Workgroup: Network Working Group
Internet-Draft:
draft-mattsson-tls-psk-ke-dont-dont-dont-02
Published: 30 December 2022
Intended Status: Informational
Expires: 3 July 2023
Authors: J. Preuß Mattsson
Ericsson

# Key Exchange Without Forward Secrecy is NOT RECOMMENDED

## Abstract

Massive pervasive monitoring attacks using key exfiltration and made possible by key exchange without forward secrecy has 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. The use of psk_ke is not following zero trust principles and governments have already made deadlines for its deprecation. This document updates the IANA PskKeyExchangeMode registry by setting the "Recommended" value for psk_ke to "N".

## About This Document

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

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 (tls) 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 will expire on 3 July 2023.

## Copyright Notice



## Table of Contents

1. Introduction
  1.1. Terminology
2. IANA Considerations
3. References
  3.1. Normative References
  3.2. Informative References
Acknowledgements
Author's Address

## 1. Introduction

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 has 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 has been marked as NOT RECOMMENDED in TLS 1.2 [RFC8447], and static RSA and DH are forbidden in TLS 1.3 [RFC8446]. A large number of TLS profiles forbid the use of key exchange without Diffie-Hellman [RFC9113] [ANSSI-TLS] [T3GPP.33.210].

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

* The general 3GPP TLS profile follows [RFC9113] and states: "Only cipher suites with AEAD (e.g., GCM) and PFS (e.g. ECDHE, DHE) shall be supported" [T3GPP.33.210].

Unfortunately TLS 1.3 allows key exchange without forward secrecy in both full handshakes and resumption handshakes with 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 [T3GPP.33.501] and [I-D.ietf-emu-aka-pfs].

Together with rsa_pkcs1, psk_ke is one of the bad apples in the 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 is 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 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 zero trust principles.

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].

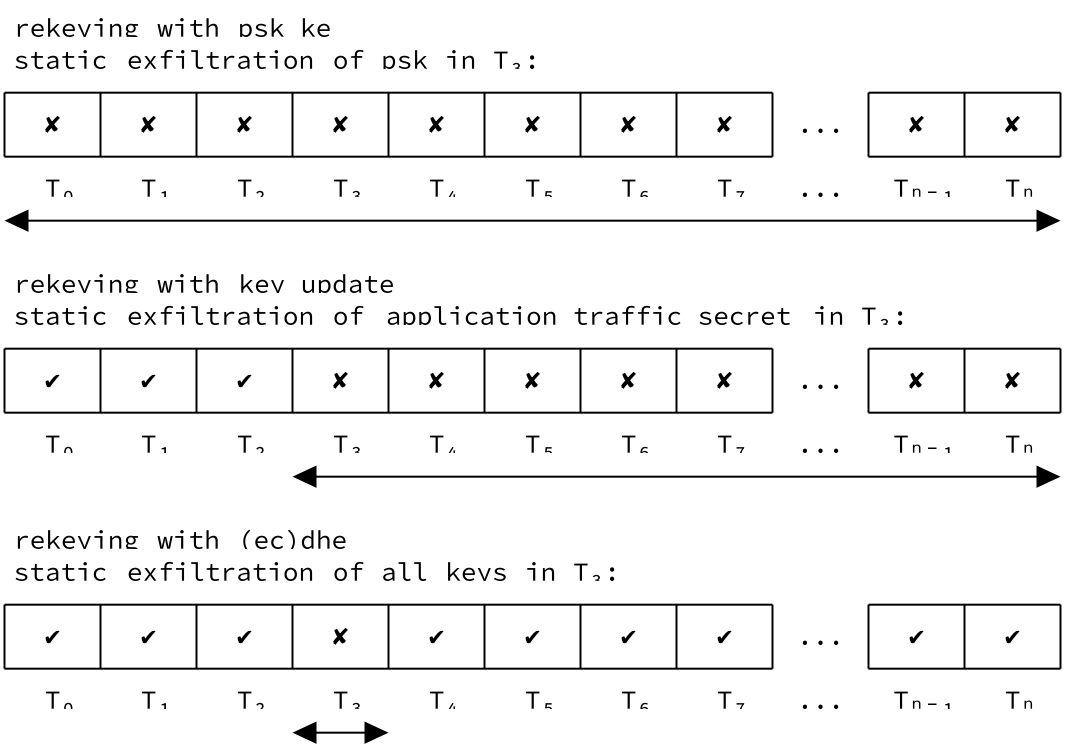

Figure 1: Impact of static key exfiltration in time period T3 when psk_ke, key_update, and (ec)dhe are used.

With modern algorithms like x25519 [RFC7748], ephemeral Diffie-Hellman introduces negligible overhead. The public keys are 32 bytes long and the operations takes 63 microseconds per endpoint on a single core AMD Ryzen 9 5950X [eBACS-DH]. Ephemeral key exchange with the quantum-restistant algorithm Kyber that NIST will standardize is even faster, especially for the TLS 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 updates the PskKeyExchangeMode registry under the Transport Layer Security (TLS) Parameters heading. For psk_ke the "Recommended" value has been set to "N".

### 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. IANA Considerations

IANA is requested to update the PskKeyExchangeMode registry under the Transport Layer Security (TLS) Parameters heading. For psk_ke the "Recommended" value has been set to "N".

## 3. References

### 3.1. 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>.

**[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>.

**[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>.

**[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>.

### 3.2. Informative References

**[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>.

**[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", December 2022, <https://bench.cr.yp.to/results-dh.html>.

**[eBACS-KEM]** eBACS: ECRYPT Benchmarking of Cryptographic Systems, "Measurements of key-encapsulation mechanisms, indexed by machine", December 2022, <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.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://www.ietf.org/archive/id/draft-ietf-emu-aka-pfs-08.txt>.

**[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://www.ietf.org/archive/id/draft-ietf-tls-rfc8446bis-05.txt>.

**[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>.

**[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>.

**[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/info/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/info/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/info/rfc7748>.

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

**[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/info/rfc9257>.

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

**[T3GPP.33.210]** 3GPP, "TS 33.210 Network Domain Security (NDS); IP network layer security", September 2022, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2279>.

**[T3GPP.33.501]** 3GPP, "TS 33.501 Security architecture and procedures for 5G System", September 2022, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169>.

## Acknowledgements

The authors want to thank Ari Keränen for his valuable comments and feedback.

## Author's Address

John Preuß Mattsson
Ericsson AB
SE-164 80 Stockholm
Sweden

Email: john.mattsson@ericsson.com