# A well-known URI for publishing ESNIKeys

draft-farrell-tls-wkesni-01

Stephen Farrell

IETF106, Singapore, November 2019

# Summary

- I have some ESNI-enabled web servers
- I update the ESNI keys regularly (hourly, but that doesn’t matter here...)
- My DNS setup doesn’t use DDNS or have an API the web server can use to write to DNS (many others might have that)
- I have a “zonefactory” machine that polls the web server for new ESNIKeys
  - When it finds a new key it tests that works and if so modifies zone file
- That benefits from a .well-known URI

# Example

https://cover.defo.ie/.well-known/esni/only.esni.defo.ie.json

^^^ public_name

^^^ name in ESNI

Result is JSON array like:

```
[{
   "ESNIKeys.version": 0xff02, "desired-ttl": 1800,
   "ESNIKeys":
"FF0282EFB718000D636F7665722E6465666F2E69650024001D0020FD073635CFB5A25C8EB
63601C2F885BD27FD0AD9B8947F4EECD02D5D32D38F2C000213010104000000005DD34EF80
00000005DD36410001A1001001604B918E967062A042E000001001500000000000000A"
}]
```

# Adopt that?

- Could be added as an appendix to ESNI draft
- Could be progressed separately in WG
- Could be sent to ISE as “here’s a thing someone does”
- Could be a dumb idea
- If (!dumb)
  - Need to tweak stuff to match ESNI draft as that develops, and whatever other implementers (if any) want
- Any of those are fine by me
- My suggestion: adopt as TLS WG draft in case there’re other uses for such a .well-known URI that emerge later

# ESNIKeys PEM Format

draft-farrell-tls-pemesni-00

Stephen Farrell

IETF106, Singapore, November 2019

# Example

```
-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VuBCIEIEDyEDpfvLoFYQi4rNjAxAz7F/Dqydv5IFmcPpIyGNd8
-----END PRIVATE KEY-----
-----BEGIN ESNIKEY-----
/wG+49mkACQAHQAgB8SUB952QOphcyUR1sAvnRhY9NSSETVDuon9/
CvoDVYAAhMBAQQAAAAAXYZC
TwAAAABdlBoPAAA=
-----END ESNIKEY-----
```

# Overview/Conclusion

- Need a file format for TLS server configuration
- One key pair per file (not a great match to ESNIKeys)
- Bit of PEM formatting (PKCS#8 PrivateKey works, invented new tag for b64 ESNIKeys); private key 1st for no good reason
- My suggestion: add as appendix to ESNI draft
- Or, could be a separate draft etc. same as wkesni
- Happy to modify to match what others do if needed