Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 10, 2015

S. Josefsson
SJD AB

June 8, 2015

EdDSA and Ed25519 for Transport Layer Security (TLS) draft-josefsson-tls-eddsa-01

Abstract

This document introduce the public-key signature algorithm EdDSA for use in Transport Layer Security (TLS). With the previous NamedCurve and ECPointFormat assignments for the Curve25519 ECDHE key exchange mechanism, this enables use of Ed25519 in TLS. New Cipher Suites for EdDSA together with AES-GCM and ChaCha20-Poly1305 are introduced here. This is intended to work with any version of TLS and Datagram TLS.

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 http://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 December 10, 2015.

Copyright Notice

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

1. Introduction

TLS [RFC5246] and DTLS [RFC6347] support different key exchange algorithms and authentication mechanisms. In ECC in TLS [RFC4492], key exchange and authentication using ECC is specified, where the NamedCurve and ECPointFormat registries and associated TLS extensions are introduced.

In [I-D.josefsson-tls-curve25519] support for ECDHE key exchange with the Curve25519 curve is added. That document introduces a new NamedCurve value for Curve25519, and a new ECPointFormat value to correspond to the public-key encoding.

This document describes how to use EdDSA and Ed25519 [I-D.josefsson-eddsa-ed25519] as a new authentication mechanism in TLS, reusing the NamedCurve and ECPointFormat values already introduced for Curve25519, and finally specifying new Cipher Suites for Ed25519 with AES-GCM [RFC5288] and ChaCha20-Poly1305 [I-D.mavrogiannopoulos-chacha-tls].

This document is a self-contained alternative to draft-josefsson-tls-eddsa2. This document specify new cipher suites for EdDSA, whereas draft-josefsson-tls-eddsa2 reuse the ECDSA cipher suites for EdDSA. It is an open issue which approach is to be prefered.

1.1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. The ECDHE_EDDSA Key Exchange Algorithm

Negotiation of the authentication mechanism is signalled by sending a SignatureAlgorithm value. Here we extend this enumeration for EdDSA.

```
enum {
   eddsa(4)
} SignatureAlgorithm;
```

EdDSA is suitable for use with TLS [RFC5246] and DTLS [RFC6347].

The new key exchange mechanism ECDHE_EDDSA provides forward secrecy. The key exchange mechanism works just like ECDHE_ECDSA but with ECDSA

replaced with EDDSA. Currently the only applicable curve is Curve25519.

The HashAlgorithm value to specify for EdDSA MUST be "none" as the EdDSA signature algorithm does not hash the input before signing.

3. Cipher Suites

The following Cipher Suite values are registered, using the ChaCha20/Poly1305 authenticated encryption with additional data (AEAD) cipher described in [I-D.mavrogiannopoulos-chacha-tls] and the AES Galois Counter Mode (GCM) cipher. The AES-GCM cipher suites use the AEAD algorithms AEAD_AES_128_GCM and AEAD_AES_256_GCM described in [RFC5116]. GCM is used as described in [RFC5288], but see also [RFC5289].

```
CipherSuite TLS_ECDHE_EDDSA_WITH_CHACHA20_POLY1305  = { 0xCC, 0xB0 }
CipherSuite TLS_ECDHE_EDDSA_WITH_AES_128_GCM_SHA256 = { 0xCC, 0xB1 }
CipherSuite TLS_ECDHE_EDDSA_WITH_AES_256_GCM_SHA384 = { 0xCC, 0xB2 }
```

The cipher suites are suitable for TLS [RFC5246] and DTLS [RFC6347].

4. IANA Considerations

EdDSA should be registered in the Transport Layer Security (TLS) Parameters [IANA-TLS] registry under "SignatureAlgorithm" as follows.

Value	Description	DTLS-OK	Reference
4	eddsa	Y	This doc

The follow cipher suites should be registered in the TLS Parameters registry under "TLS Cipher Suite Registry" as follows. They should all be marked as DTLS-OK.

```
CipherSuite TLS_ECDHE_EDDSA_WITH_CHACHA20_POLY1305  = { 0xCC, 0xB0 }
CipherSuite TLS_ECDHE_EDDSA_WITH_AES_128_GCM_SHA256 = { 0xCC, 0xB1 }
CipherSuite TLS_ECDHE_EDDSA_WITH_AES_256_GCM_SHA384 = { 0xCC, 0xB2 }
```

5. Security Considerations

The security considerations of TLS [RFC5246], DTLS [RFC6347], ECC in TLS [RFC4492] Curve25519 in TLS [I-D.josefsson-tls-curve25519], EdDSA and Ed25519 [I-D.josefsson-eddsa-ed25519], ChaCha20-Poly1305

[I-D.mavrogiannopoulos-chacha-tls], AES-GCM [RFC5116] an AES-GCM in TLS [RFC5288] are inherited.

As with all cryptographic algorithms, the reader should stay informed about new research insights into the security of the algorithms involved.

While discussed in the EdDSA/Ed25519 specification and papers, we would like to stress the significance of secure implementation of EdDSA/Ed25519. For example, implementations ought to be constant-time to avoid certain attacks.

6. Acknowledgements

Thanks to Klaus Hartke and Nicolas Williams for fixes to the document.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[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.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, January 2008.

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

[RFC5288] Badra, M. and I. Hajjeh, "ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)", RFC 5288, March 2009.

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

[I-D.josefsson-tls-curve25519] Josefsson, S. and M. Pegourie-Gonnard, "Curve25519 for ephemeral key exchange in Transport Layer Security (TLS)", draft-josefsson-tls-curve25519-06 (work in progress), September 2014.

[I-D.josefsson-eddsa-ed25519]
Josefsson, S. and N. Moller, "EdDSA and Ed25519", draft-josefsson-eddsa-ed25519-02 (work in progress), February 2015.

[I-D.mavrogiannopoulos-chacha-tls]
Langley, A., Chang, W., Mavrogiannopoulos, N., Strombergson, J., and S. Josefsson, "The ChaCha Stream Cipher for Transport Layer Security", draft-mavrogiannopoulos-chacha-tls-04 (work in progress), December 2014.

7.2. Informative References

[RFC5289] Badra, M. and I. Hajjeh, "ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)", RFC 5289, March 2009.

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

Author's Address

Simon Josefsson
SJD AB

Email: simon@josefsson.org