SSLKEYLOGFILE Extension for ECH

`draft-ietf-tls-ech-keylogfile-01`

Yaroslav Rosomakho*

Hannes Tschofenig

Recap

- ECH_SECRET label to log HPKE shared_secret
- ECH_CONFIG label to log ECHConfig
- Outer ClientHello Random as keys for ECH_SECRET and ECH_CONFIG
- Inner ClientHello Random for the rest of the session as long as ECH was accepted

Changes since -00

- “To minimize the risk of accidental activation in production, implementers SHOULD incorporate appropriate compile-time controls”
- New SSLKEYLOGFILE Labels IANA registry request
  - Original SSLKEYLOGFILE entries
  - ECH SSLKEYLOGFILE entries
  - Extended Key Update SSLKEYLOGFILE entries

Thank you!

- Is this ready for WGLC?