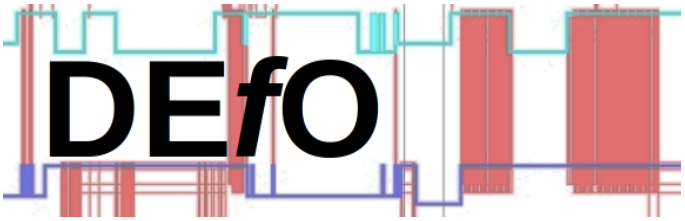

QUIC and ECH

Ana

Wednesday 24th September, 2025

(early) work-in-progress: build time 15:19 UTC

Abstract

Encrypted Client Hello (ECH) is a privacy-enhancement for the Transport Layer Security (TLS) protocol that underlies all web security and the security of many other Internet protocols. While the specification for ECH is relatively mature, (though not yet an Internet-RFC), and while implementations are already widespread, work remains to ensure that a random client and server can successfully use ECH. QUIC is... To that end, this report describes issues with ECH-enabling QUIC as an input to future work on that topic.

Contents

Keywords: Encrypted Client Hello (ECH), QUIC

1 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. The primary audience for this document are those implementing and deploying ECH. Secondarily, there may be lessons to learn for those designing protocols like ECH.

The Open Technology Fund (OTF, `https://www.opentech.fund/`) have funded the DEfO project (`https://defo.ie`) to develop ECH implementations for OpenSSL, and to otherwise encourage implementation and deployment of ECH. As we expect the implementation and deployment environment for ECH to change over time, this report will be updated as events warrant and is currently versioned based on the build-time of this PDF.

2 QUIC and ECH

TBD

3 Existing Implementations

TBD

4 Issues Arising

TBD

5 Conclusions

TBD

Acknowledgements

Thanks to the Open Technology Fund for ongoing funding of the DEfO project. (And for their patience while the IETF process for ECH takes... ages;-) Thanks in particular to the people working on DEfO who contributed to this work including: Kerry Hartnett, John Hess, Iain Learmonth,

Niall O'Reilly, Jochen Sprickerhof and Hans-Christoph Steiner. Thanks also to the developers of other ECH implementations (including NSS, boringssl, wolfssl, golang and rustls) for co-operating as we worked on interoperability, and to the maintainers of OpenSSL, curl, lighttpd and haproxy for ECH related discussions and PR-processing along the way.

All errors and omissions of course remain the fault of the author.

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/

Appendices

Appendix A Document Versions

As stated, we plan to update this report from time to time and versioning is based on the build time. This appendix notes the major changes between "published" versions.

- 2025-09-24: Initial version.