A Well-known URL for publishing service parameters
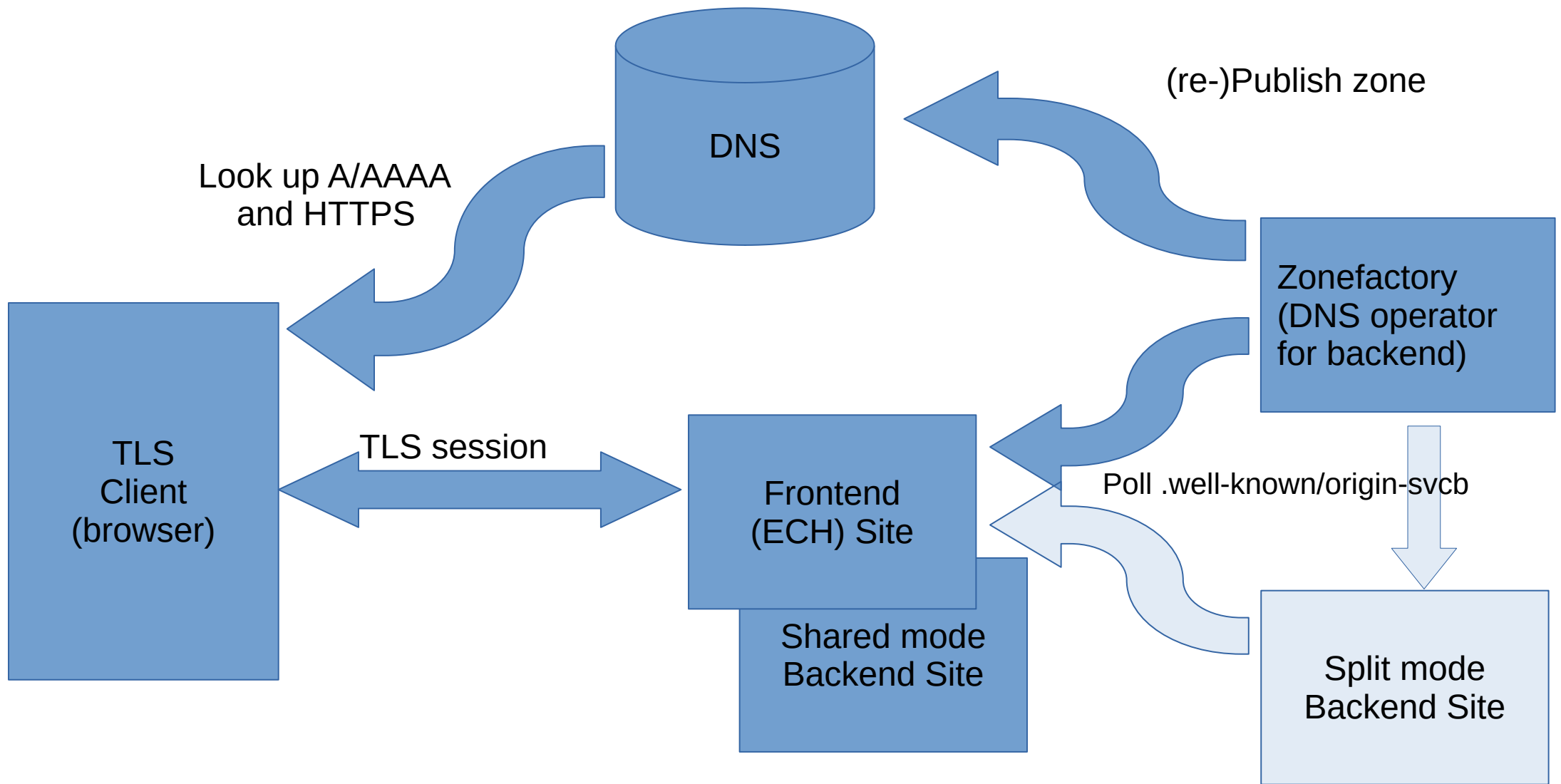
https://datatracker.ietf.org/doc/html/draft-ietf-tls-wkech

Stephen Farrell, Rich Salz, Ben Schwartz

IETF 123

Description

- ECH keys used at client-facing (web) servers (CFS) may be updated regularly (e.g. hourly) and are published to DNS in HTTPS RRs
- Other HTTPS RR content, e.g. ALPN values, might also be better managed at a CFS
- A "Zone Factory" (ZF) polls for this information via a .well-known URL, getting back a JSON structure
- If JSON changes from last time, then validate content and all being good, publish
- Git repo for spec: https://github.com/sftcd/wkesni

DNS

(re-)Publish zone

Look up A/AAAA
and HTTPS

Zonefactory
(DNS operator
for backend)

TLS
Client
(browser)

TLS session

Frontend
(ECH) Site

Poll .well-known/origin-svcb

Shared mode
Backend Site

Split mode
Backend Site

State of Play

- Draft -08 published 2025-07-07

- Note: draft previously bounced around dispatch/dnsop/tls before landing here

- Authors think it's ready for WGLC

- There's an implementation (bash scripts on CFS side, python on ZF side) with a small test deployment
  - https://github.com/defo-project/zone-factory/tree/mo-dep
  - Seems to work fine

Example

```
$ curl https://defo.ie/.well-known/origin-svcb
{
 "regeninterval" : 3600,
 "endpoints" : [ {
    "priority" : 1,
    "params" : {
       "ipv4hint" : ["213.108.108.101"],
       "ech" :
"AID+DQA8bwAgACAD99Nn5w3yRXF5GRcXzKNErYYtlxH5+IS5dQJzdHq3bgAEAAEAAQANY2
92ZXIuZGVmby5pZQAA/
g0APH8AIAAgkq9+fORtmI8hXAtKayssOOm+NSP+4j6HaIhS4R5G+EIABAABAAEADWNvdmVy
LmRlZm8uaWUAAA==",
       "ipv6hint" : ["2a00:c6c0:0:116:5::10"]
    }
 }]
}
```

Open Issues

- Be more precise with "pass the checks":
    - https://github.com/sftcd/wkesni/issues/53

- Better ZF definition
    - https://github.com/sftcd/wkesni/issues/52

Recently Closed Issues

- Default priorities
    - https://github.com/sftcd/wkesni/issues/46
- Delete DELETE
    - https://github.com/sftcd/wkesni/issues/45
- Some ZFs could use CAA
    - https://github.com/sftcd/wkesni/issues/44
- Don't publish private keys
    - https://github.com/sftcd/wkesni/issues/42
- Who's authoritative for which JSON bits
    - https://github.com/sftcd/wkesni/issues/41
- JSON encoding lists
    - https://github.com/sftcd/wkesni/issues/40

Conclusion

- Ready for WGLC?
  - Presumably with a related call to the dnsop list in parallel or sequentially