

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 31, 2015

J. Mattsson
D. Migault
Ericsson
June 29, 2015

ECDHE_PSK with AES-GCM and AES-CCM Cipher Suites
for Transport Layer Security (TLS)
draft-mattsson-tls-ecdhe-psk-aead-00

Abstract

This memo defines several new cipher suites for the Transport Layer Security (TLS) protocol. The cipher suites are all based on the Ephemeral Elliptic Curve Diffie-Hellman with Pre-Shared Key (ECDHE_PSK) key exchange together with the Authenticated Encryption with Associated Data (AEAD) algorithms AES-GCM and AES-CCM. PSK provides light and efficient authentication, ECDHE provides perfect forward secrecy, and AES-GCM and AES-CCM provides encryption and integrity protection.

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 31, 2015.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. ECDHE_PSK with AES-GCM and AES-CCM Cipher Suites	3
3. Applicable TLS Versions	3
4. IANA Considerations	3
5. Security Considerations	4
6. Acknowledgements	4
7. References	4
Authors' Addresses	5

1. Introduction

This document defines new cipher suites that provide Pre-Shared Key (PSK) authentication, Perfect Forward Secrecy (PFS), and Authenticated Encryption with Associated Data (AEAD).

Pre-Shared Key (PSK) Authentication is widely used in many scenarios. One deployment is 3GPP networks where pre-shared keys are used to authenticate both subscriber and network. Another deployment is Internet of Things where PSK authentication is often preferred for performance and energy efficiency reasons. In both scenarios the endpoints are owned/controlled by a party that provisions the pre-shared keys and makes sure that they provide a high level of entropy.

Perfect Forward Secrecy (PFS) is a strongly recommended feature in security protocol design and can be accomplished by using an ephemeral Diffie-Hellman key exchange method. Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) provides PFS with excellent performance and small key sizes. ECDHE is mandatory to implement in both HTTP/2 [[RFC7540](#)] and CoAP [[RFC7252](#)].

AEAD algorithms that combine encryption and integrity protection are strongly recommended [[RFC7525](#)], and non-AEAD algorithms will likely be forbidden to use in TLS1.3. The AEAD algorithms considered in this document are AES-CCM and AES-GCM. The use of AES-CCM in TLS is defined in [[RFC6655](#)] and the use of AES-GCM is defined [[RFC5288](#)].

[[RFC4279](#)] defines Pre-Shared Key (PSK) cipher suites for TLS but does not consider Elliptic Curve Cryptography. [[RFC5489](#)] introduces Elliptic Curve Cryptography for TLS but does not consider PSK authentication. [[RFC5487](#)] describes the use of AES-GCM in combination with PSK authentication, but does not consider ECDHE.

[RFC5489] describes the use of PSK in combination with ECDHE but does not consider AES-GCM or AES-CCM.

2. ECDHE_PSK with AES-GCM and AES-CCM Cipher Suites

The cipher suites defined in this document are based on the AES-GCM and AES-CCM Authenticated Encryption with Associated Data (AEAD) algorithms AEAD_AES_128_GCM, AEAD_AES_256_GCM, AEAD_AES_128_CCM, and AEAD_AES_256_CCM described in [RFC5116]. The following cipher suites are defined:

```
TLS_PSK_ECDHE_WITH_AES_128_GCM           = {TDB0,TDB1};
TLS_PSK_ECDHE_WITH_AES_256_GCM           = {TDB2,TDB3};
TLS_PSK_ECDHE_WITH_AES_128_CCM_8         = {TDB4,TDB5};
TLS_PSK_ECDHE_WITH_AES_128_CCM           = {TDB6,TDB7};
TLS_PSK_ECDHE_WITH_AES_256_CCM           = {TDB8,TDB9};
```

These cipher suites make use of the default TLS 1.2 Pseudorandom Function (PRF), which uses HMAC with the SHA-256 hash function. Clients and Servers MUST NOT negotiate curves of less than 256 bits and the Pre-Shared-Keys MUST NOT have an entropy of less than 128 bits.

3. Applicable TLS Versions

These cipher suites make use of the authenticated encryption with additional data (AEAD) defined in TLS 1.2 [RFC5246]. Earlier versions of TLS do not have support for AEAD and consequently, these cipher suites MUST NOT be negotiated in TLS versions prior to 1.2. Clients MUST NOT offer these cipher suites if they do not offer TLS 1.2 or later. Servers, which select an earlier version of TLS MUST NOT select one of these cipher suites. A client MUST treat the selection of these cipher suites in combination with a version of TLS that does not support AEAD (i.e., TLS 1.1 or earlier) as an error and generate a fatal 'illegal_parameter' TLS alert.

4. IANA Considerations

This document defines the following new cipher suites, whose values have been assigned in the TLS Cipher Suite Registry defined by [RFC5246].

```
TLS_PSK_ECDHE_WITH_AES_128_GCM           = {TDB0,TDB1};
TLS_PSK_ECDHE_WITH_AES_256_GCM           = {TDB2,TDB3};
TLS_PSK_ECDHE_WITH_AES_128_CCM_8         = {TDB4,TDB5};
TLS_PSK_ECDHE_WITH_AES_128_CCM           = {TDB6,TDB7};
TLS_PSK_ECDHE_WITH_AES_256_CCM           = {TDB8,TDB9};
```

5. Security Considerations

Most of the security considerations in [\[RFC5246\]](#), [\[RFC4279\]](#), [\[RFC4492\]](#), [\[RFC5288\]](#), [\[RFC5489\]](#), and [\[RFC6655\]](#) apply to this document as well. The cipher suites defined in this document provides perfect forward secrecy.

6. Acknowledgements

7. References

- [RFC4279] Eronen, P. and H. Tschofenig, "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", [RFC 4279](#), December 2005.
- [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] Salowey, J., Choudhury, A., and D. McGrew, "AES Galois Counter Mode (GCM) Cipher Suites for TLS", [RFC 5288](#), August 2008.
- [RFC5487] Badra, M., "Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode", [RFC 5487](#), March 2009.
- [RFC5489] Badra, M. and I. Hajjeh, "ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)", [RFC 5489](#), March 2009.
- [RFC6655] McGrew, D. and D. Bailey, "AES-CCM Cipher Suites for Transport Layer Security (TLS)", [RFC 6655](#), July 2012.
- [RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", [RFC 7252](#), June 2014.
- [RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", [BCP 195](#), [RFC 7525](#), May 2015.

[RFC7540] Belshe, M., Peon, R., and M. Thomson, "Hypertext Transfer Protocol Version 2 (HTTP/2)", [RFC 7540](#), May 2015.

Authors' Addresses

John Mattsson
Ericsson AB
SE-164 80 Stockholm
Sweden

Email: john.mattsson@ericsson.com

Daniel Migault
Ericsson
8400 boulevard Decarie
Montreal, QC H4P 2N2
Canada

Phone: +1 514-452-2160
Email: daniel.migault@ericsson.com