Internet Engineering Task Force (IETF)
Request for Comments: 8442
Category: Standards Track
ISSN: 2070-1721

J. Mattsson
D. Migault
Ericsson

September 2018

ECDHE_PSK with AES-GCM and AES-CCM Cipher Suites for TLS 1.2 and DTLS 1.2

Abstract

This document defines several new cipher suites for version 1.2 of the Transport Layer Security (TLS) protocol and version 1.2 of the Datagram Transport Layer Security (DTLS) protocol. These cipher suites are 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 forward secrecy, and AES-GCM and AES-CCM provide encryption and integrity protection.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8442.

Table of Contents

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). The cipher suites are defined for version 1.2 of the Transport Layer Security (TLS) protocol [RFC5246] and version 1.2 of the Datagram Transport Layer Security (DTLS) protocol [RFC6347].

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 and/or 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 the Constrained Application Protocol (CoAP) [RFC7252].

AEAD algorithms that combine encryption and integrity protection are strongly recommended for (D)TLS [RFC7525], and TLS 1.3 [RFC8446] forbids the use of non-AEAD algorithms. The AEAD algorithms considered in this document are AES-GCM and AES-CCM. The use of AES-GCM in TLS is defined in [RFC5288], and the use of AES-CCM is defined in [RFC6655].

[RFC4279] defines PSK cipher suites for TLS but does not consider elliptic curve cryptography. [RFC8422] 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. Requirements Notation

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

The cipher suites defined in this document are based on the following AES-GCM and AES-CCM AEAD algorithms: AEAD_AES_128_GCM [RFC5116], AEAD_AES_256_GCM [RFC5116], AEAD_AES_128_CCM [RFC5116], and AEAD_AES_128_CCM_8 [RFC6655].

Messages and premaster secret construction in this document are defined in [RFC5489]. The ServerKeyExchange and ClientKeyExchange messages are used, and the premaster secret is computed as for the ECDHE_PSK key exchange. The elliptic curve parameters used in the Diffie-Hellman parameters are negotiated using extensions defined in [RFC8422].

For TLS 1.2 and DTLS 1.2, the following cipher suites are defined:

```
TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256   = {0xD0,0x01}
TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384   = {0xD0,0x02}
TLS_ECDHE_PSK_WITH_AES_128_CCM_8_SHA256 = {0xD0,0x03}
TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256   = {0xD0,0x05}
```

The assigned code points can only be used for TLS 1.2 and DTLS 1.2.

The cipher suites defined in this document MUST NOT be negotiated for any version of (D)TLS other than version 1.2. Servers MUST NOT select one of these cipher suites when selecting a (D)TLS version other than version 1.2. A client MUST treat the selection of these cipher suites in combination with a different version of (D)TLS as an error and generate a fatal 'illegal_parameter' TLS alert.

Cipher suites TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_AES_128_CCM_8_SHA256, and TLS_AES_128_CCM_SHA256 are used to support equivalent functionality in TLS 1.3 [RFC8446].

4. IANA Considerations

This document defines the following new cipher suites for TLS 1.2 and DTLS 1.2. The values have been assigned in the "TLS Cipher Suites" registry defined by [RFC8446] and [RFC8447].

Value	Description	DTLS-OK	Recommended
{0xD0,0x01}	TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256	Y	Y
{0xD0,0x02}	TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384	Y	Y
{0xD0,0x03}	TLS_ECDHE_PSK_WITH_AES_128_CCM_8_SHA256	Y	N
{0xD0,0x05}	TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256	Y	Y

5. Security Considerations

The security considerations in TLS 1.2 [RFC5246], DTLS 1.2 [RFC6347], PSK Ciphersuites for TLS [RFC4279], ECDHE_PSK [RFC5489], AES-GCM [RFC5288], and AES-CCM [RFC6655] apply to this document as well.

All the cipher suites defined in this document provide confidentiality, mutual authentication, and forward secrecy. The AES-128 cipher suites provide 128-bit security, and the AES-256 cipher suites provide at least 192-bit security. However, AES_128_CCM_8 only provides 64-bit security against message forgery.

The pre-shared keys used for authentication MUST have a security level equal to or higher than the cipher suite used, i.e., at least 128-bit security for the AES-128 cipher suites and at least 192-bit security for the AES-256 cipher suites.

GCM or CCM encryption that reuses a nonce with a same key undermines the security of GCM and CCM. As a result, GCM and CCM MUST only be used with a system guaranteeing nonce uniqueness [RFC5116].

6. References

6.1. 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>.

[RFC4279] Eronen, P., Ed. and H. Tschofenig, Ed., "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279, DOI 10.17487/RFC4279, December 2005, <https://www.rfc-editor.org/info/rfc4279>.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, DOI 10.17487/RFC5116, January 2008, <https://www.rfc-editor.org/info/rfc5116>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[RFC5288] Salowey, J., Choudhury, A., and D. McGrew, "AES Galois Counter Mode (GCM) Cipher Suites for TLS", RFC 5288, DOI 10.17487/RFC5288, August 2008, <https://www.rfc-editor.org/info/rfc5288>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <https://www.rfc-editor.org/info/rfc6347>.

[RFC6655] McGrew, D. and D. Bailey, "AES-CCM Cipher Suites for Transport Layer Security (TLS)", RFC 6655, DOI 10.17487/RFC6655, July 2012, <https://www.rfc-editor.org/info/rfc6655>.

[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>.

6.2. Informative References

[RFC5487] Badra, M., "Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode", RFC 5487, DOI 10.17487/RFC5487, March 2009, <https://www.rfc-editor.org/info/rfc5487>.

[RFC5489] Badra, M. and I. Hajjeh, "ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)", RFC 5489, DOI 10.17487/RFC5489, March 2009, <https://www.rfc-editor.org/info/rfc5489>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/info/rfc7252>.

[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, DOI 10.17487/RFC7525, May 2015, <https://www.rfc-editor.org/info/rfc7525>.

[RFC7540] Belshe, M., Peon, R., and M. Thomson, Ed., "Hypertext Transfer Protocol Version 2 (HTTP/2)", RFC 7540, DOI 10.17487/RFC7540, May 2015, <https://www.rfc-editor.org/info/rfc7540>.

[RFC8447] Salowey, J. and S. Turner, "IANA Registry Updates for TLS and DTLS", RFC 8447, DOI 10.17487/RFC8447, August 2018, <https://www.rfc-editor.org/info/rfc8447>.

Acknowledgements

The authors would like to thank Ilari Liusvaara, Eric Rescorla, Dan Harkins, Russ Housley, Dan Harkins, Martin Thomson, Nikos Mavrogiannopoulos, Peter Dettman, Xiaoyin Liu, Joseph Salowey, Sean Turner, Dave Garrett, Martin Rex, and Kathleen Moriarty for their valuable comments and feedback.

Authors' Addresses

John Mattsson
Ericsson AB
SE-164 80 Stockholm
Sweden

Phone: +46 76 115 35 01
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