Workgroup: Transport Layer Security
Internet-Draft:
draft-mattsson-tls-psk-ke-dont-dont-dont-05
Published: 19 January 2023
Intended Status: Standards Track
Expires: 23 July 2023
Authors: J. Preuß Mattsson
Ericsson

NULL Encryption and Key Exchange Without Forward Secrecy are Discouraged

Abstract

Massive pervasive monitoring attacks using key exfiltration and made possible by key exchange without forward secrecy have been reported. If key exchange without Diffie-Hellman is used, static exfiltration of the long-term authentication keys enables passive attackers to compromise all past and future connections. Malicious actors can get access to long-term keys in different ways: physical attacks, hacking, social engineering attacks, espionage, or by simply demanding access to keying material with or without a court order. Exfiltration attacks are a major cybersecurity threat. If NULL encryption is used an on-path attacker can read all application data. The use of psk_ke and NULL encryption are not following zero trust principles of minimizing the impact of breach and governments have already made deadlines for their deprecation. This document evaluates TLS pre-shared key exchange modes, (EC)DHE groups, signature algorithms, and cipher suites and downgrades many entries to "N" and "D" where "D" indicates that the entries are "Discouraged".

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://emanjon.github.io/draft-mattsson-tls-psk-ke-dont-dont-dont/draft-mattsson-tls-psk-ke-dont-dont-dont.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-mattsson-tls-psk-ke-dont-dont-dont/.

Discussion of this document takes place on the Transport Layer Security Working Group mailing list (mailto:tls@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/tls/. Subscribe at https://www.ietf.org/mailman/listinfo/tls/.

Source for this draft and an issue tracker can be found at https://github.com/emanjon/draft-mattsson-tls-psk-ke-dont-dont-dont.

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 23 July 2023.

Copyright Notice

Copyright (c) 2023 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 (https://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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

[RFC8447] added a Recommended column to many of the TLS registries. The Recommended column did originally non-normatively indicate parameters that are generally recommended for implementations to support. The meaning of the column was changed by [I-D.ietf-tls-rfc8447bis] to indicate that the IETF has consensus that the item is RECOMMENDED, i.e., using normative [RFC2119] language. [I-D.ietf-tls-rfc8447bis] also introduced a third value "D" indicating that an item is discouraged and SHOULD NOT or MUST NOT be used. This means that all current values need to be reevaluated. The current values also need to be reevaluated as attacks, government requirements, and best practices have changed in the more than 4 years since [RFC8446] and [RFC8447] were published.

This document evaluates TLS pre-shared key exchange modes, (EC)DHE groups, signature algorithms, and cipher suites and downgrades many entries to "N" and "D" where "D" indicates that the entries are "Discouraged". While TLS 1.2 is obsolete [RFC8446] and two NIST compatible [NIST-TLS] implementations will therefore never negotiate TLS 1.2 after January 1, 2024, DTLS 1.3 [RFC9147] was recently published. DTLS 1.2 will therefore continue to be allowed for several years and a distinction between recommended and discouraged parameters is warranted.

1.1. Terminology

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.

2. Key Exchange Without Forward Secrecy

Key exchange without forward secrecy enables passive monitoring [RFC7258]. Massive pervasive monitoring attacks using key exfiltration and made possible by key exchange without forward secrecy have been reported [Heist], and many more have likely happened without ever being reported. If key exchange without Diffie-Hellman is used, access to the long-term authentication keys enables passive attackers to compromise all past and future connections. Malicious actors can get access to long-term keys in different ways: physical attacks, hacking, social engineering attacks, espionage, or by simply demanding access to keying material with or without a court order. Exfiltration attacks are a major cybersecurity threat [Exfiltration].

All cipher suites without forward secrecy have been marked as NOT RECOMMENDED in TLS 1.2 [I-D.ietf-tls-rfc8447bis], and static RSA and DH are forbidden in TLS 1.3 [RFC8446]. A large number of TLS profiles and implementations forbid the use of key exchange without Diffie-Hellman.

- ANSSI states that for all versions of TLS: "The perfect forward secrecy property must be ensured" [ANSSI-TLS].

- The general 3GPP TLS 1.2 profile follows [RFC9113] and states: "Only cipher suites with AEAD (e.g., GCM) and PFS (e.g. ECDHE, DHE) shall be supported" [TS.33.210].

- BoringSSL has chosen to not implement psk_ke, so that TLS 1.3 resumption always incorporates fresh key material [BoringSSL].

Unfortunately, TLS 1.3 allows key exchange without forward secrecy in both full handshakes and resumption handshakes with the psk_ke. As stated in [RFC8446], psk_ke does not fulfill one of the fundamental TLS 1.3 security properties, namely "Forward secret with respect to long-term keys". When the PSK is a group key, which is now formally allowed in TLS 1.3 [RFC9257], psk_ke fails yet another one of the fundamental TLS 1.3 security properties, namely "Secrecy of the session keys" [Akhmetzyanova] [RFC9257]. PSK authentication has yet another big inherent weakness as it often does not provide "Protection of endpoint identities". It could be argued that PSK authentication should be not recommended solely based on this significant privacy weakness. The 3GPP radio access network that to a large degree relies on PSK are fixing the vulnerabilities by augmenting PSK with ECIES and ECDHE, see Annex C of [TS.33.501] and [I-D.ietf-emu-aka-pfs].

Together with ffdhe2048 and rsa_pkcs1, psk_ke is one of the bad apples in the standards track TLS 1.3 fruit basket. Organizations like BSI [BSI] has already produced recommendations regarding its deprecation.

- BSI states regarding psk_ke that "This mode should only be used in special applications after consultation of an expert." and has set a deadline that use is only allowed until 2026.

Two essential zero trust principles are to assume that breach is inevitable or has likely already occurred [NSA-ZT], and to minimize impact when breach occur [NIST-ZT]. One type of breach is key compromise or key exfiltration. Different types of exfiltration are defined and discussed in [RFC7624]. Static exfiltration where the keys are transferred once has a lower risk profile than dynamic exfiltration where keying material or content is transferred to the attacker frequently. Forcing an attacker to do dynamic exfiltration

minimizes the impact of breach and should be considered best practice. This significantly increases the risk of discovery for the attacker.

One way to force an attacker to do dynamic exfiltration is to frequently rerun ephemeral Diffie-Hellman. For IPsec, ANSSI [ANSSI-PFS] recommends enforcing periodic rekeying with ephemeral Diffie-Hellman, e.g., every hour and every 100 GB of data, in order to limit the impact of a key compromise. This should be considered best practice for all protocols and systems. The Double Ratchet Algorithm in the Signal protocol [Signal] enables very frequent use of ephemeral Diffie-Hellman. The practice of frequently rerunning ephemeral Diffie-Hellman follows directly from the two zero trust principles mentioned above.

In TLS 1.3, the application_traffic_secret can be rekeyed using key_update, a resumption handshake, or a full handshake. The term forward secrecy is not very specific, and it is often better to talk about the property that compromise of key A does not lead to compromise of key B. Figure 1 illustrates the impact of some examples of static key exfiltration when psk_ke, key_update, and (ec)dhe are used for rekeying. Each time period T_i uses a single application_traffic_secret. ✘ means that the attacker has access to the application_traffic_secret in that time period and can passively eavesdrop on the communication. ✔ means that the attacker does not have access to the application_traffic_secret. Exfiltration and frequently rerunning EC(DHE) is discussed in Appendix F of [I-D.ietf-tls-rfc8446bis].

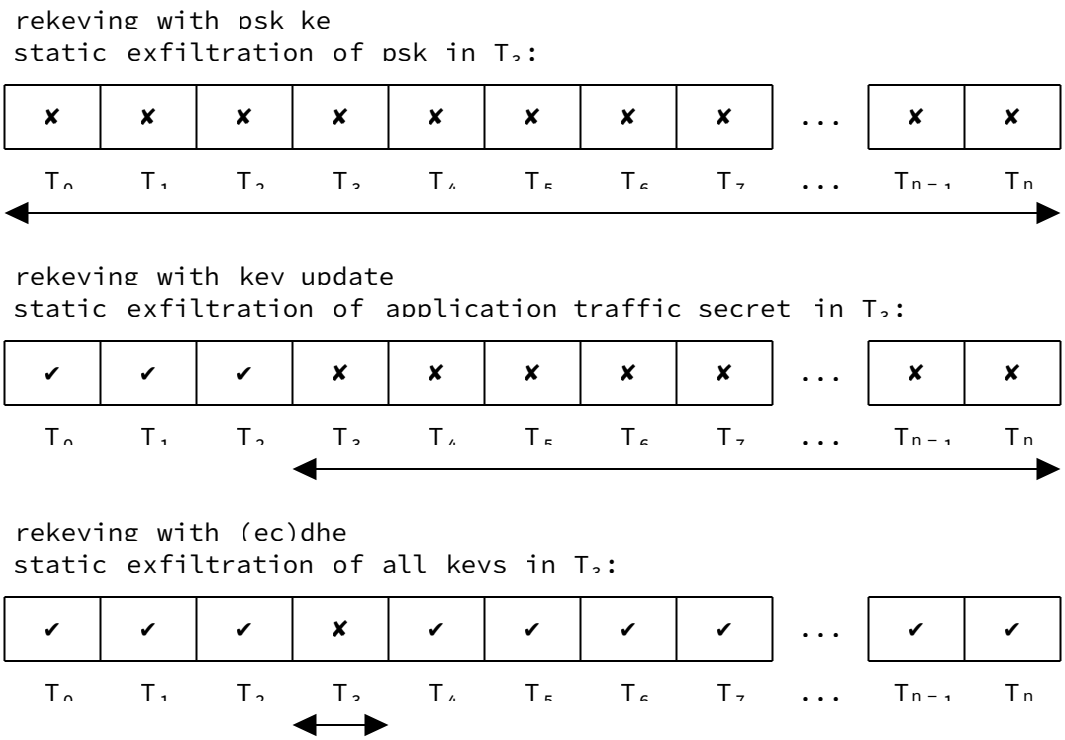

Figure 1: Impact of static key exfiltration in time period T3 when psk_ke, key_update, and (ec)dhe are used.

Modern ephemeral key exchange algorithms like x25519 [RFC7748] are very fast and have small message overhead. The public keys are 32 bytes long and the cryptographic operations take 53 microseconds per endpoint on a single core AMD Ryzen 5 5560U [eBACS-DH]. Ephemeral key exchange with the quantum-resistant algorithm Kyber that NIST will standardize is even faster. For the current non-standardized version of Kyber512 the cryptographic operations take 12 microseconds for the client and 8 microseconds for the server [eBACS-KEM].

Unfortunately, psk_ke is marked as "Recommended" in the IANA PskKeyExchangeMode registry. This may severely weaken security in deployments following the "Recommended" column. Introducing TLS 1.3 in 3GPP had the unfortunate and surprising effect of drastically lowering the minimum security when TLS is used with PSK authentication. Some companies in 3GPP have been unwilling to mark psk_ke as not recommended as it is so clearly marked as "Recommended" by the IETF. By labeling psk_ke as "Recommended", IETF is legitimizing and implicitly promoting bad security practice.

This document sets the "Recommended" value of psk_ke to "D" indicating that it is "Discouraged".

[RFC9113] describes and classifies prohibited TLS 1.2 cipher suites without forward secrecy. This document sets the "Recommended" value of all cipher suites listed in Appendix A of [RFC9113] as well as TLS_PSK_WITH_CHACHA20_POLY1305_SHA256 to "D" indicating that they are "Discouraged".

3. Cipher Suites with NULL Encryption

Cipher suites with NULL encryption enables passive monitoring [RFC7258] and were completely removed from TLS 1.3 [RFC8446]. Unfortunately, the independent stream document [RFC9150] reintroduced cipher suites with NULL Encryption in TLS 1.3 even though NULL encryption violates several of the fundamental TLS 1.3 security properties, namely "Protection of endpoint identities", "Confidentiality", and "Length concealment". Some companies in 3GPP have already suggested to use [RFC9150] in QUIC but luckily this is forbidden by [RFC9001] and hopefully it will stay like that.

Modern encryption algorithms like AES-GCM [RFC5288] are very fast and have small message overhead. Upcoming algorithms like AEGIS [I-D.irtf-cfrg-aegis-aead] is much faster than AES-GCM [AEGIS-PERF]. NULL encryption has no raison d'être in two-party protocols.

Two essential zero trust principles are to assume that breach is inevitable or has likely already occurred [NSA-ZT], and to minimize impact when breach occur [NIST-ZT]. One type of breach is an on-path attacker present on the enterprise network. In [NIST-ZT2], NIST states as the first basic assumption for network connectivity for any organization that utilizes zero trust is that:

* "The entire enterprise private network is not considered an implicit trust zone. Assets should always act as if an attacker is present on the enterprise network, and communication should be done in the most secure manner available. This entails actions such as authenticating all connections and encrypting all traffic."

This document sets the "Recommended" value of TLS_SHA256_SHA256 and TLS_SHA384_SHA384 to "D" indicating that they are "Discouraged".

4. Obsolete Key Exchange

Government organizations like NIST, ANSSI, BSI, and NSA have already produced recommendations regarding the deprecation of key exchange algorithms with less than 128-bit security such as ffdhe2048. NIST [NIST-Lifetime] and ANSSI [ANSSI-TLS] only allow 2048-bit Finite Field Diffie-Hellman if the application data does not have to be protected after 2030. If the application data had a security life of ten years, NIST and ANSSI allowed use of ffdhe2048 until December 31, 2020. BSI [BSI] allowed use of ffdhe2048 up to the year 2022.

The Commercial National Security Algorithm Suite (CNSA) [RFC9151] forbids the use of ffdhe2048. ECDHE groups that offer less than 128-bit security are forbidden to use in TLS 1.3. This document sets the "Recommended" value of ffdhe2048, secp160k1, secp160r1, secp160r2, sect163k1, sect163r1, sect163r2, secp192k1, secp192r1, sect193r1, sect193r2, secp224k1, secp224r1m sect233k1, sect233r1, and sect239k1 to "D" indicating that they are "Discouraged".

[I-D.ietf-tls-deprecate-obsolete-kex] describes and classifies cipher suites with obsolete key exchange methods in TLS 1.2 but does not downgrade the "Recommended" value. This document sets the "Recommended" value of all cipher suites listed in Appendix A of [I-D.ietf-tls-deprecate-obsolete-kex] to "D" indicating that they are "Discouraged".

5. Signature Algorithms with PKCS #1 v1.5 Padding or SHA-1

Recommendations regarding RSASSA-PKCS1-v1_5 in certificates varies. The RSA Cryptography Specifications [RFC8017] specifies that "RSASSA-PSS is REQUIRED in new applications. RSASSA-PKCS1-v1_5 is included only for compatibility with existing applications.". BSI [BSI] allows use of the PKCS #1 v1.5 padding scheme in certificates up to the year 2025. The Commercial National Security Algorithm (CNSA) [RFC9151] requires offer of rsa_pkcs1_sha384 in certificates. This document sets the "Recommended" value of rsa_pkcs1_sha256, rsa_pkcs1_sha384, and rsa_pkcs1_sha512 to "N".

[RFC8446] forbids the use of RSASSA-PKCS1-v1_5 in signed TLS handshake messages. [I-D.davidben-tls13-pkcs1] registered new RSASSA-PKCS1-v1_5 signature algorithms for use in signed TLS 1.3 handshake messages. This document sets the "Recommended" value of rsa_pkcs1_sha256_legacy, rsa_pkcs1_sha384_legacy, and rsa_pkcs1_sha512_legacy to "D" indicating that they are "Discouraged".

[RFC8446] labels rsa_pkcs1_sha1 and ecdsa_sha1 as legacy algorithms which are being deprecated and that endpoints SHOULD NOT or MUST NOT negotiate. This document sets the "Recommended" value of rsa_pkcs1_sha1 and ecdsa_sha1 to "D" indicating that they are "Discouraged".

6. IANA Considerations

6.1. TLS PskKeyExchangeMode

IANA is requested to update the TLS PskKeyExchangeMode registry under the Transport Layer Security (TLS) Parameters heading. For the following entry the "Recommended" value has been set to "D" indicating that the item is "Discouraged".

Description	Recommended
psk_ke	D

Table 1: Downgraded TLS PSK Key Exchange Modes

6.2. TLS Cipher Suites

IANA is requested to update the TLS Cipher Suites registry under the Transport Layer Security (TLS) Parameters heading. For all cipher suites listed in Appendix A of [RFC9113], all cipher suites listed in Appendix A of [I-D.ietf-tls-deprecate-obsolete-kex], and the following entries the "Recommended" value have been set to "D" indicating that the items are "Discouraged".

Description	Recommended
TLS_SHA256_SHA256	D
TLS_SHA384_SHA384	D
TLS_PSK_WITH_CHACHA20_POLY1305_SHA256	D

Table 2: Downgraded TLS Cipher Suites

6.3. TLS Supported Groups

IANA is requested to update the TLS Supported Groups registry under the Transport Layer Security (TLS) Parameters heading. For the following entries the "Recommended" value have been set to "D" indicating that the items are "Discouraged".

Description	Recommended
sect163k1	D
sect163r1	D
sect163r2	D
sect193r1	D
sect193r2	D
sect233k1	D
sect233r1	D
sect239k1	D
secp160k1	D
secp160r1	D
secp160r2	D
secp192k1	D
secp192r1	D
secp224k1	D
secp224r1	D
ffdhe2048	D

Table 3: Downgraded TLS Supported Groups

6.4. TLS SignatureScheme

IANA is requested to update the TLS SignatureScheme registry under the Transport Layer Security (TLS) Parameters heading. For the following entries the "Recommended" value have been set to "N" or "D" where "D" indicates that the items are "Discouraged".

Description	Recommended
rsa_pkcs1_sha1	D
ecdsa_sha1	D
rsa_pkcs1_sha256	N
rsa_pkcs1_sha256_legacy	D
rsa_pkcs1_sha384	N
rsa_pkcs1_sha384_legacy	D
rsa_pkcs1_sha512	N
rsa_pkcs1_sha512_legacy	D

Table 4: Downgraded TLS Signature Schemes

7. References

7.1. Normative References

[I-D.ietf-tls-deprecate-obsolete-kex] Bartle, C. and N. Aviram, "Deprecating Obsolete Key Exchange Methods in TLS", Work in Progress, Internet-Draft, draft-ietf-tls-deprecate-obsolete-kex-01, 11 December 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-deprecate-obsolete-kex-01>.

[I-D.ietf-tls-rfc8447bis] Salowey, J. A. and S. Turner, "IANA Registry Updates for TLS and DTLS", Work in Progress, Internet-Draft, draft-ietf-tls-rfc8447bis-02, 24 October 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8447bis-02>.

[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/rfc/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/rfc/rfc8174>.

[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/rfc/rfc8446>.

[RFC9113] Thomson, M., Ed. and C. Benfield, Ed., "HTTP/2", RFC 9113, DOI 10.17487/RFC9113, June 2022, <https://www.rfc-editor.org/rfc/rfc9113>.

[RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", RFC 9147, DOI 10.17487/RFC9147, April 2022, <https://www.rfc-editor.org/rfc/rfc9147>.

7.2. Informative References

[AEGIS-PERF] Frank Denis, "BoringSSL AEADs comparison", October 2022, <https://github.com/jedisct1/openssl-family-bench/blob/master/img/boring-aeads.png>.

[Akhmetzyanova] Akhmetzyanova, L., Alekseev, E., Smyshlyaeva, E., and A. Sokolov, "Continuing to reflect on TLS 1.3 with external PSK", April 2019, <https://eprint.iacr.org/2019/421.pdf>.

[ANSSI-PFS] Agence nationale de la sécurité des systèmes d'information, "Recommendations for securing networks with IPsec", August 2015, <https://www.ssi.gouv.fr/uploads/2015/09/NT_IPsec_EN.pdf>.

[ANSSI-TLS] Agence nationale de la sécurité des systèmes d'information, "Security Recommendations for TLS", January 2017, <https://www.ssi.gouv.fr/uploads/2017/02/security-recommendations-for-tls_v1.1.pdf>.

[BoringSSL] Google, "BoringSSL", January 2023, <https://boringssl.googlesource.com/boringssl/>.

[BSI] Bundesamt für Sicherheit in der Informationstechnik, "Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths Part 2 – Use of Transport Layer Security (TLS)", February 2022, <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-2.pdf>.

[eBACS-DH] eBACS: ECRYPT Benchmarking of Cryptographic Systems, "Measurements of public-key Diffie–Hellman secret-sharing systems, indexed by machine", January 2023, <https://bench.cr.yp.to/results-dh.html>.

[eBACS-KEM] eBACS: ECRYPT Benchmarking of Cryptographic Systems, "Measurements of key-encapsulation mechanisms, indexed by machine", January 2023, <https://bench.cr.yp.to/results-kem.html>.

[Exfiltration]
APNIC, "How to: Detect and prevent common data exfiltration attacks", March 2022, <https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/>.

[Heist] The Intercept, "How Spies Stole the Keys to the Encryption Castle", February 2015, <https://theintercept.com/2015/02/19/great-sim-heist/>.

[I-D.davidben-tls13-pkcs1]
Benjamin, D., "Legacy RSASSA-PKCS1-v1_5 codepoints for TLS 1.3", Work in Progress, Internet-Draft, draft-davidben-tls13-pkcs1-00, 29 July 2019, <https://datatracker.ietf.org/doc/html/draft-davidben-tls13-pkcs1-00>.

[I-D.ietf-emu-aka-pfs] Arkko, J., Norrman, K., Torvinen, V., and J. P. Mattsson, "Forward Secrecy for the Extensible Authentication Protocol Method for Authentication and Key Agreement (EAP-AKA' FS)", Work in Progress, Internet-Draft, draft-ietf-emu-aka-pfs-08, 23 October 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-emu-aka-pfs-08>.

[I-D.ietf-tls-rfc8446bis]
Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-rfc8446bis-05, 24 October 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8446bis-05>.

[I-D.irtf-cfrg-aegis-aead] Denis, F., Scotoni, F. E. R., and S. Lucas, "The AEGIS family of authenticated encryption algorithms", Work in Progress, Internet-Draft, draft-irtf-cfrg-aegis-aead-00, 5 August 2022, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-aegis-aead-00>.

[NIST-Lifetime] National Institute of Standards and Technology, "Recommendation for Key Management: Part 1 – General", May 2020, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf>.

[NIST-TLS] National Institute of Standards and Technology, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations", August 2019, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf>.

[NIST-ZT] National Institute of Standards and Technology, "Implementing a Zero Trust Architecture", December 2022, <https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35b-preliminary-draft-2.pdf>.

[NIST-ZT2] National Institute of Standards and Technology, "Zero Trust Architecture", August 2020, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>.

[NSA-ZT] National Security Agency, "Embracing a Zero Trust Security Model", February 2021, <https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF>.

[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/rfc/rfc5288>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/rfc/rfc7258>.

[RFC7624] Barnes, R., Schneier, B., Jennings, C., Hardie, T., Trammell, B., Huitema, C., and D. Borkmann, "Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement", RFC 7624, DOI 10.17487/RFC7624, August 2015, <https://www.rfc-editor.org/rfc/rfc7624>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/rfc/rfc7748>.

[RFC8017] Moriarty, K., Ed., Kaliski, B., Jonsson, J., and A. Rusch, "PKCS #1: RSA Cryptography Specifications Version

2.2", RFC 8017, DOI 10.17487/RFC8017, November 2016, <https://www.rfc-editor.org/rfc/rfc8017>.

[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/rfc/rfc8447>.

[RFC9001] Thomson, M., Ed. and S. Turner, Ed., "Using TLS to Secure QUIC", RFC 9001, DOI 10.17487/RFC9001, May 2021, <https://www.rfc-editor.org/rfc/rfc9001>.

[RFC9150] Cam-Winget, N. and J. Visoky, "TLS 1.3 Authentication and Integrity-Only Cipher Suites", RFC 9150, DOI 10.17487/RFC9150, April 2022, <https://www.rfc-editor.org/rfc/rfc9150>.

[RFC9151] Cooley, D., "Commercial National Security Algorithm (CNSA) Suite Profile for TLS and DTLS 1.2 and 1.3", RFC 9151, DOI 10.17487/RFC9151, April 2022, <https://www.rfc-editor.org/rfc/rfc9151>.

[RFC9257] Housley, R., Hoyland, J., Sethi, M., and C. A. Wood, "Guidance for External Pre-Shared Key (PSK) Usage in TLS", RFC 9257, DOI 10.17487/RFC9257, July 2022, <https://www.rfc-editor.org/rfc/rfc9257>.

[Signal] Signal, "The Double Ratchet Algorithm", November 2016, <https://signal.org/docs/specifications/doubleratchet/>.

[TS.33.210] 3GPP, "TS 33.210 Network Domain Security (NDS); IP network layer security", 3GPP TS 33.210 17.1.0 , September 2022, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2279>.

[TS.33.501] 3GPP, "TS 33.501 Security architecture and procedures for 5G System", 3GPP TS 33.501 18.0.0 , December 2022, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169>.

Acknowledgements

The authors want to thank Ari Keränen, Eric Rescorla, and Paul Wouters for their valuable comments and feedback.

Author's Address

John Preuß Mattsson
Ericsson AB
SE-164 80 Stockholm

Sweden

Email: john.mattsson@ericsson.com