Internet Engineering Task Force (IETF)
Internet-Draft
Intended status: Standards Track
Expires: 27 July 2026

S. Farrell
Trinity College Dublin

23 January 2026

PEM file format for ECH
draft-farrell-tls-pemesni-13

Abstract

Encrypted ClientHello (ECH) key pairs need to be configured into TLS servers, which can be built using different TLS libraries. This document specifies a file format to use, similar to how RFC 7468 defines other PEM file formats.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 27 July 2026.

Table of Contents

1. Introduction

Encrypted ClientHello (ECH) [I-D.ietf-tls-esni] for TLS1.3 [RFC8446] defines a confidentiality mechanism for server names and other ClientHello content in TLS. That requires publication of an ECHConfigList data structure in an HTTPS or SVCB RR [RFC9460] in the DNS. An ECHConfigList can contain one or more ECHConfig values. An ECHConfig structure contains the public component of a key pair that will typically be periodically (re-)generated by some key manager for a TLS server. TLS servers then need to be configured to use these key pairs, and given that various TLS servers can be built with different TLS libraries, there is a benefit in having a standard format for ECH key pairs and configs, just as was done with [RFC7468].

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. ECHConfig file

A PEM ECH file contains zero or one private key and one encoded ECHConfigList.

The public and private keys MUST both be PEM encoded [RFC7468]. The file contains the concatenation of the PEM encoding of the private key (if present) followed by the PEM encoding of the public key(s) as an ECHConfigList. When a private key is present, the ECHConfigList MUST contain an ECHConfig that matches the private key. The private key MUST be encoded as a PKCS#8 PrivateKey [RFC7468]. The public

key(s) MUST be the base64 encoded (see Section 4 of [RFC4648]) form of an ECHConfigList value that can be published in the DNS using an HTTPS RR as described in [I-D.ietf-tls-svcb-ech]. The string "ECHCONFIG" MUST be used in the PEM file delimiter for the public key.

Any content after the PEM encoded ECHConfigList SHOULD be ignored.

Figure 1 shows an example ECHConfig PEM File

```
-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VuBCIEICjd4yGRdsoP9gU7YT7My8DHx1Tjme8GYDXrOMCi8v1V
-----END PRIVATE KEY-----
-----BEGIN ECHCONFIG-----
AD7+DQA65wAgACA8wVN2BtscOl3vQheUzHeIkVmKIiydUhDCliA4iyQRCwAEAAEA
AQALZXhhbXBsZS5jb20AAA==
-----END ECHCONFIG-----
```

Figure 1: Example ECHConfig PEM file

If the above ECHConfigList were published in the DNS for foo.example.com, then one could access that as shown in Figure 2.

```
$ dig +short HTTPS foo.example.com
1 . ech=AD7+DQA65wAgACA8wVN2BtscOl3vQheUzHeIkVmKIiydUhDCliA4iyQR
wAEAAEAAQALZXhhbXBsZS5jb20AAA==
```

Figure 2: Use of dig to get the ECHConfigList from DNS

TLS servers using this file format might configure multiple file names as part of their overall configuration, if, for example, only the ECHConfigList values from a subset of those files are to be used as the value for retry_configs in the ECH fallback scenario.

The ECHConfigList in a PEM file might contain more than one ECHConfig if, for example, those ECHConfig values contain different extensions or different public_name values. Consistent with [I-D.ietf-tls-esni], the ECHConfig values within an ECHConfigList appear in decreasing order of preference. If the ECHConfigList value is to be used as the retry_configs value, then that might contain different public keys. (Nonetheless, when a private key is present, that MUST match the public key from one of the ECHConfig values.)

4. Security Considerations

Storing cryptographic keys in files leaves them vulnerable should anyone get read access to the filesystem on which they are stored. The same protection mechanisms that would be used for a server's PEM encoded HTTPS certificate private key should be used for the PEM ECH configuration.

The security considerations of [I-D.ietf-tls-svcb-ech] apply when retrieving an ECHConfigList from the DNS.

For clarity, only the ECHConfigList is to be published in the DNS - the private key from an ECH PEM file MUST NOT be published in the DNS.

5. Acknowledgements

Thanks to Daniel McCarney, Jim Reid and Peter Yee for comments.

6. IANA Considerations

This document contains no IANA considerations.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/info/rfc4648>.

[RFC7468] Josefsson, S. and S. Leonard, "Textual Encodings of PKIX, PKCS, and CMS Structures", RFC 7468, DOI 10.17487/RFC7468, April 2015, <https://www.rfc-editor.org/info/rfc7468>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[I-D.ietf-tls-esni]
Rescorla, E., Oku, K., Sullivan, N., and C. A. Wood, "TLS Encrypted Client Hello", Work in Progress, Internet-Draft, draft-ietf-tls-esni-25, 14 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-esni-25>.

7.2. Informative References

[RFC9460] Schwartz, B., Bishop, M., and E. Nygren, "Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)", RFC 9460, DOI 10.17487/RFC9460, November 2023, <https://www.rfc-editor.org/info/rfc9460>.

[I-D.ietf-tls-svcb-ech]
Schwartz, B. M., Bishop, M., and E. Nygren, "Bootstrapping TLS Encrypted ClientHello with DNS Service Bindings", Work in Progress, Internet-Draft, draft-ietf-tls-svcb-ech-08, 16 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-svcb-ech-08>.

Appendix A. Changes

From -12 to -13:

* Changes resulting from IESG review.

From -11 to -12:

* Changes resulting from IETF last call reviews.

From -10 to -11:

* Change to standards track as agreed with shepherd/AD.

From -09 to -10:

* Tweaks to fit being AD sponsored.

From -08 to -09:

* Minor clarification of encoding based on current OpenSSL ECH feature branch code.

From -07 to -08:

* Processed some github comments

From -06 to -07:

* Refresh due to expiry.

From -05 to -06:

* Refresh due to expiry.

From -04 to -05:

* Refresh due to expiry.

From -03 to -04:

* Refresh due to expiry.

From -02 to -03:

* Refresh due to expiry and not possible ISE destination

From -01 to -02:

* ECHO -> ECH

From -00 to -01:

* ESNI -> ECHO

Author’s Address

Stephen Farrell
Trinity College Dublin
Dublin
2
Ireland
Phone: +353-1-896-2354
Email: stephen.farrell@cs.tcd.ie