A well-known URL for publishing ECHConfigLists

https://datatracker.ietf.org/doc/draft-farrell-tls-wkesni/

Stephen Farrell is to blame (but is co-chairing openpgp now)
Joe Salowey is being kind enough to present for him
IETF113, Vienna, March 2022

Summary

- There are a bunch of ECH-enabled web servers at https://defo.ie/ (for interop testing)
- ECH keys are updated regularly (hourly, but that doesn't matter here...)
- That DNS setup doesn't use DDNS or provide an API the ECH-enabled frontend can use to write to DNS for the backend (others might have that)
- There is a "zonefactory" machine that knows the names of the backend servers and polls the frontend for new ECHConfigLists
  - When it finds new keys it tests those work and if so modifies zone file and re-publishes
- That benefits from a .well-known URL
  - Could work without a .well-known (configure full URLs at zonefactory) but configuring just the names seems more resilient

Example

https://cover.defo.ie/.well-known/ech/draft-13.esni.defo.ie.json

^^^ public_name

^^^ name in inner CH SNI

Response at 2022-03-14T13:50: a JSON array...

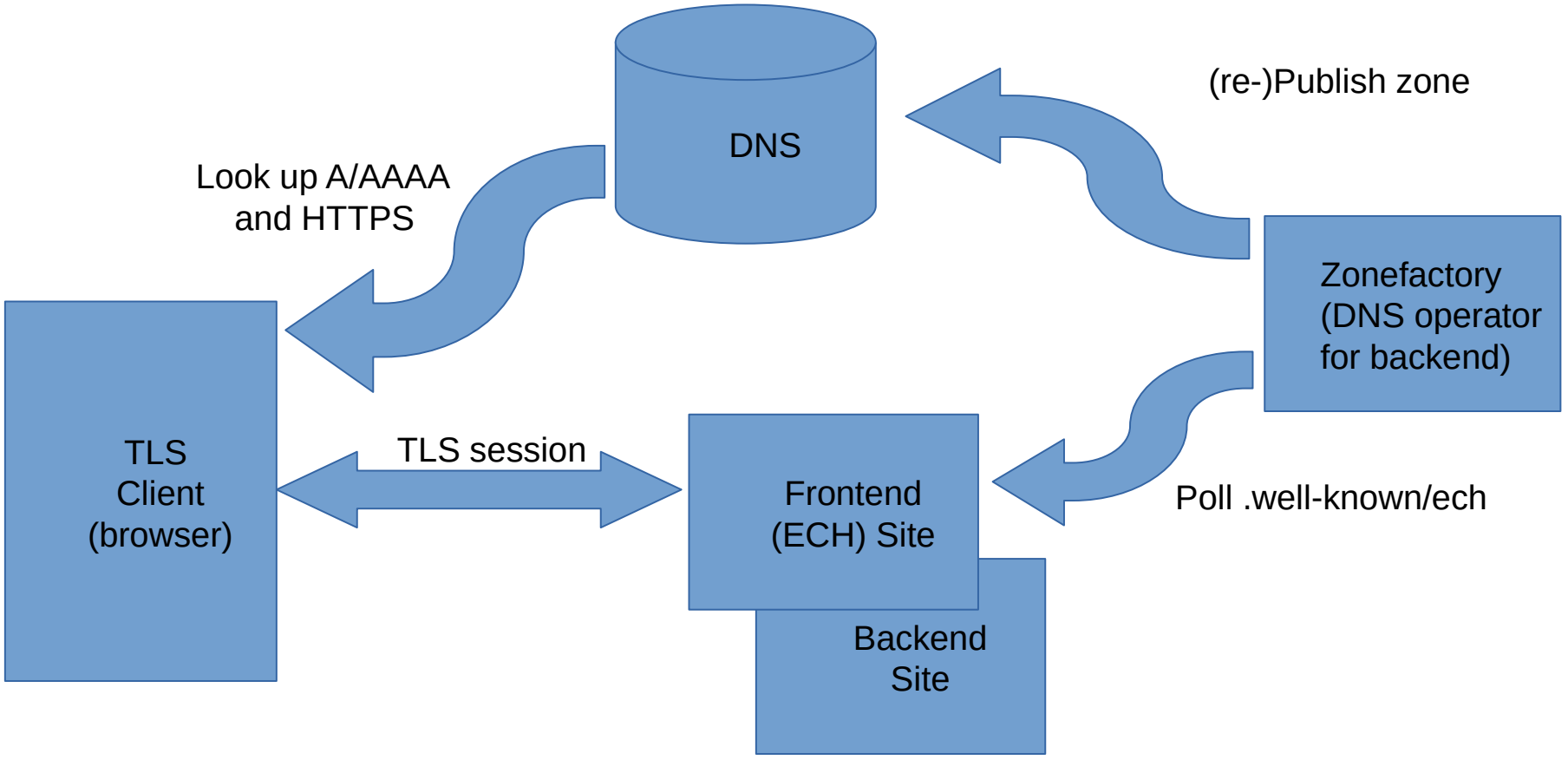

```
[
    {
        "desired-ttl": 1800,
        "ports":  [ 8413,8414,9413,10413,11413 ],
        "echconfiglist":
"AQD+DQA8AgAgACCuXw02/lUWxgMiwhhZzjkP11LxoTwi4TLxDH/gMtVBIQAEAAEAAQANY292ZXIuZGVmby5pZQAA/
g0APL8AIAAg9yNI2MhNZrf7XJGeOUowNMJCTeVZJ7i+jP+mxds5znMABAABAAEADWNvdmVyLmRlZm8uaWUAAP4NADzoACAAIKhvKLr
j0yWuzZiRJZyYnwoH6EEFXLVr8QI4iEG4wXJCAAQAAQABAA1jb3Zlci5kZWZvLmllAAD+DQA8YQAgACCKnTfgeEF8xz/
SDTHmlcZHThsym3vybQbBFlQ6oaypMQAEAAEAAQANY292ZXIuZGVmby5pZQAA"
    }
]
```

CDN Scenario

- The defo.ie web-sites are small and just for interop testing, so don’t provide the hiding-in-crowds aspect of ECH, but CDNs might also benefit from this (not that SF knows what CDNs want:-) in a scenario like this…

- cdn.example.net is doing ECH for client web-sites (e.g. example.com)
- Some client web-sites don’t use the CDN as their DNS operator
- cdn.example.net wants to regularly update ECHConfigLists for example.com (and ~all other client web-sites)
- example.com’s DNS operator can poll the relevant URL once it knows that example.com uses cdn.example.net for ECH

Picture


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/ech
Backend
Site

ECH or more generic?

- A question (to which SF doesn’t know the answer) is whether an ECH-specific URL as proposed here would be more or less useful than something more generic?
- Current guess: the ECH frontend/backend thing is specific and simple enough that an ECH-specific mechanism is maybe correct
  - Trying to tackle the full generality of SVCB/HTTPS RRs this way seems… wrong

It’s a working work-in-progress

- Could be a bad_idea
- If (!bad_idea)
  - Change stuff as other implementers want
  - ALPN has been suggested as being useful
  - The JSON response details will certainly need work when someone else looks at ‘em, and/or as some other zonefactory DNS tooling is used
  - Do the proper administrivia (.well-known registration, i18n…)
- Hopefully not much work, as it kinda just works
  - As of now, only for defo.ie but changing from ESNI to ECH wasn’t hard at all and an implementation can be done with pretty simple scripting

Thanks again to Joe!

Dispatch?

- Dispatch possibilities:
  - Could be added as an appendix to ECH draft (probably not)
  - Could be progressed in a new WG (almost certainly not)
  - Could be proposed for adoption in one of tls, dnsop, httpbis
  - Could be sent to ISE as “here’s a thing someone did”
- SF’s preference: propose for adoption as tls WG draft (and keep dnsop/httpbis in the loop)