Transport Layer Security
Internet-Draft
Updates: 8446 (if approved)
Intended status: Standards Track
Expires: 2 March 2026

D. Benjamin
Google LLC

29 August 2025

TLS Key Share Prediction
draft-ietf-tls-key-share-prediction-03

Abstract

This document defines a mechanism for servers to communicate key share preferences in DNS. Clients may use this information to reduce TLS handshake round-trips.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://tlswg.github.io/tls-key-share-prediction/draft-ietf-tls-key-share-prediction.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-tls-key-share-prediction/.

Discussion of this document takes place on the Transport Layer Security Working Group mailing list (mailto:tls@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/tls/. Subscribe at https://www.ietf.org/mailman/listinfo/tls/.

Source for this draft and an issue tracker can be found at https://github.com/tlswg/tls-key-share-prediction.

Status of This Memo

This Internet-Draft will expire on 2 March 2026.

Table of Contents

1. Introduction

Named groups in TLS 1.3 [RFC8446] are negotiated with two lists in the ClientHello: The client sends its full preferences in the supported_groups extension, but also generates key shares for a subset in the key_share extension. Named groups in this subset may be used in one, while named groups outside the subset requires a HelloRetryRequest and two round trips. The additional round trip is undesirable for performance, but unused key shares consume network and computational resources, so clients often do not generate key shares for all groups.

Post-quantum key encapsulation methods (KEMs) have large keys and ciphertexts, so network costs are particularly pronounced. As a TLS ecosystem transitions from one post-quantum KEM to another, it is challenging to pick key shares without prior knowledge of the server's policies:

1. Predicting both post-quantum KEMs consumes excessive bandwidth on the unused option.

2. Predicting the old post-quantum KEM adds a round-trip cost to newer servers. Servers will be unlikely to transition as a result.

3. Predicting the new post-quantum KEM adds a round-trip cost to older servers. Particularly early in the transition, when most servers do not implement the new KEM, this may significantly regress performance.

This document defines a method for servers to declare their named group preferences in DNS, using SVCB or HTTPS resource records [RFC9460]. This allows the client to predict key shares more accurately.

2. Conventions and Definitions

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. DNS Service Parameter

This document defines the tls-supported-groups SvcParamKey [RFC9460], which specifies the endpoint’s TLS supported group preferences, as a non-empty sequence of TLS NamedGroup codepoints in order of decreasing preference, with no duplicates. This allows clients connecting to the endpoint to reduce the likelihood of needing a HelloRetryRequest.

3.1. Format

The presentation value of the SvcParamValue is a non-empty comma-separated list (Appendix A.1 of [RFC9460]) of decimal integers between 0 and 65535 (inclusive) in ASCII, with no duplicate integers. Any other value is a syntax error. To enable simpler parsing, this SvcParam MUST NOT contain escape sequences.

The wire format of the SvcParamValue is a sequence of 2-octet numeric values in network byte order. An empty list of values is invalid, as is a list containing duplicates.

For example, a TLS server which prefers x25519 (29) and also supports secp256r1 (23) would add a tls-supported-groups SvcParamValue containing 29 and 23. The presentation value would be "29,23". The wire format of the SvcParamValue would be four octets, represented in hexadecimal as 001d0017.

The following is an example of the value appearing in a complete DNS record in the presentation syntax:

```
example.net.  7200  IN SVCB 3 server.example.net. (
    port="8004" tls-supported-groups=29,23 )
```

3.2. Configuring Services

Services SHOULD include supported TLS named groups, in order of decreasing preference in the tls-supported-groups parameter of their HTTPS or SVCB endpoints. As TLS preferences are updated, services SHOULD update the DNS record to match. Services MAY include GREASE values [RFC8701] in this list.

3.3. Client Behavior

When connecting to a service endpoint whose HTTPS or SVCB record contains the tls-supported-groups parameter, the client evaluates the server preferences against its own to predict which named group will be chosen. When evaluating the server preferences, the client MUST ignore any codepoints that it does not support or recognize. If there is a named group in common, the client MAY send a key_share extension containing just that named group in the initial ClientHello. To avoid downgrade attacks, the client MUST continue to send its full preferences in the supported_groups extension. See Section 4 for additional discussion on downgrades.

3.4. Misprediction

Although this service parameter is intended to reduce key share mispredictions, mispredictions may still occur in some scenarios. For example:

* The client has fetched a stale HTTPS or SVCB record that no longer reflects the server preferences

* The server is in the process of deploying a change to named group preferences, and different server instances temporary evaluate different preferences

* The client was unable to fetch the HTTPS or SVCB record

* The client and server implement incompatible selection algorithms, such that client's evaluation of the service parameter did not match the server's final selection

Clients and servers MUST correctly handle mispredictions by responding to and sending HelloRetryRequest, respectively.

4. Security Considerations

This document introduces a mechanism for clients to vary the key_share extension based on DNS. DNS responses are unauthenticated in many deployments, so this can permit attacker influence over the client's predicted named groups. That, in turn, can influence the named group selected by the TLS server, as TLS's downgrade protections only extend to the ClientHello itself. However, the client continues to send its full preferences in supported_groups, so this influence is limited by the server's named group selection policy:

Servers which select purely based on preference orders will first select a named group on supported_groups, and then consider key_share only to send HelloRetryRequest or ServerHello. When connecting to such servers, attackers cannot influence the selection with this mechanism.

However, some servers prioritize round-trip times over preference orders. That is, when choosing between a named group in key_share and a more preferable (e.g. more secure) named group not in key_share, these servers will select the less preferable one in key_share. In this case, an attacker may be able to influence the selection by forging an HTTPS or SVCB record. Per Section 4.2.8 of [RFC8446], the client's key_share extension does not reflect its full preference list in supported_groups. Thus, this server behavior is only appropriate when the two options are of comparable preference, such that round trip concerns dominate. In particular, it is NOT RECOMMENDED when choosing between post-quantum and classical named groups.

As these semantics were already prescribed in [RFC8446], it is safe for clients to admit attacker control over the set of named groups preferred in key_share, provided supported_groups always reflects the true client preference. Servers are expected to evaluate the combination of key_share and supported_groups according to the defined semantics and their selection goals.

To reduce the risk of downgrade attacks with incorrectly deployed servers, clients MAY choose to ignore tls-supported-groups when the result would predict a less preferred group. For example, a client

that implements a combination of post-quantum groups and ECDH groups MAY limit its influence to predicting post-quantum groups. This optimizes transitions between post-quantum groups, where the bandwidth concerns are more pronounced, but means ECDH-only servers cannot take advantage of the mechanism.

5. IANA Considerations

This document updates the Service Parameter Keys registry [RFC9460] with the following entry:

Number	Name	Meaning	Format Reference	Change Controller
9	tls-supported-groups	Supported groups in TLS	(this document) Section 3.1	IETF

Table 1

6. 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/rfc/rfc2119>.

[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>.

[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/rfc/rfc8446>.

[RFC8701] Benjamin, D., "Applying Generate Random Extensions And Sustain Extensibility (GREASE) to TLS Extensibility", RFC 8701, DOI 10.17487/RFC8701, January 2020, <https://www.rfc-editor.org/rfc/rfc8701>.

[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/rfc/rfc9460>.

Acknowledgments

The author would like to thank David Adrian, Bob Beck, Sophie Schmieg, Martin Thomson, and Bas Westerbaan for discussions and review of this document.

Author’s Address

David Benjamin
Google LLC
Email: davidben@google.com