A Well-known URL for publishing ECH config data

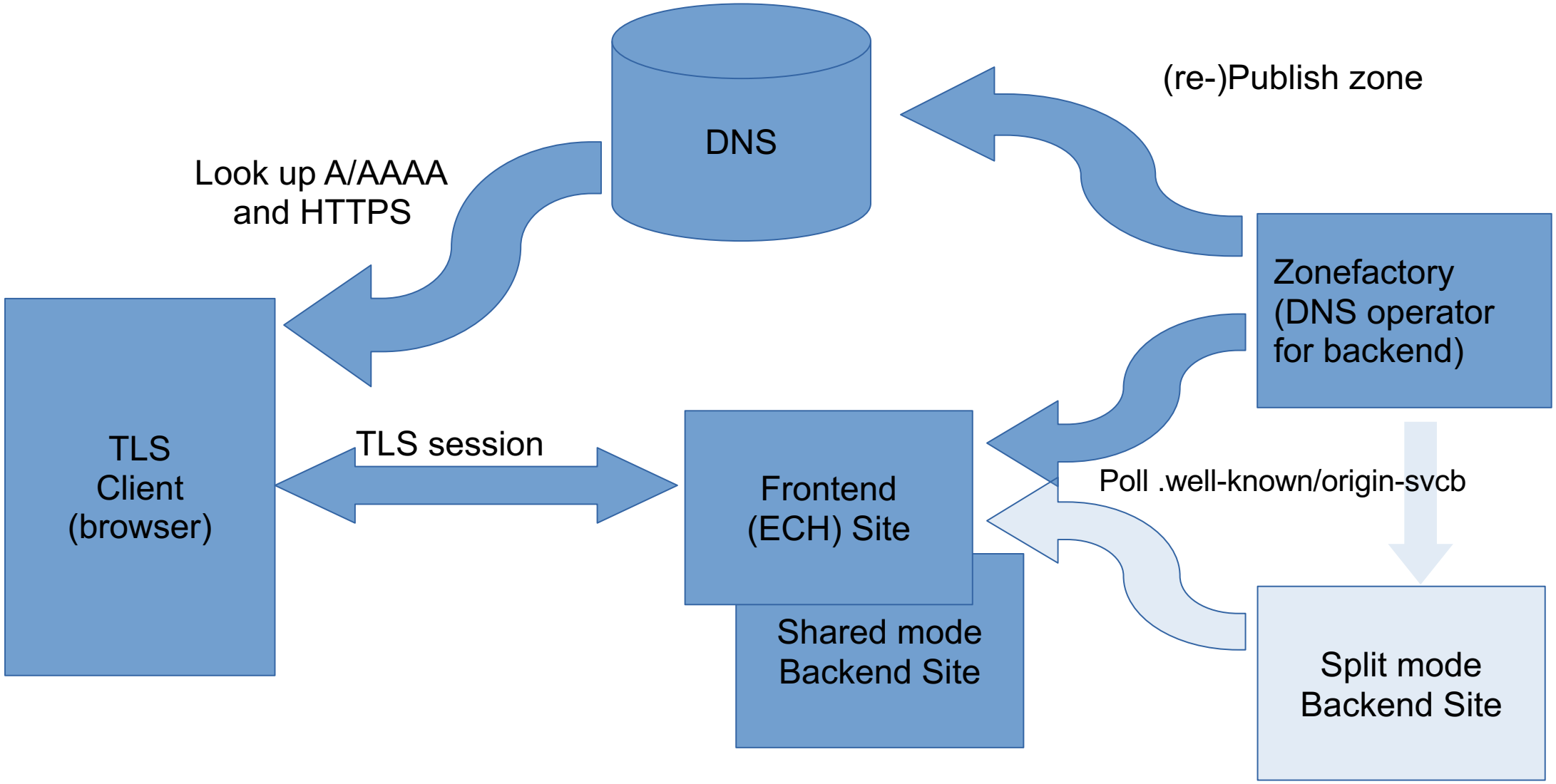
Stephen Farrell, **Rich Salz**, Ben Schwartz

IETF 120

Description

- ECH keys are **updated regularly** and must be published to DNS

- A “Zone Factory” polls origins via WK resource
  - If they changed, it test them (keys) for validity
  - Publishes updates to DNS


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

Changes

- Many editorial
  - xml2rfc v3
- Greater compliance with HTTPS SVCB
- IANA considerations
  - Register well-known “origin-svcb” entry
  - Add JSON Service Binding registry for top-level elements
- Security considerations
- Resolved many issues

Examples

```
{
        "regeninterval": 3600,
        "endpoints": [
            {
                "priority": 1,
                "target": "cdn.example.",
                "params": { "ech": "AD7+DQA65wAgAC..AA==" }
            } ...
        ]
}
```

```
{
        "regeninterval": 108000,
        "endpoints": [
                { "alias": "cdn1.example.com” }
        ]
}
```

https://github.com/sftcd/wkesni/issues

- #18 – Any I18N issues? (Placeholder)
- #21 – Architecture for intermediaries
  - “Things” in front of the origin; e.g., load-balancers with different protocols; HTTP gateways
- #16 – One origin can “claim” to speak for others; under-specified? (MT’s early review)
- #14 – Is this still ECH-specific?
  - Thread on TLS mailing list

Next Steps

- Please review, send feedback
- Particularly around issue #14
- Maybe WGLC after IETF 121?