Network Working Group
Internet-Draft
Updates: 4492 (if approved)
Intended status: Informational
Expires: March 15, 2015

S. Josefsson
SJD AB
M. Pegourie-Gonnard
Independant / PolarSSL

September 11, 2014

Additional Elliptic Curves for Transport Layer Security (TLS) Key Agreement
draft-josefsson-tls-additional-curves-01

Abstract

This document specifies the use of additional elliptic curves (M-221, E-222, Curve1174, E-382, M-383, Curve383187, Curve41417, Ed448-Goldilocks, M-511, and E-521) for key exchange in the Transport Layer Security (TLS) protocol. As such it updates RFC 4492.

1. Introduction

In [SafeCurves] and [I-D.ladd-safecurves] additional elliptic curves are described that have performance and security advantages, of different strengths, for uses that may include key agreement. The complete list of curves is M-221 (aka Curve2213), E-222, Curve1174, E-382, M-383, Curve383187, Curve41417 (aka Curve3617), Ed448-Goldilocks, M-511 (aka Curve511187), and E-521. In this document we refer to that list of curves informally as "additional safe curves" or simply "additional curves".

Note that Curve25519 is excluded from this document since it is covered in [I-D.josefsson-tls-curve25519]. These two drafts may eventually be merged. Currently the Curve25519 draft is more mature and ready for implementation, whereas this draft is more food for discussion.

[RFC4492] defines the usage of elliptic curves for authentication and key agreement in TLS 1.0 and TLS 1.1, and these mechanisms are also applicable to TLS 1.2 [RFC5246]. The use of ECC curves for key exchange requires the definition and assignment of additional NamedCurve IDs. This document specify that value for the additional curves, as well as the minor changes in key selection and representation that are required to accommodate for the curves slightly different nature.

This document only describes usage of additional curves for ephemeral key exchange (ECDHE), not for use with long-term keys embedded in PKIX certificates (ECDH_RSA and ECDH_ECDSA). This is because the additional curves are not directly suitable for authentication with ECDSA, and thus not applicable for signing of e.g. PKIX certificates.

2. New NamedCurve type

Curve negotiation is the same for the additional curves as for other curves, but is restricted to using the named_curve type in the ServerKeyEchange message: the explicit_prime type is only suited to curves in short Weierstrass form. This document adds a new NamedCurve value for the additional curves as follows.

```
enum {
  M221(TBD1),
  E222(TBD2),
  Curve1174(TBD3),
  E382(TBD4),
  M383(TBD5),
  Curve383187(TBD6),
  Curve41417(TBD7),
  Ed448-Goldilocks(TBD8),
  M511(TBD9),
  E521(TBD10)
} NamedCurve;
```

The curves are suitable for use with DTLS [RFC6347].

Since these curves are not designed to be used in signatures, clients who offer ECDHE_ECDSA ciphersuites and advertise support for any of these curves in the elliptic_curves ClientHello extension SHOULD also advertise support for at least one other curve, suitable for ECDSA. Servers MUST NOT select an ECDHE_ECDSA ciphersuite if the only common curve is one of these curves.

3. Acknowledgement

This document was inspired by the content and structure of [RFC7027].

4. IANA Considerations

IANA is requested to assign numbers for the additional curves listed in Section 2 to the Transport Layer Security (TLS) Parameters registry EC Named Curve [IANA-TLS] as follows.

Value	Description	DTLS-OK	Reference
TBD1	M221	Y	This doc
TBD2	E222	Y	This doc
TBD3	Curve1174	Y	This doc
TBD4	E382	Y	This doc
TBD5	M383	Y	This doc
TBD6	Curve383187	Y	This doc
TBD7	Curve41417	Y	This doc
TBD8	Ed448-Goldilocks	Y	This doc
TBD9	M511	Y	This doc
TBD10	E521	Y	This doc

Table 1

5. Security Considerations

The security considerations of [RFC5246] and most of the security considerations of [RFC4492] apply accordingly.

See also [SafeCurves] and [I-D.ladd-safecurves] for more security discussions.

6. References

6.1. Normative References

[RFC4492] Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", RFC 4492, May 2006.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[I-D.ladd-safecurves]
Ladd, W., "Additional Elliptic Curves for IETF protocols", draft-ladd-safecurves-04 (work in progress), March 2014.

6.2. Informative References

[RFC7027] Merkle, J. and M. Lochter, "Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS)", RFC 7027, October 2013.

[I-D.josefsson-tls-curve25519]
Josefsson, S. and M. Pegourie-Gonnard, "Curve25519 for ephemeral key exchange in Transport Layer Security (TLS)", draft-josefsson-tls-curve25519-05 (work in progress), April 2014.

[IANA-TLS]
Internet Assigned Numbers Authority, "Transport Layer Security (TLS) Parameters", <http://www.iana.org/assignments/tls-parameters/tls-parameters.xml>.

[SafeCurves]
Bernstein, D. and T. Lange, "SafeCurves: choosing safe curves for elliptic-curve cryptography.", January 2014, <http://safecurves.cr.yp.to/>.

Authors' Addresses

Simon Josefsson
SJD AB

Email: simon@josefsson.org

Manuel Pegourie-Gonnard
Independant / PolarSSL

Email: mpg@elzevir.fr