# ECH Interoperability Report

Stephen Farrell stephen.farrell@cs.tcd.ie

Stephen Farrell

Trinity College Dublin/Tolerant Networks Ltd.

stephen.farrell@cs.tcd.ie

work-in-progress 2024/11/28:16:31

**Abstract**

The abstract.

**Index Terms**

Encrypted Client Hello (ECH), Interoperability

## I. Introduction

Deployments of the Transport Layer Security (TLS [1]) protocol expose the name of the server (e.g. the web site DNS name) via the Server Name Indication (SNI) field in the first message sent (the ClientHello). The Encrypted Client Hello (ECH) [2] extension to TLS is a privacy-enhancing scheme that aims to address this leak.

This report describes the current state of ECH interoperability.

## II. Software

This section describes libraries, clients and servers that support ECH.

### A. Libraries

OpenSSL, boringssl, NSS, WolfSSL, gnutls, golang, rustls, python

### B. Clients

*1) Browsers:* firefox, chromium, brave, vivaldi

*2) Command Line Tools:* curl

### C. Servers

ours: nginx, apache, lighttpd, haproxy

## III. Services

Describe services

## IV. Interoperability

Describe interop

## V. Conclusions

Conclude

## Acknowledgements

Thanks to DEfO folks, OTF...

## References

[1] E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.3,” RFC 8446, Aug. 2018. [Online]. Available: https://www.rfc-editor.org/info/rfc8446

[2] E. Rescorla, K. Oku, N. Sullivan, and C. A. Wood, “TLS Encrypted Client Hello,” Internet Engineering Task Force, Internet-Draft draft-ietf-tls-esni-22, Sep. 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-esni/22/