Workgroup: TLS
Internet-Draft: draft-cem-compressed-curves-01
Published: 25 October 2021
Intended Status: Informational
Expires: 28 April 2022
Authors: C. Mehner
USAA

TLS Compressed Elliptic Curve Code Points

Abstract

This document defines new Transport Layer Security (TLS) Supported Groups to allow negotiation in TLS for encoding certain elliptic curve public keys in a compressed form rather than the more verbose method specified in [RFC8446] and [RFC8422].

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 28 April 2022.

Table of Contents

1. Introduction

Versions of TLS prior to 1.3 allowed for Elliptic Curve Cryptography (ECC) Point Compression negotiation, by sending a however in TLS 1.3 and Section 5.1.2 of [RFC8422], that mechanism was deprecated in favor of having one point encoding format for each negotiated curve. Utilizing point compression is important to reduce the size of negotiated curves within TLS in general, but especially with [I-D.draft-ietf-tls-ctls].

The code points defined in this document are intended for use in TLS, dTLS, cTLS, and other similar protocols that negotiate Elliptic Curve Groups for key exchange.

1.1. 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.

All TLS notation comes from Section 3 of [RFC8446].

2. Supported Groups

This document defines three new TLS Supported Groups for the compressed forms of secp256r1, secp384r1, and secp521r1 (collectively colloquially called the NIST Curves). The compressed forms of these groups are indicated by adding a letter 'c' at the end of the descriptive name. The new groups are secp256r1c, secp384r1c, and secp521r1c. TLS groups using compressed NIST curves MUST use these newly defined group identifiers.

The "TLS Supported Groups" name space is maintained by IANA.

```
enum {
  secp256r1c(tbd1), secp384r1c(tbd2), secp521r1c(tbd3)
} NamedGroup;

struct {
  NamedGroup named_group_list<2..2^16-1>;
} NamedGroupList;
```

2.1. ECDHE Parameters

In Section 4.2.8.2 of [RFC8446] the encoding method for ECDHE Parameters is described, this document adds a new struct to serialize the new parameters. The method for determining the values for the elements of the serialized structure are documented in [SEC1].

For secp256r1c, secp384r1c, and secp521r1c, the contents are the serialized value of the following struct defined using the presentation language in Section 3 of [RFC8446]:

```
struct {
  CompressedY;
  opaque X[coordinate_length];
} CompressedPointRepresentation;

enum { evenY(2), oddY(3) } CompressedY
```

3. IANA Considerations

IANA is requested to assign the value tbd1 to secp256r1c, the value tbd2 to secp384r1c, and the value tbd3 to secp521r1c in the "TLS Supported Groups" registry. For these three new supported groups the "DTLS OK" is set to 'Y'. For tbd1 and tbd2 the "Recommended" column is set to 'Y' and for tbd3 the "Recommended" column is set to 'N'.

4. Security Considerations

The security considerations of [RFC8422] and [RFC8422] apply to the selection of TLS named groups and the use of the curves specified in this document.

5. References

5.1. 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>.

[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>.

[RFC8422] Nir, Y., Josefsson, S., and M. Pegourie-Gonnard, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier", RFC 8422, DOI 10.17487/RFC8422, August 2018, <https://www.rfc-editor.org/info/rfc8422>.

[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>.

[SEC1] Brown, D., "Standards for Efficient Cryptography 1 (SEC 1)", Standards for Efficient Cryptography Group , 21 May 2009, <https://www.secg.org/sec1-v2.pdf>.

5.2. Informative References

[I-D.draft-ietf-tls-ctls] Rescorla, E., Barnes, R., and H. Tschofenig, "Compact TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-ctls-04, 25 October 2021, <https://www.ietf.org/archive/id/draft-ietf-tls-ctls-04.txt>.

Author's Address

Carl Mehner
USAA

Email: carl.mehner@usaa.com