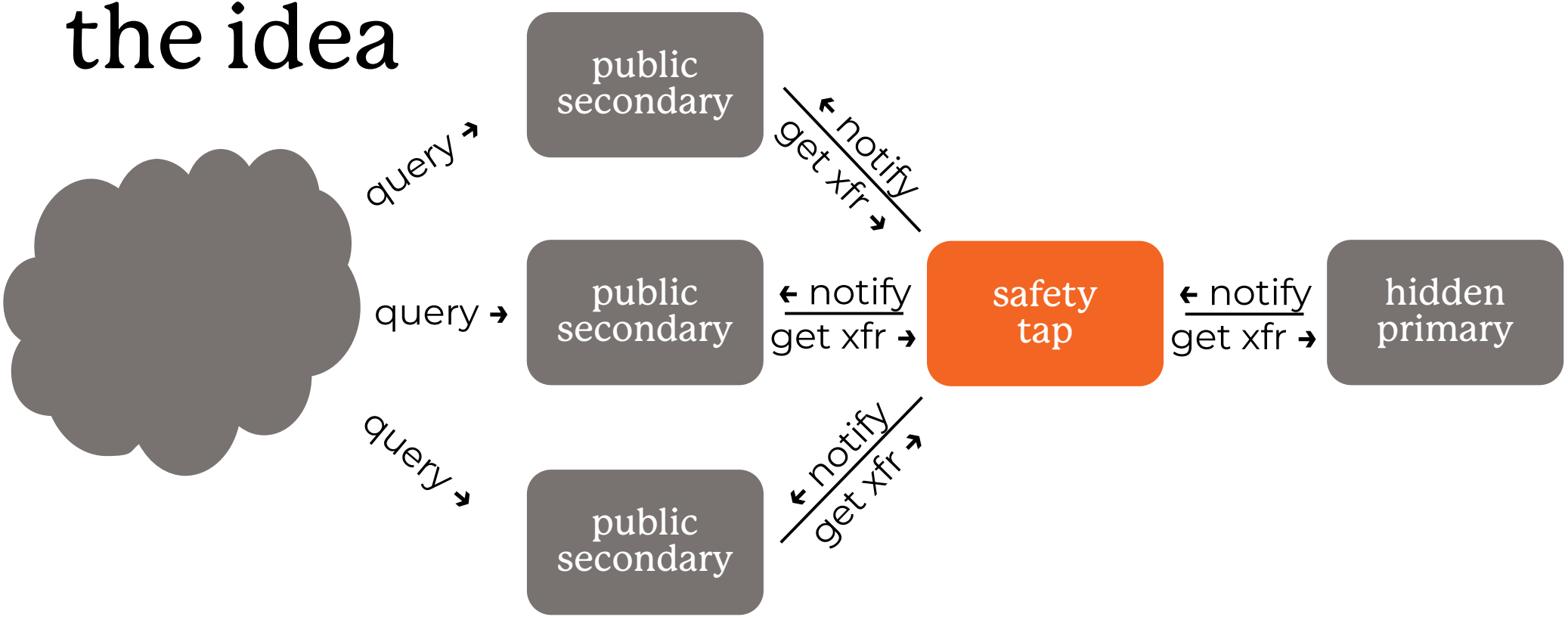
Bump in the wire zone verification

Willem Toorop @ the 53rd CENTR Tech

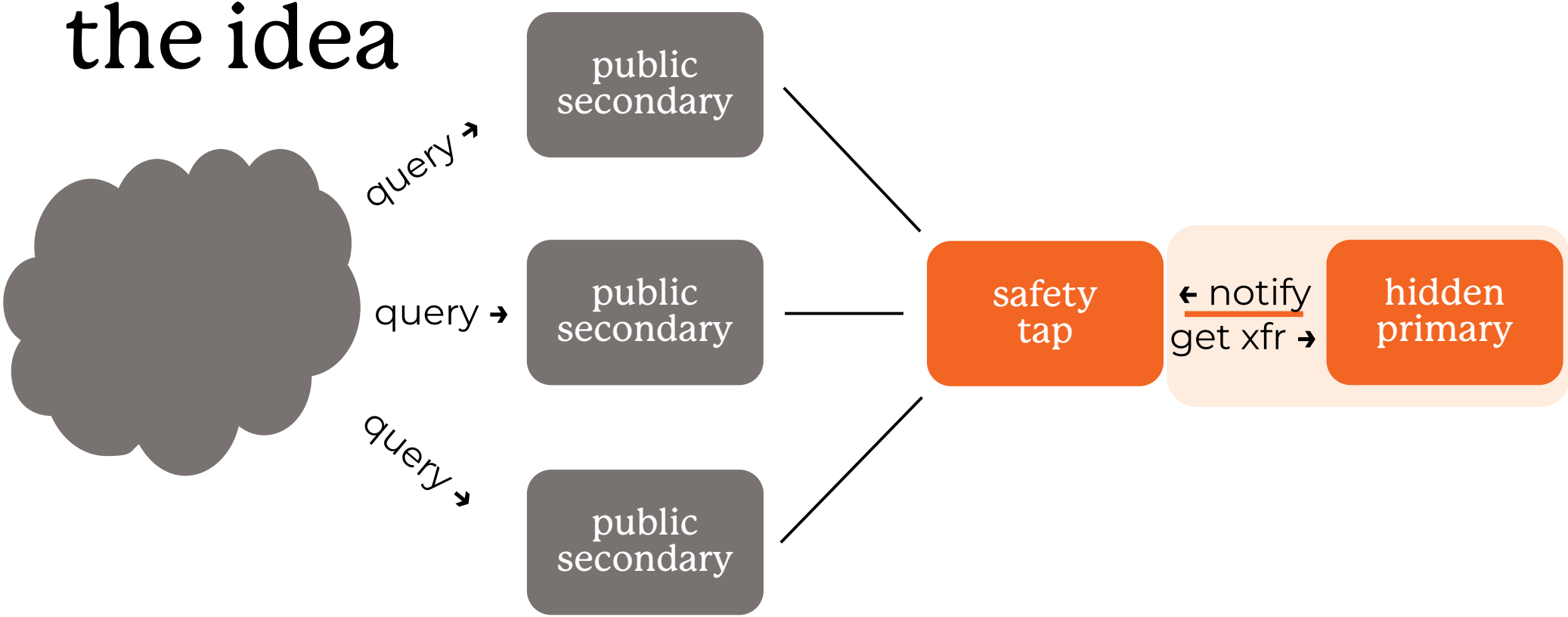
2011

- Just after the root was signed, multiple DNSSEC incidents
- Anand Buddhdev & Wolfgang Nagele came visit and suggested a safety tap
- NSD appeared very suitable for that

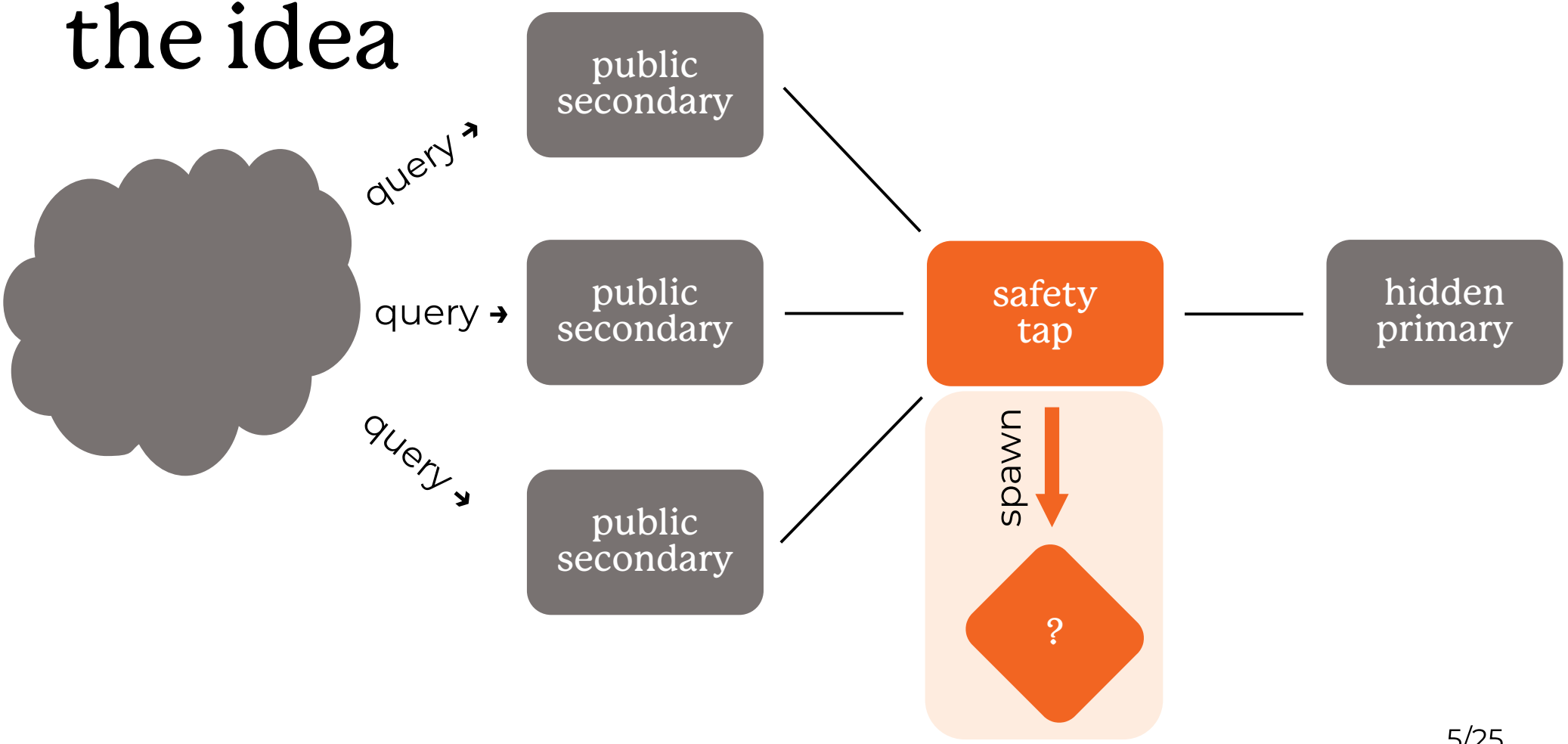
the idea


query
query
query
public secondary
public secondary
public secondary
notify
get xfr
notify
get xfr
notify
get xfr
safety tap
notify
get xfr
hidden primary

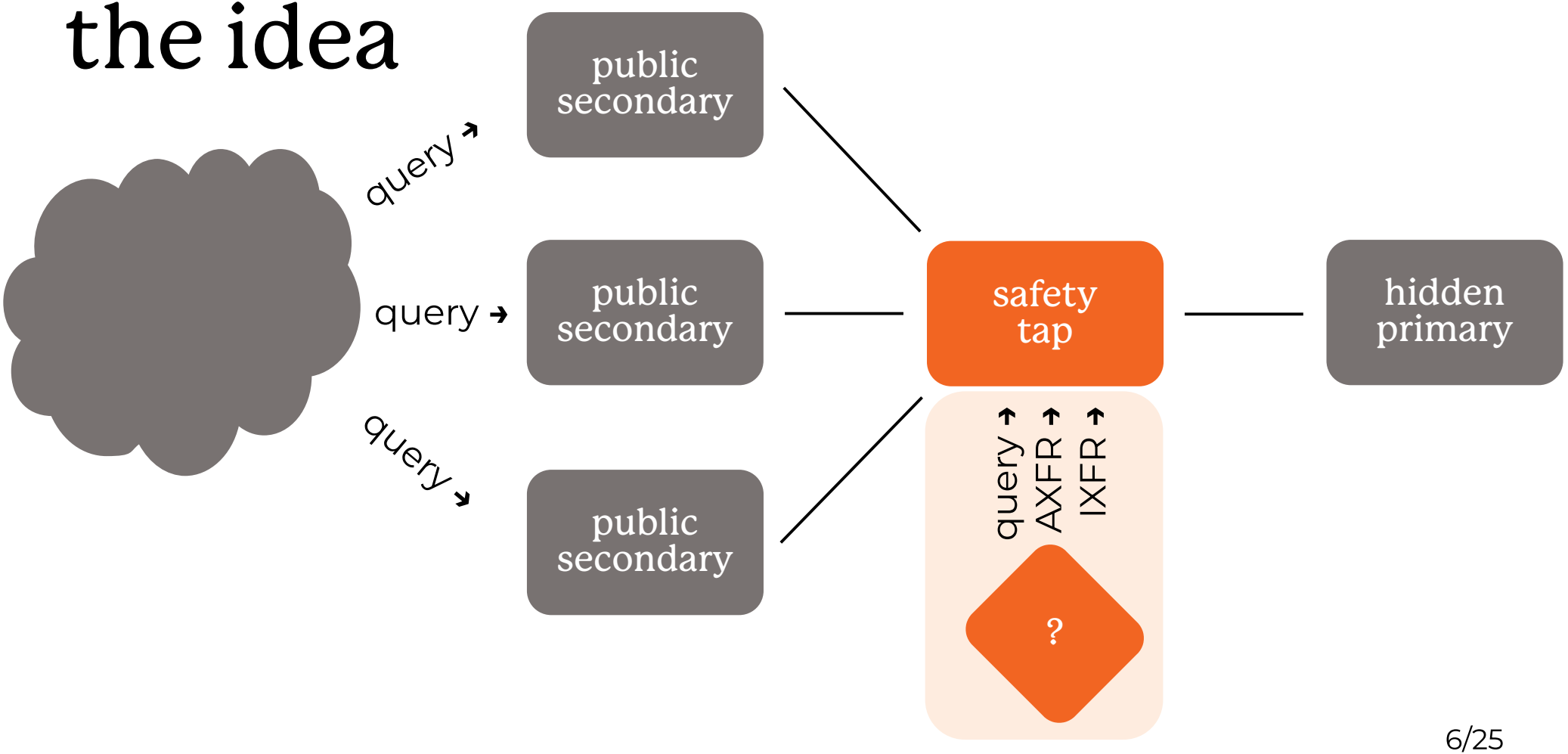
the idea


query
query
query
public secondary
public secondary
public secondary
safety tap
notify
get xfr
hidden primary

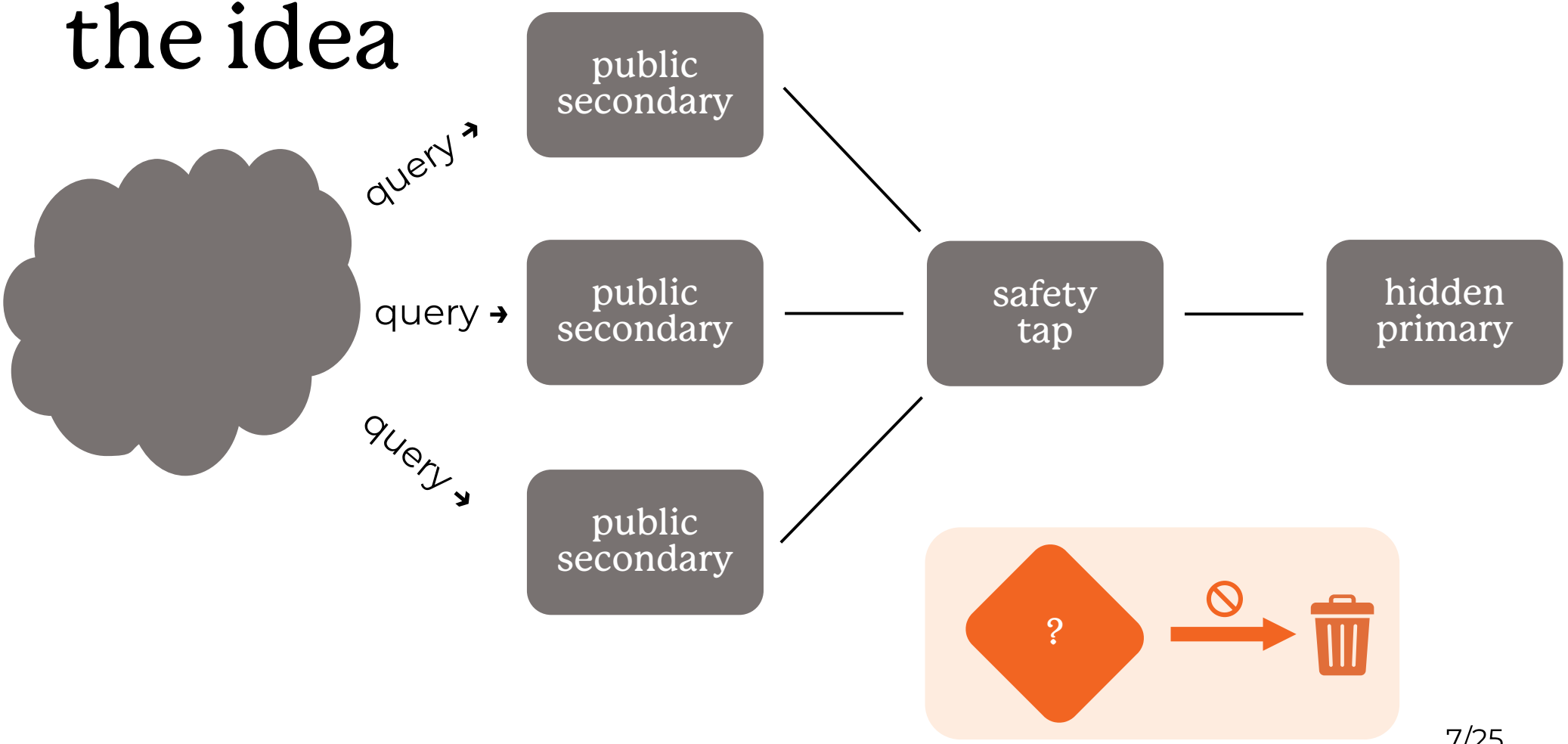
the idea


query
query
query
public secondary
public secondary
public secondary
safety tap
hidden primary
spawn
?

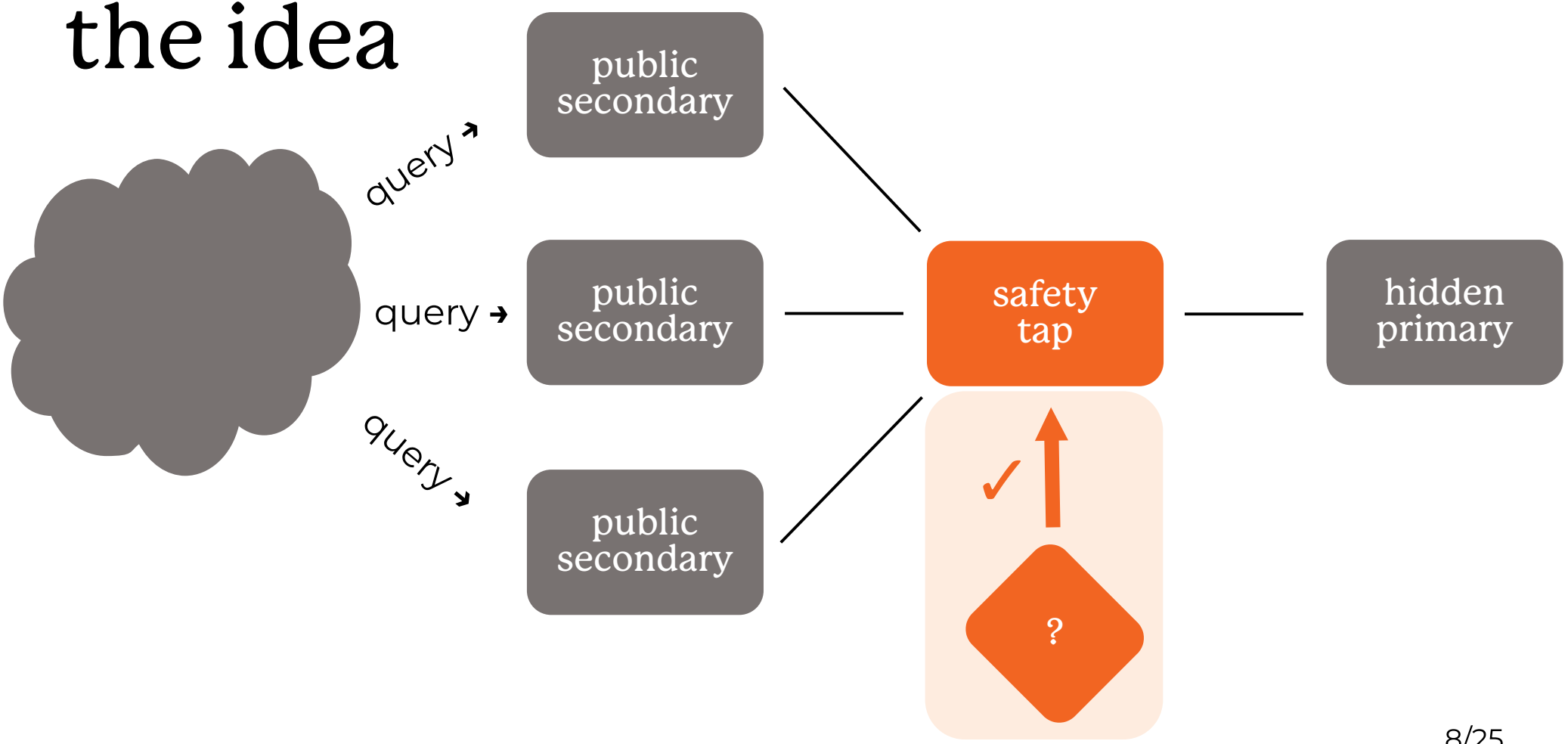
the idea


query
query
query
public secondary
public secondary
public secondary
safety tap
hidden primary
query
AXFR
IXFR
?

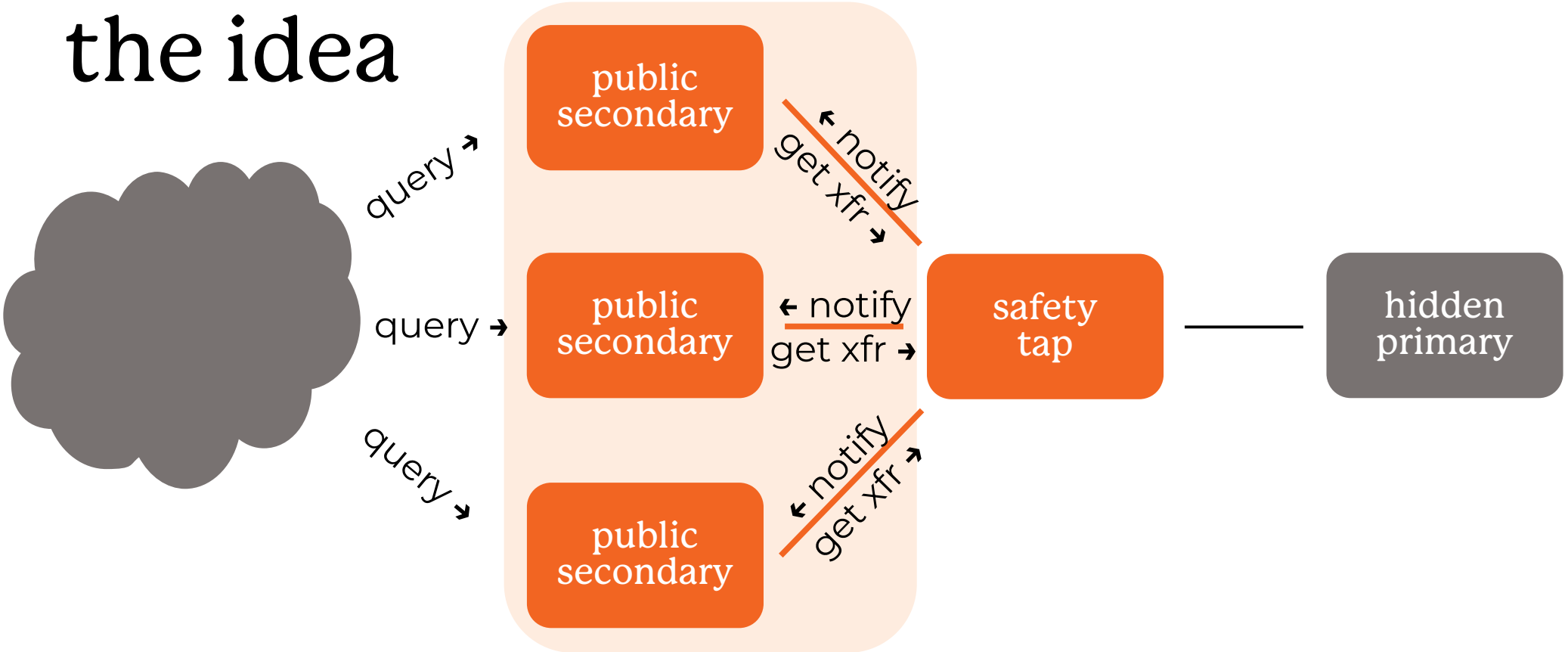
the idea


query
query
query
public secondary
public secondary
public secondary
safety tap
hidden primary
?

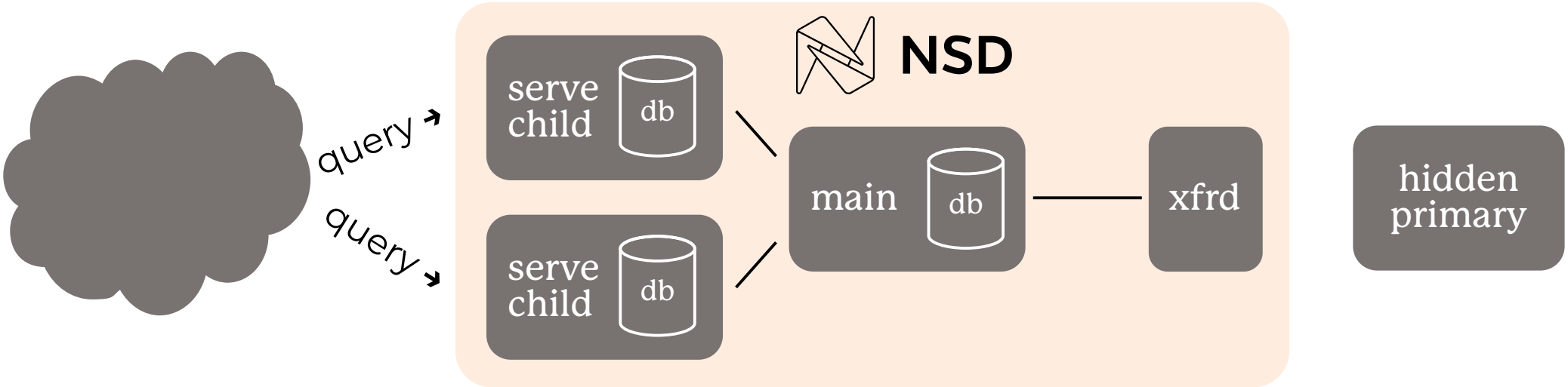
the idea


query
query
query
public secondary
public secondary
public secondary
safety tap
hidden primary
✓
?

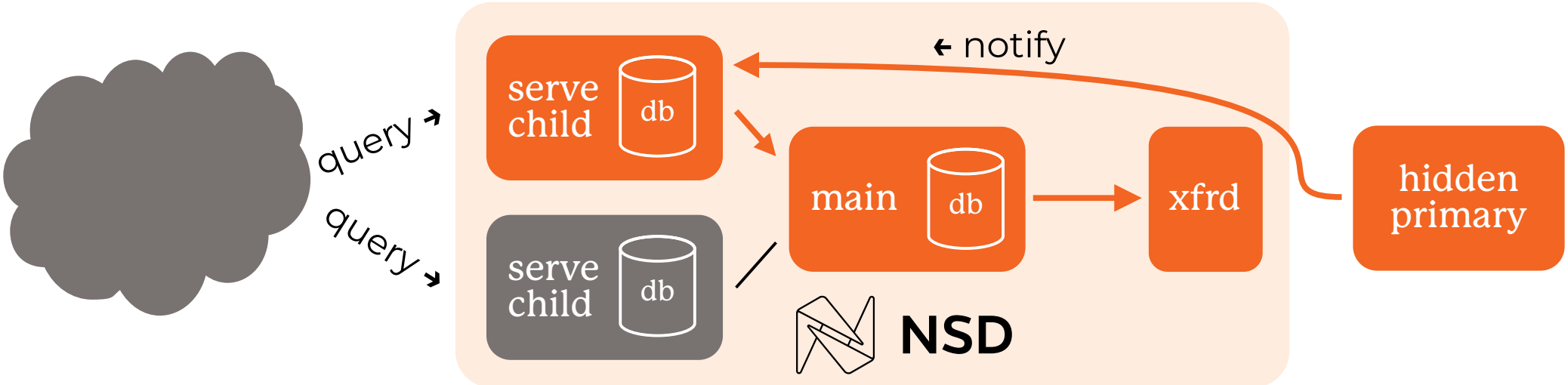
the idea


query
query
query
public secondary
public secondary
public secondary
notify
get xfr
notify
get xfr
notify
get xfr
safety tap
hidden primary

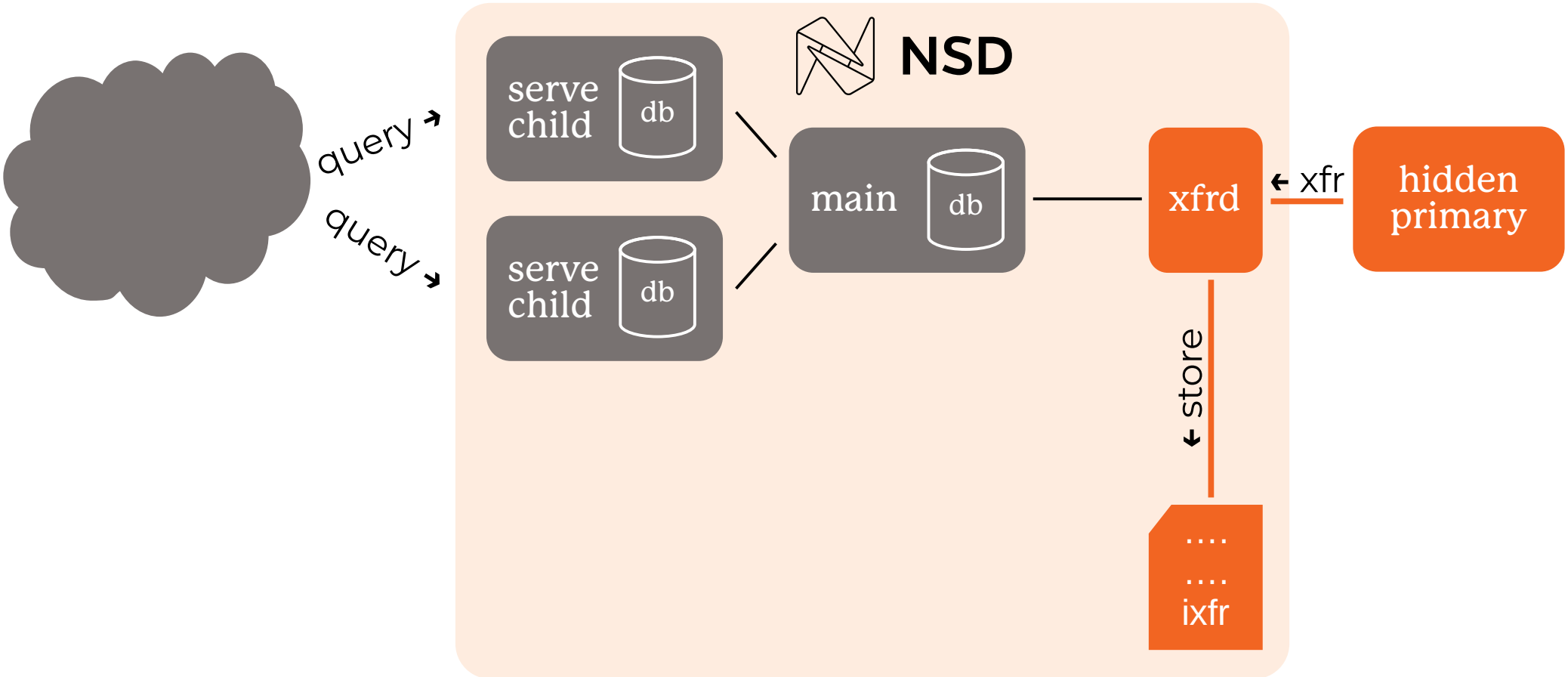
a good fit for NSD



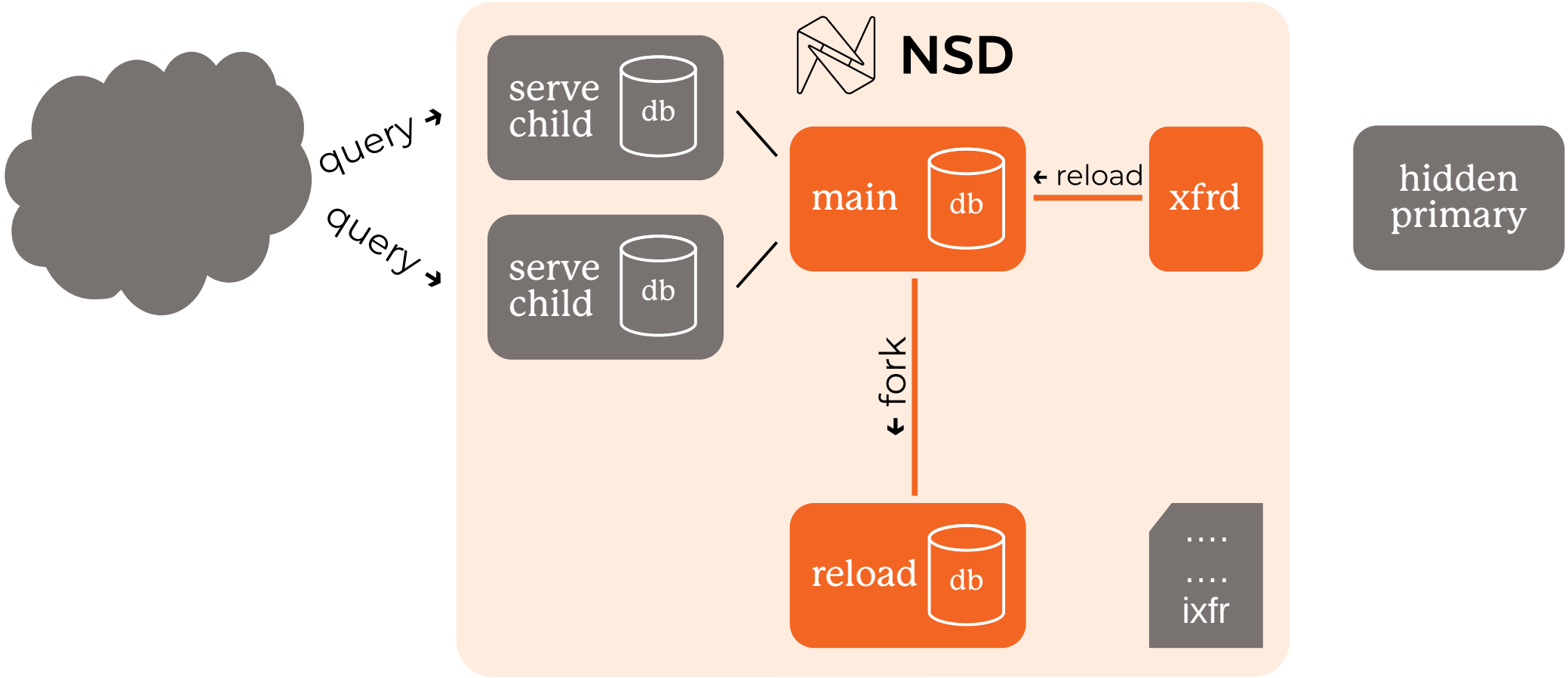
a good fit for NSD



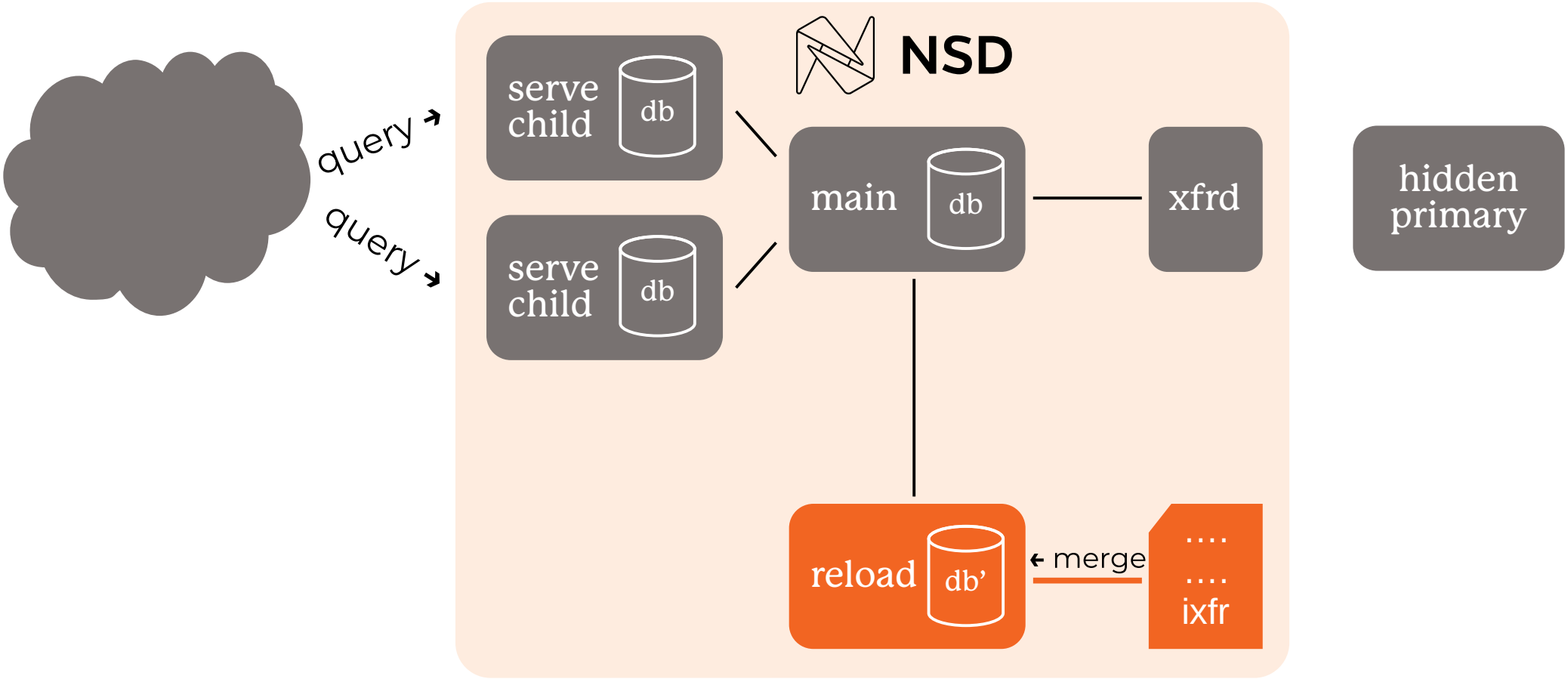
a good fit for NSD



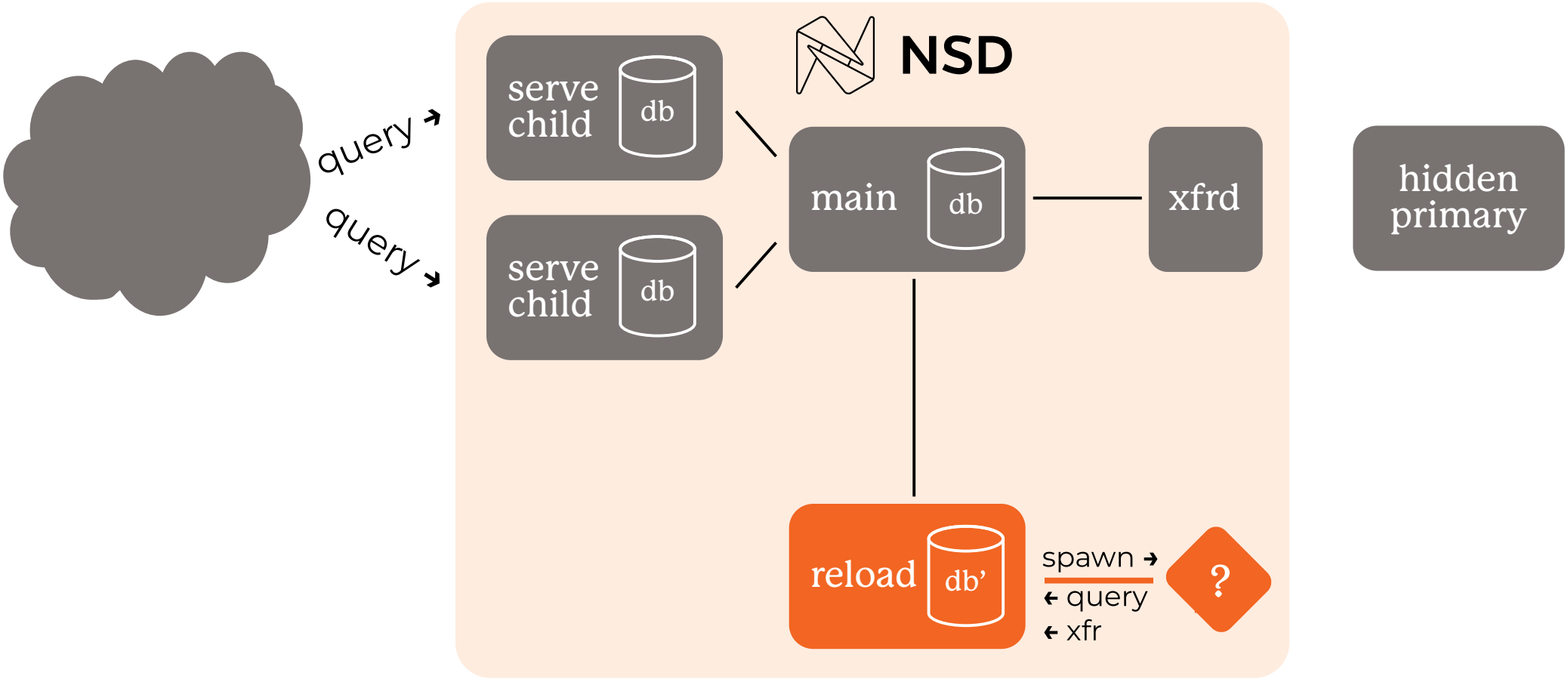
a good fit for NSD



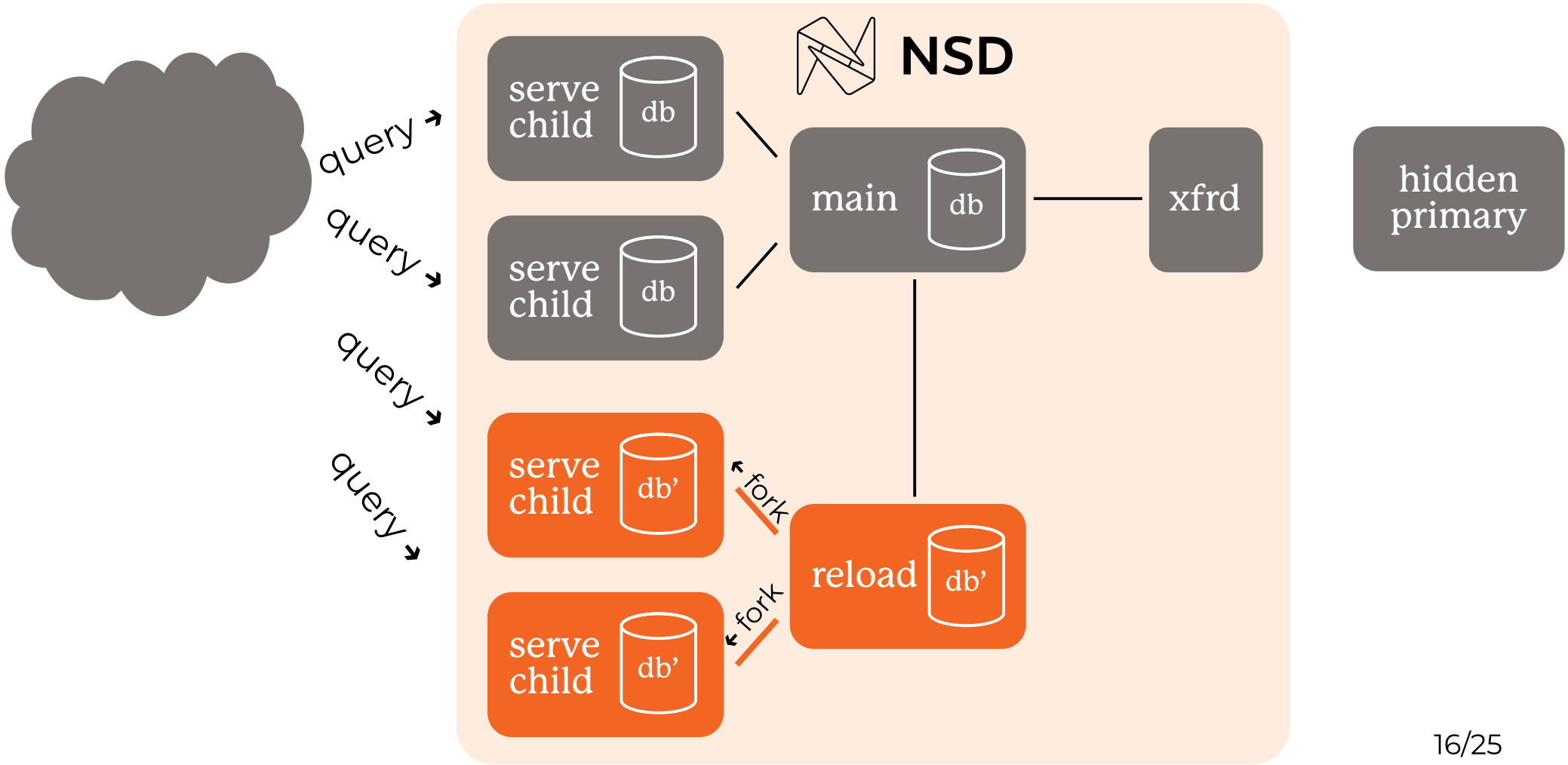
a good fit for NSD



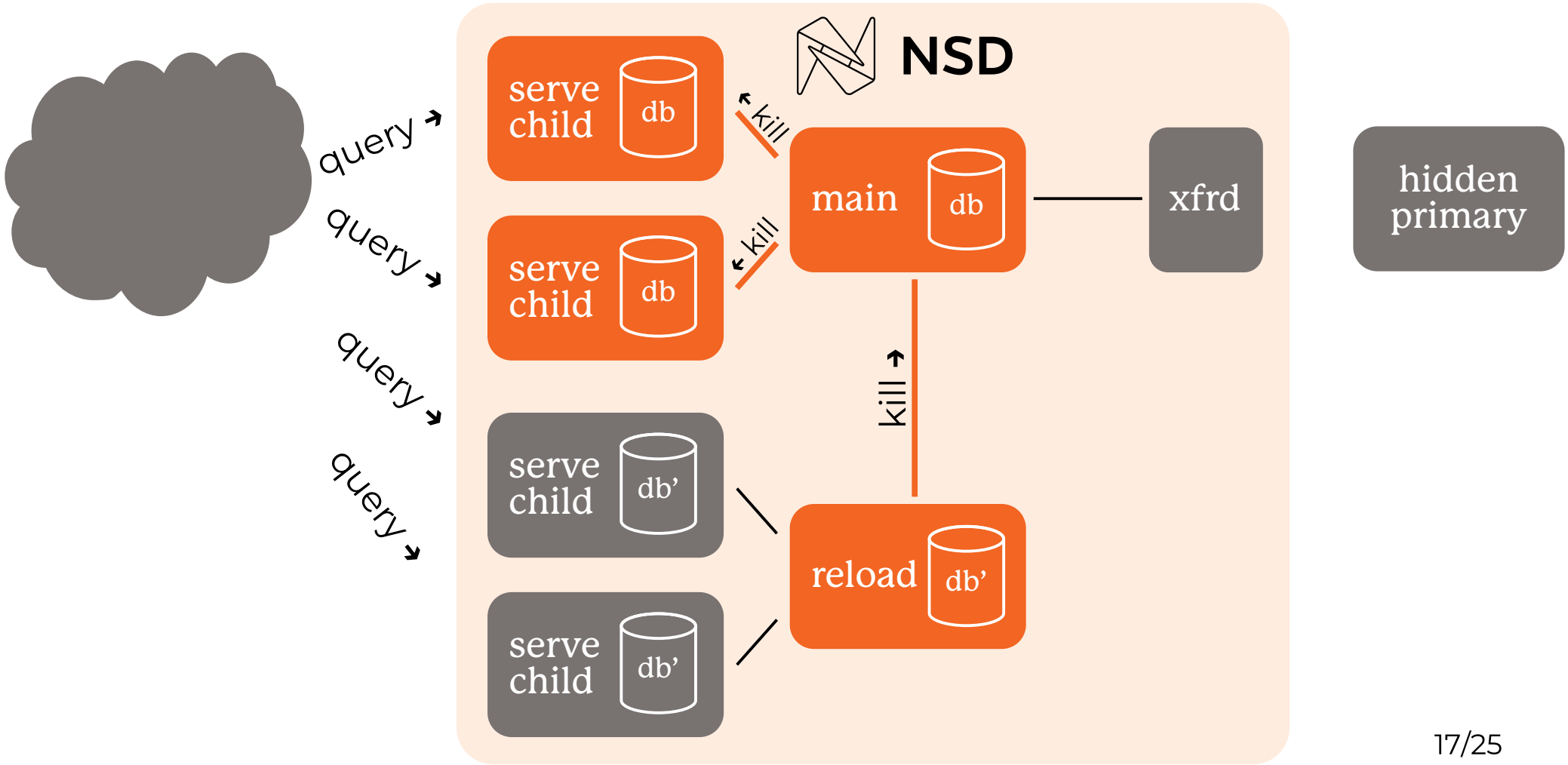
a good fit for NSD



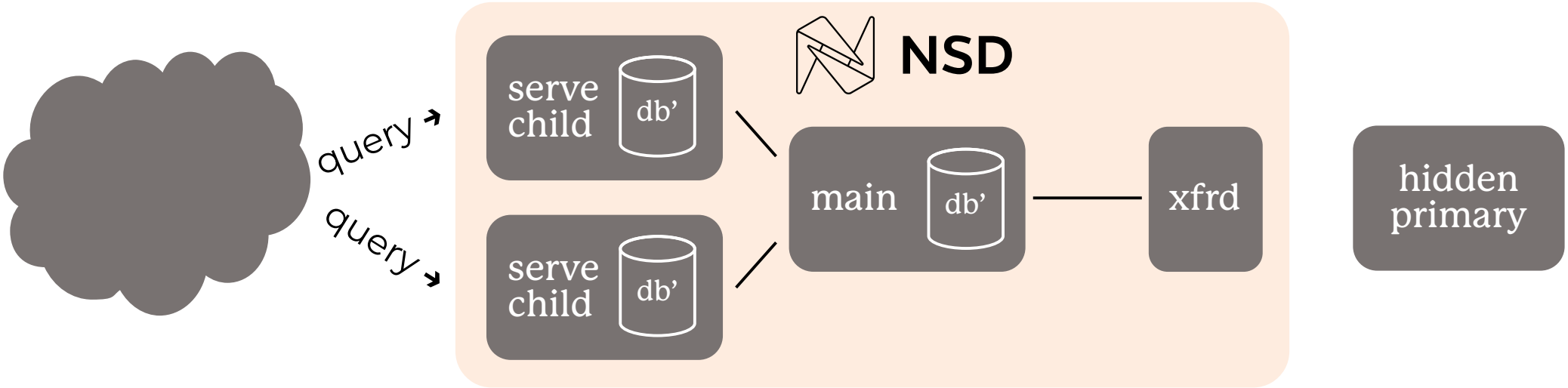
a good fit for NSD



a good fit for NSD



a good fit for NSD



feature in NSD

- Feature released as CreDNS (fork from NSD 3.2.10 - 2012)
- Merged into NSD since version 4.6.0 - 2022

```
verify:
        enable: yes
        verify-zones: <yes or no>
        verifier: <program with arguments>
        ip-address: <ip4 or ip6>[@port]
        verifier-count: <# concurrently running verifiers>
zone:
        verify-zone: yes
        verifier: <program with arguments or empty to inherit>
        verifier-timeout: <# seconds or inherit>
        verifier-feed-zone: <yes, no or inherit>
```

feature in NSD

- Environment variables available to the verifier script:

```
VERIFY_ZONE              name of the changed zone
VERIFY_IP_ADDRESSES      list of <address@port> values
VERIFY_IP_ADDRESS        first ip address in the list   VERIFY_PORT
VERIFY_IP4_ADDRESS       first ip4 address in the list  VERIFY_IP4_PORT
VERIFY_IP6_ADDRESS       first ip6 address in the list  VERIFY_IP6_PORT
VERIFY_ZONE_ON_STDIN     yes or not set

VERIFY_ZONE_SERIAL       serial number of the changed zone
VERIFY_ZONE_PREV_SERIAL  serial number to which the xfr was applied
```

feature in NSD

- Example simple verifier

```
verifier: ldns-verify-zone -kKexample.com.+013+370.key -Z
```

- Verify only changes by Unbound with a stub zone

```
stub-zone:
        name: example.com
        stub-addr: 127.0.0.1@5347
```

- Example verifier script to verifying only changes

```
dig @127.0.0.1 -p 5357 -t ixfr=${VERIFY_ZONE_PREV_SERIAL} example.com \
| <query each changed, added or deleted name and type against unbound>
```

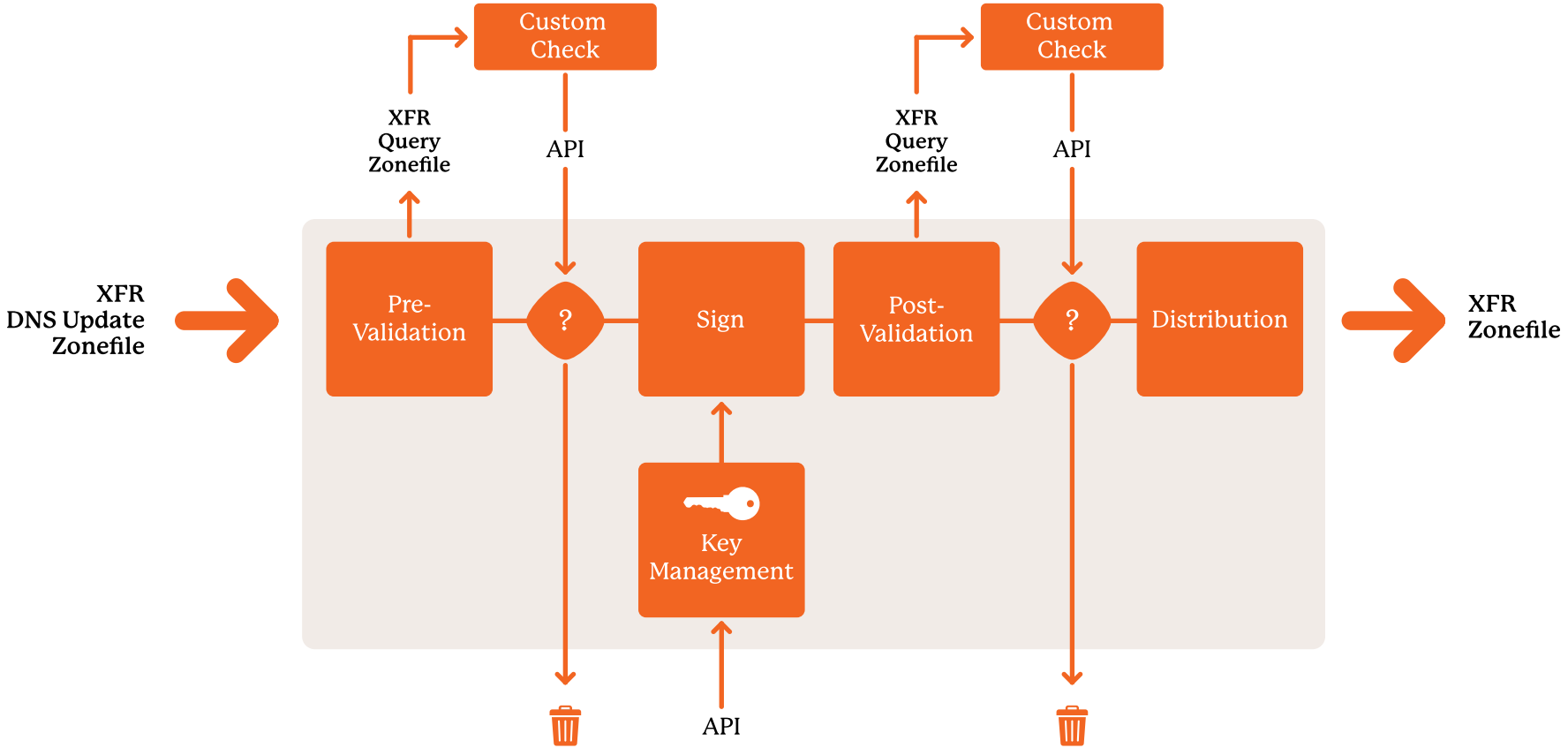
usage and community interest

- .SE’s requirements and design principles: draft-johani-tld-zone-pipeline
- .HU’s signing pipeline https://ripe89.ripe.net/archives/video/1466/

new implementations

- Knot-DNS since 3.5.0 (September 2025)
  - external-validation
  - DNSSEC Validation as part of Signing Pipeline
- Running verifier signaled on DBUS
- Knot-DNS already had built-in:
  - dnssec-validation (since 3.0 - 2020)
  - zonemd-verify (since 3.1 - 2021)

new implementations - Cascade



NLnet *Labs*

Bump in the wire zone verification

Willem Toorop @ the 53rd CENTR Tech