# 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 124

# State of Play

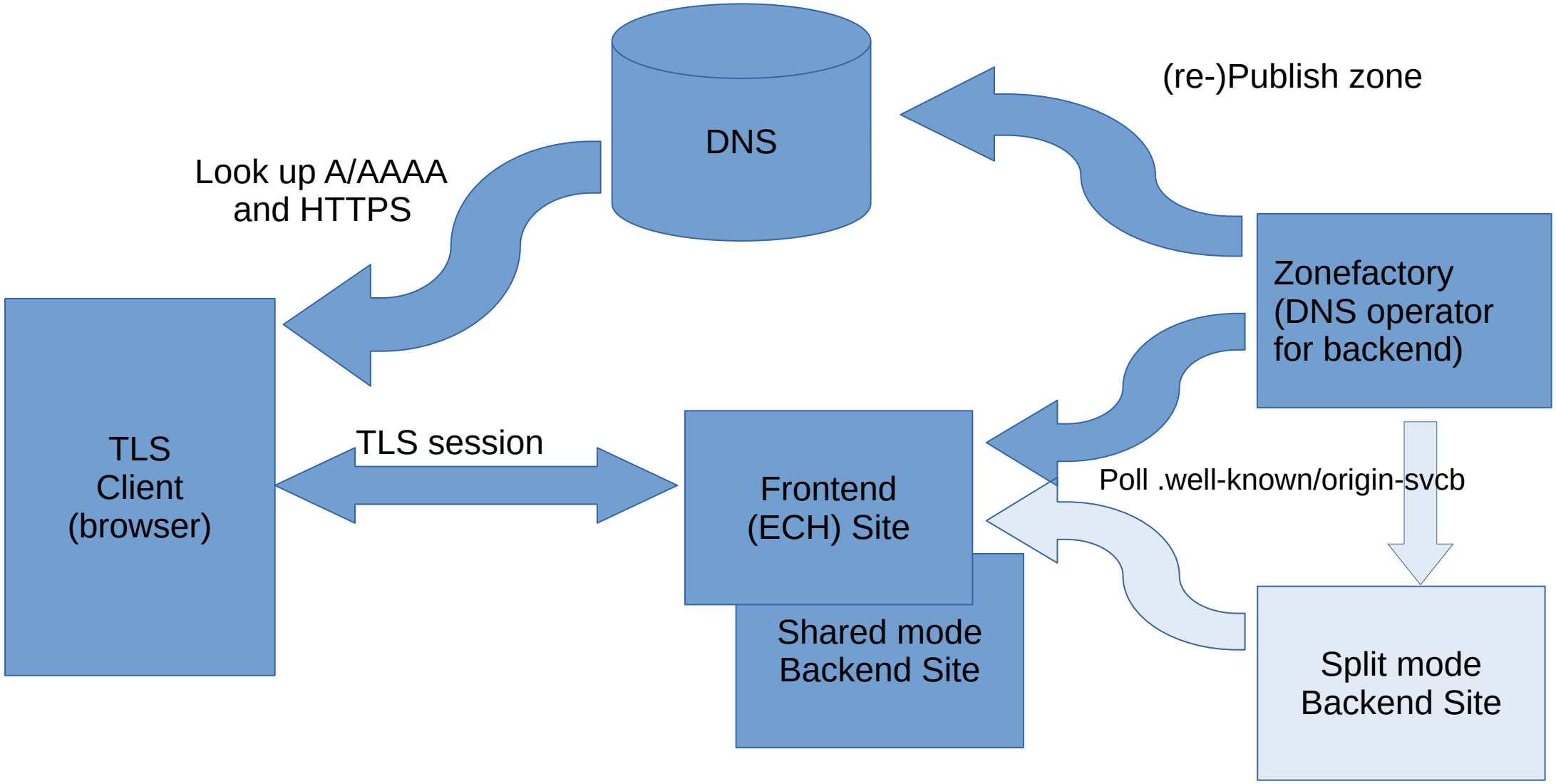
- Draft -10 published 2025-10-19 responding to comments from IETF-123, Watson and a couple of others
- Authors think it’s ready for WGLC (again:-)
  - Plan: do WGLC then hold ‘till we get a 2nd implementation
- No open issues at the moment
- Some backup slides follow but we can skip ‘em if not needed

# 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"]
    }
 }]
}
```

# 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