TLS Working Group
Internet-Draft
Intended status: Standards Track
Expires: 18 December 2025

B. Schwartz
Meta Platforms, Inc.
M. Bishop
E. Nygren
Akamai Technologies

16 June 2025

Bootstrapping TLS Encrypted ClientHello with DNS Service Bindings
draft-ietf-tls-svcb-ech-08

Abstract

To use TLS Encrypted ClientHello (ECH) the client needs to learn the ECH configuration for a server before it attempts a connection to the server. This specification provides a mechanism for conveying the ECH configuration information via DNS, using a SVCB or HTTPS resource record (RR).

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 18 December 2025.

Copyright Notice

Table of Contents

1. Overview

The Service Bindings framework [SVCB] allows server operators to publish a detailed description of their service in the Domain Name System (see [RFC1034], [BCP219]) using SVCB or HTTPS records. Each SVCB record describes a single "alternative endpoint", and contains a collection of "SvcParams" that can be extended with new kinds of information that may be of interest to a client. Clients can use the SvcParams to improve the privacy, security, and performance of their connection to this endpoint.

This specification defines a new SvcParam to enable the use of TLS Encrypted ClientHello [ECH] in TLS-based protocols. This SvcParam can be used in SVCB, HTTPS or any future SVCB-compatible DNS records, and is intended to serve as the primary bootstrap mechanism for ECH.

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. SvcParam for ECH configuration

The "ech" SvcParamKey conveys the ECH configuration of an alternative endpoint. It is applicable to all schemes that use TLS-based protocols (including DTLS [RFC9147] and QUIC version 1 [RFC9001]) unless otherwise specified.

In wire format, the value of the parameter is an ECHConfigList (Section 4 of [ECH]), including the redundant length prefix. In presentation format, the value is the ECHConfigList in Base 64 Encoding (Section 4 of [RFC4648]). Base 64 is used here to simplify integration with TLS server software. To enable simpler parsing, this SvcParam MUST NOT contain escape sequences.

```
ech="AEj+DQBEAQAgACAdd+scUi0IYFsXnUIU7ko2Nd9+F8M26pAGZVpz/KrWPgAEAAEAAWQ
VZWNoLXNpdGVzLmV4YW1wbGUubmV0AAA="
```

Figure 1: ECH SvcParam with a public_name of "ech-sites.example.net".

4. Requirements for server deployments

When publishing a record containing an "ech" parameter, the publisher MUST ensure that all IP addresses of TargetName correspond to servers that have access to the corresponding private key or are authoritative for the public name. (See Sections 6.1.7 and 8.1.1 of [ECH] for requirements related to the public name.) Otherwise, connections will fail entirely.

These servers SHOULD support a protocol version that is compatible with ECH. At the time of writing, the compatible versions are TLS 1.3, DTLS 1.3, and QUIC version 1. If the server does not support a compatible version, each connection attempt will have to be retried, delaying the connection and wasting resources.

5. Requirements for client implementations

This section describes client behavior in using ECH configurations provided in SVCB or HTTPS records.

5.1. Disabling fallback

The SVCB-optional client behavior specified in (Section 3 of [SVCB]) permits clients to fall back to a direct connection if all SVCB options fail. This behavior is not suitable for ECH, because fallback would negate the privacy benefits of ECH. Accordingly, ECH-capable SVCB-optional clients MUST switch to SVCB-reliant connection establishment if SVCB resolution succeeded (as defined in Section 3 of [SVCB]) and all alternative endpoints have an "ech" SvcParam.

5.2. ClientHello construction

When ECH is in use, the TLS ClientHello is divided into an unencrypted "outer" and an encrypted "inner" ClientHello. The outer ClientHello is an implementation detail of ECH, and its contents are controlled by the ECHConfig in accordance with [ECH]. The inner ClientHello is used for establishing a connection to the service, so its contents may be influenced by other SVCB parameters. For example, the requirements related to ALPN protocol identifiers in Section 7.1.2 of [SVCB] apply only to the inner ClientHello. Similarly, it is the inner ClientHello whose Server Name Indication (SNI) identifies the desired service.

5.3. Performance optimizations

Prior to retrieving the SVCB records, the client does not know whether they contain an "ech" parameter. As a latency optimization, clients MAY prefetch DNS records that will only be used if this parameter is not present (i.e. only in SVCB-optional mode).

The "ech" SvcParam alters the contents of the TLS ClientHello if it is present. Therefore, clients that support ECH MUST NOT issue any TLS ClientHello until after SVCB resolution has completed. (See Section 5.1 of [SVCB]).

6. Interaction with HTTP Alt-Svc

HTTP clients that implement both HTTP Alt-Svc [RFC7838] and the HTTPS record type [SVCB] can use them together, provided that they only perform connection attempts that are "consistent" with both sets of parameters (Section 9.3 of [SVCB]). At the time of writing, there is no defined parameter related to ECH for Alt-Svc. Accordingly, a connection attempt that uses ECH is considered "consistent" with an Alt-Svc Field Value that does not mention ECH.

Origins that publish an "ech" SvcParam in their HTTPS record SHOULD also publish an HTTPS record with the "ech" SvcParam for every alt-authority offered in its Alt-Svc Field Values. Otherwise, clients might reveal the name of the server in an unencrypted ClientHello to an alt-authority.

If all HTTPS records for an alt-authority contain "ech" SvcParams, the client MUST adopt SVCB-reliant behavior (as in Section 5.1) for that RRSet. This precludes the use of certain connections that Alt-Svc would otherwise allow, as discussed in Section 9.3 of [SVCB].

7. Examples

```
$ORIGIN simple.example. ; Simple example zone
@ 300 IN A     192.0.2.1
         AAAA  2001:db8::1
         HTTPS 1 . ech=ABC...
www 300 IN A 192.0.2.1
           AAAA 2001:db8::1
           HTTPS 1 . ech=ABC...
```

Figure 2: Simple example zone with the same configuration on the apex and web domain. It is compatible with clients that do or do not support HTTPS records.

```
$ORIGIN heterogeneous.example. ; Example zone with two pools of servers
pool1 300 IN    A    192.0.2.1
                AAAA 2001:db8:1::a
pool2 300 IN    A    192.0.2.2
                AAAA 2001:db8:2::a
service 300 IN SVCB 1 pool1 ech=ABC...
               SVCB 1 pool2 ech=DEF...
               A 192.0.2.1
               A 192.0.2.2
               AAAA 2001:db8:1::a
               AAAA 2001:db8:2::a
```

Figure 3: Service that allows clients to choose between two server pools with different ECH configurations.

```
$ORIGIN cdn.example. ; CDN operator zone
pool 300 IN A 192.0.2.1
           AAAA 2001:db8::1
           HTTPS 1 . ech=ABC...

$ORIGIN customer.example. ; CDN customer's zone
@   3600 IN HTTPS 0 pool.cdn.example.
; Apex IP records for compatibility with clients that do not support
; HTTPS records.
@   300  IN A    192.0.2.1
           AAAA 2001:db8::1

www 300  IN CNAME pool.cdn.example.
```

Figure 4: ECH usage pattern for an aliasing-based CDN.

```
$ORIGIN secret.example. ; High confidentiality zone
www     3600 IN HTTPS 1 backend ech=ABC... mandatory=ech
backend 300  IN A     192.0.2.1
               AAAA  2001:db8::1
```

Figure 5: A domain that is only reachable using ECH.

```
$ORIGIN cdn1.example. ; First CDN operator zone
pool 300 IN A     192.0.2.1
           AAAA  2001:db8::1
           HTTPS 1 . ech=ABC...

$ORIGIN cdn2.example. ; Second CDN operator zone
pool 300 IN A     192.0.2.2
           AAAA  2001:db8::2
           HTTPS 1 . ech=DEF...

;; Multi-CDN customer zone (version 1)
$ORIGIN customer.example.
@   3600 IN HTTPS 0 pool.cdn1.example.
; Apex IP records for compatibility with clients that do not support
; HTTPS records.
@   300  IN A    192.0.2.1
           AAAA 2001:db8::1
www 3600  IN CNAME pool.cdn1.example.

;; Multi-CDN customer zone (version 2)
@   3600 IN HTTPS 0 pool.cdn2.example.
@   300  IN A    192.0.2.2
           AAAA 2001:db8::2
www 3600  IN CNAME pool.cdn2.example.
```

Figure 6: Multi-CDN configuration using server-side selection.

```
$ORIGIN dns.example. ; DNS server example.
@    3600 IN A     192.0.2.1
             AAAA  2001:db8::1
             HTTPS 1 . ech=ABC... alpn=h3 dohpath=/q{?dns}

_dns 3600 IN SVCB  1 @ ech=ABC... alpn=dot,doq,h3 dohpath=/q{?dns}
```

Figure 7: Example of a DNS server that supports ECH.

8. Security Considerations

A SVCB RRSet containing some RRs with "ech" and some without is vulnerable to a downgrade attack: a network intermediary can block connections to the endpoints that support ECH, causing the client to fall back to a non-ECH endpoint. This configuration is NOT RECOMMENDED, but it may be unavoidable when combining endpoints from different providers or conducting a staged rollout. Zone owners who do use such a mixed configuration SHOULD mark the RRs with "ech" as more preferred (i.e. lower SvcPriority value) than those without, in order to maximize the likelihood that ECH will be used in the absence of an active adversary.

When Encrypted ClientHello is deployed, the inner TLS SNI is protected from disclosure to attackers. However, there are still many ways that an attacker might infer the SNI. Even in an idealized deployment, ECH’s protection is limited to an anonymity set consisting of all the ECH-enabled server domains supported by a given client-facing server that share an ECH configuration. An attacker who can enumerate this set can always guess the encrypted SNI with probability at least 1/K, where K is the number of domains in the set. Some attackers may achieve much greater accuracy using traffic analysis, popularity weighting, and other mechanisms (see e.g., [CLINIC]).

ECH ensures that TLS does not disclose the SNI, but the same information is also present in the DNS queries used to resolve the server’s hostname. This specification does not conceal the server name from the DNS resolver. If DNS messages are sent between the client and resolver without authenticated encryption, an attacker on this path can also learn the destination server name. A similar attack applies if the client can be linked to a request from the resolver to a DNS authority.

An attacker who can prevent SVCB resolution can deny clients any associated security benefits. A hostile recursive resolver can always deny service to SVCB queries, but network intermediaries can

often prevent resolution as well, even when the client and recursive resolver validate DNSSEC [RFC9364] and use a secure transport. These downgrade attacks can prevent a client from being aware that "ech" is configured which could result in the client sending the ClientHello in cleartext. To prevent downgrades, Section 3.1 of [SVCB] recommends that clients abandon the connection attempt when such an attack is detected.

9. IANA Considerations

In the "DNS SVCB Service Parameter Keys (SvcParamKeys)" registry on the "DNS Service Bindings (SVCB)" page, IANA is instructed to modify the entry for "ech" as follows:

Number	Name	Meaning	Format Reference	Change Controller
5	ech	TLS Encrypted ClientHello Config	(This document)	IETF

Table 1

10. References

10.1. Normative References

[ECH] 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>.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/rfc/rfc1034>.

[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/rfc/rfc2119>.

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

[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/rfc/rfc8174>.

[RFC9364] Hoffman, P., "DNS Security Extensions (DNSSEC)", BCP 237, RFC 9364, DOI 10.17487/RFC9364, February 2023, <https://www.rfc-editor.org/rfc/rfc9364>.

[SVCB] 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/rfc/rfc9460>.

10.2. Informative References

[BCP219] Best Current Practice 219, <https://www.rfc-editor.org/info/bcp219>. At the time of writing, this BCP comprises the following:

Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219, RFC 9499, DOI 10.17487/RFC9499, March 2024, <https://www.rfc-editor.org/info/rfc9499>.

[CLINIC] Miller, B., Huang, L., Joseph, A., and J. Tygar, "I Know Why You Went to the Clinic: Risks and Realization of HTTPS Traffic Analysis", Springer International Publishing, Lecture Notes in Computer Science pp. 143-163, DOI 10.1007/978-3-319-08506-7_8, ISBN ["9783319085050", "9783319085067"], 2014, <https://doi.org/10.1007/978-3-319-08506-7_8>.

[RFC7838] Nottingham, M., McManus, P., and J. Reschke, "HTTP Alternative Services", RFC 7838, DOI 10.17487/RFC7838, April 2016, <https://www.rfc-editor.org/rfc/rfc7838>.

[RFC9001] Thomson, M., Ed. and S. Turner, Ed., "Using TLS to Secure QUIC", RFC 9001, DOI 10.17487/RFC9001, May 2021, <https://www.rfc-editor.org/rfc/rfc9001>.

[RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", RFC 9147, DOI 10.17487/RFC9147, April 2022, <https://www.rfc-editor.org/rfc/rfc9147>.

Authors' Addresses

Ben Schwartz
Meta Platforms, Inc.

Email: ietf@bemasc.net

Mike Bishop
Akamai Technologies
Email: mbishop@evequefou.be

Erik Nygren
Akamai Technologies
Email: erik+ietf@nygren.org