EAP Method Update
Internet-Draft
Intended status: Standards Track
Expires: 23 January 2026

T. Reddy
Nokia

22 July 2025

Post-Quantum Enhancements to EAP-TLS and EAP-TTLS
draft-reddy-emu-pqc-eap-tls-01

Abstract

This document proposes enhancements to the Extensible Authentication Protocol with Transport Layer Security (EAP-TLS) and EAP Tunneled TLS (EAP-TTLS) to incorporate post-quantum cryptographic mechanisms. It also addresses challenges related to large certificate sizes and long certificate chains, as identified in RFC9191, and provides recommendations for integrating PQC algorithms into EAP-TLS and EAP-TTLS deployments.

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-reddy-emu-pqc-eap-tls/.

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

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 January 2026.

Table of Contents

1. Introduction

The emergence of a Cryptographically Relevant Quantum Computer (CRQC) would break the mathematical assumptions that underpins widely deployed public-key algorithms, rendering them insecure and obsolete. As a result, there is an urgent need to update protocols and infrastructure with post-quantum cryptographic (PQC) algorithms designed to resist attacks from both quantum and classical adversaries. The cryptographic primitives requiring replacement are discussed in [I-D.ietf-pquip-pqc-engineers], and the NIST PQC Standardization process has initially selected algorithms such as ML-KEM, SLH-DSA, and ML-DSA for usage in security protocols.

To mitigate the risks posed by a CRQC, such as the potential compromise of encrypted data and the forging of digital signatures, existing security protocols must be upgraded to support PQC. These risks include "Harvest Now, Decrypt Later" (HNDL) attack, where adversaries capture encrypted traffic today with the intent to decrypt it once CRQCs become available. Protocols such as EAP-TLS and EAP-TTLS are widely used for network access authentication in

Enterprise and Wireless environments. To continue providing long-term confidentiality and authentication guarantees, EAP-TLS and EAP-TTLS must evolve to incorporate post-quantum algorithms.

However, transitioning these protocols to support PQC introduces practical challenges. [RFC9191] highlights issues related to large certificates and certificate chains in EAP-TLS, which can lead to session failures due to round-trip limitations. PQC certificates and certificate chains tend to be significantly larger than their traditional counterparts, further exacerbating these issues by increasing TLS handshake sizes and the likelihood of session failures. To address these challenges, this draft proposes mitigation strategies that enable the use of PQC within EAP-TLS and EAP-TTLS, ensuring secure and efficient authentication even in constrained network environments.

2. Conventions and Definitions

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.

This document adopts terminology defined in [I-D.ietf-pquip-pqt-hybrid-terminology]. For the purposes of this document, it is useful to categorize cryptographic algorithms into three distinct classes:

* Traditional Algorithm: An asymmetric cryptographic algorithm based on integer factorization, finite field discrete logarithms, or elliptic curve discrete logarithms. In the context of TLS, an example of a traditional key exchange algorithm is Elliptic Curve Diffie-Hellman (ECDH), which is almost exclusively used in its ephemeral mode, referred to as Elliptic Curve Diffie-Hellman Ephemeral (ECDHE).

* Post-Quantum Algorithm: An asymmetric cryptographic algorithm designed to be secure against attacks from both quantum and classical computers. An example of a post-quantum key exchange algorithm is the Module-Lattice Key Encapsulation Mechanism (ML-KEM).

* Hybrid Algorithm: We distinguish between key exchanges and signature algorithms:

- Hybrid Key Exchange: A key exchange mechanism that combines two component algorithms - one traditional algorithm and one post-quantum algorithm. The resulting shared secret remains secure as long as at least one of the component key exchange algorithms remains unbroken.

- PQ/T Hybrid Digital Signature: A multi-algorithm digital signature scheme composed of two or more component signature algorithms, where at least one is a post-quantum algorithm and at least one is a traditional algorithm.

Digital signature algorithms play a critical role in X.509 certificates, Certificate Transparency Signed Certificate Timestamps, Online Certificate Status Protocol (OCSP) statements, and any other mechanism that contributes signatures during a TLS handshake or in context of a secure communication establishment.

3. Data Confidentiality in EAP-TLS

One of the primary threats to EAP-TLS and EAP-TTLS is the HNDL attack. In this scenario, adversaries can passively capture EAP-TLS handshakes such as those transmitted over the air in Wi-Fi networks and store them for future decryption once CRQCs become available.

While EAP-TLS 1.3 [RFC9190] was designed to provide strong forward secrecy and protect user privacy by encrypting client identity and reducing exposure of session metadata, HNDL attacks effectively nullify these protections. If the handshake is not quantum-resistant, a future CRQC could retroactively decrypt session traffic, revealing:

* The identity of the authenticated client.

* Client credentials used in certificate-based authentication (e.g., usernames, device or organization identifiers).

To preserve the intended privacy guarantees of TLS 1.3 and protect against HNDL, EAP-TLS and EAP-TTLS deployments MUST adopt post-quantum key exchange mechanisms, as outlined in Section 4 of [I-D.reddy-uta-pqc-app]. These mechanisms ensure that even if handshake data is recorded today, it cannot be decrypted in the future, maintaining the confidentiality and privacy of the TLS session.

Furthermore, to support hybrid or PQC-only key exchange in bandwidth or latency-constrained EAP deployments, EAP clients and servers should apply the optimizations described in Section 4.1 of [I-D.reddy-uta-pqc-app] to minimize performance overhead.

4. Post-Quantum Authentication in EAP-TLS

Although CRQCs could eventually decrypt recorded TLS sessions to recover derived keys and access confidential data, they cannot retroactively compromise client or server authentication if the attacker did not possess the corresponding private key at the time of the handshake. However, EAP-TLS and EAP-TTLS deployments rely on X.509 certificates issued by certificate authorities (CAs), and the transition to post-quantum (PQ) authentication is constrained by the long lifecycle involved to distribute, deploy, and validate new trust anchors. If CRQCs arrive sooner than anticipated, authentication systems may lack the agility to adapt in time.

This makes PQC authentication a critical requirement for EAP-TLS and EAP-TTLS deployments deployments. An on-path attacker equipped with a CRQC could compute a server’s private key before the certificate expires, enabling real-time impersonation of access points (APs). This could deceive users into revealing credentials or connecting to rogue networks, leading to privacy violations and potential client credential theft.

To mitigate these risks, EAP-TLS and EAP-TTLS deployments MUST adopt either pure PQ or PQ/T certificate-based authentication, as described in Section 5 of [I-D.reddy-uta-pqc-app].

A composite certificate contains both a traditional public key algorithm (e.g., ECDSA) and a post-quantum algorithm (e.g., ML-DSA) within a single X.509 certificate. This design enables both algorithms to be used in parallel, the traditional component ensures compatibility with existing infrastructure, while the post-quantum component introduces resistance against future quantum attacks. This approach facilitates early adoption of PQC without requiring immediate disruption to established PKI deployments.

The use of post-quantum or hybrid certificates increases the size of individual certificates, certificate chains, and signatures, resulting in significantly larger handshake messages. These larger payloads can lead to packet fragmentation, retransmissions, and handshake delays, issues that are particularly disruptive in constrained or lossy network environments.

To address these impacts, EAP-TLS and EAP-TTLS deployments can apply certificate chain optimization techniques outlined in Section 6.1 of [I-D.reddy-uta-pqc-app] to reduce transmission overhead and improve handshake reliability.

5. EST Integration

The EAP-client is expected to validate the certificate presented by the EAP-server using a trust anchor that is provisioned out-of-band prior to authentication (e.g., using EST). The Intermediate certificates are provided by the EAP server during the EAP-TLS handshake. The EAP client relies solely on the pre-provisioned trust anchor to build and validate the certificate chain. This model assumes a managed deployment environment with explicitly configured trust relationships between the EAP-client and EAP-server.

To further reduce handshake overhead, particularly in deployments using large certificate chains due to post-quantum (PQ) or composite certificates, this draft proposes an optimization that leverages the Enrollment over Secure Transport (EST) protocol [RFC7030], extended by [RFC8295]. Specifically, it allows intermediate certificates to be retrieved in advance by using EST, thereby avoiding the need to transmit them during each EAP-TLS exchange.

This section defines extensions to EST to support retrieval of the certificate chain used by a EAP server and EAP clients. The first extension enables clients to obtain access to the complete set of published intermediate certificates of the EAP server.

A new path component is defined under the EST well-known URI:

GET /.well-known/est/eapservercertchain

The ’/eapservercertchain’ is intended for informational retrieval only and does not require client authentication. It allows clients to retrieve the intermediate certificate chain that the EAP server presents during TLS handshakes. This request is performed using the HTTPS protocol. The EST server MUST support requests without requiring client authentication. The certificate chain provided by the EST server MUST be the same certificate chain EAP server uses in a EAP-TLS or EAP-TTLS session.

The second extension enables EAP servers to obtain access to the complete set of published intermediate certificates of the EAP clients. Rather than relying on static configuration, the EAP server can dynamically fetch the client’s intermediate certificate chain from a trusted EST server within the same administrative domain.

A new path component is defined under the EST well-known URI:

GET /.well-known/est/eapclientcertchain

The ’/eapclientcertchain’ is intended for informational retrieval only and does not require client authentication. It allows EAP server to retrieve the intermediate certificate chain that the EAP clients present during TLS handshakes. This request is performed using the HTTPS protocol. The EST server MUST support requests without requiring client authentication. The certificate chain provided by the EST server MUST be the same certificate chain EAP clients use in the EAP-TLS or EAP-TTLS session.

EAP servers and clients are RECOMMENDED to cache retrieved certificate chains to reduce latency and network overhead. However, they SHOULD implement mechanisms to detect changes or expiration. These include periodic re-fetching, honoring HTTP cache control headers (e.g., Cache-Control, ETag), and verifying the validity period of intermediate certificates.

As an alternative, a device MAY attempt to retrieve the certificate chain from the EST server (e.g., /eapservercertchain or /eapclientcertchain) only when certificate validation fails during an EAP-TLS or EAP-TTLS handshake. While this on-demand retrieval can serve as a fallback to recover from outdated intermediate certificate, it has the drawback of delaying authentication.

After retrieving intermediate certificates via EST, a EAP client that believes it has a complete set of intermediate certificates to authenticate the EAP server sends the tls_flags extension as defined in [I-D.kampanakis-tls-scas-latest] with the 0xTBD1 flag set to 1 in its ClientHello message. Similarly, a EAP server that believes it has a complete set of intermediate certificates to authenticate the EAP client sends the same tls_flags extension with 0xTBD1 set to 1 in its CertificateRequest message. In both cases, only the end-entity certificates will be provided by the EAP client and server during the TLS handshake, relying on the recipient to possess or retrieve the necessary intermediate certificates for certificate chain validation.

6. Security Considerations

The security considerations outlined in [I-D.reddy-uta-pqc-app] and [I-D.ietf-pquip-pqc-engineers] must be carefully evaluated and taken into account for both EAP-TLS and EAP-TTLS deployments.

Acknowledgements

TBA.

References

Normative References

[I-D.reddy-uta-pqc-app]
Reddy.K, T. and H. Tschofenig, "Post-Quantum Cryptography Recommendations for TLS-based Applications", Work in Progress, Internet-Draft, draft-reddy-uta-pqc-app-08, 2 July 2025, <https://datatracker.ietf.org/doc/html/draft-reddy-uta-pqc-app-08>.

[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>.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, DOI 10.17487/RFC7030, October 2013, <https://www.rfc-editor.org/rfc/rfc7030>.

[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>.

[RFC8295] Turner, S., "EST (Enrollment over Secure Transport) Extensions", RFC 8295, DOI 10.17487/RFC8295, January 2018, <https://www.rfc-editor.org/rfc/rfc8295>.

[RFC9190] Preu Mattsson, J. and M. Sethi, "EAP-TLS 1.3: Using the Extensible Authentication Protocol with TLS 1.3", RFC 9190, DOI 10.17487/RFC9190, February 2022, <https://www.rfc-editor.org/rfc/rfc9190>.

Informative References

[I-D.ietf-pquip-pqc-engineers]
Banerjee, A., Reddy.K, T., Schoinianakis, D., Hollebeek, T., and M. Ounsworth, "Post-Quantum Cryptography for Engineers", Work in Progress, Internet-Draft, draft-ietf-pquip-pqc-engineers-13, 1 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-engineers-13>.

[I-D.ietf-pquip-pqt-hybrid-terminology]
D, F., P, M., and B. Hale, "Terminology for Post-Quantum Traditional Hybrid Schemes", Work in Progress, Internet-Draft, draft-ietf-pquip-pqt-hybrid-terminology-06, 10 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqt-hybrid-terminology-06>.

[I-D.kampanakis-tls-scas-latest]
Kampanakis, P., Bytheway, C., Westerbaan, B., and M. Thomson, "Suppressing CA Certificates in TLS 1.3", Work in Progress, Internet-Draft, draft-kampanakis-tls-scas-latest-03, 5 January 2023, <https://datatracker.ietf.org/doc/html/draft-kampanakis-tls-scas-latest-03>.

[RFC9191] Sethi, M., Preu Mattsson, J., and S. Turner, "Handling Large Certificates and Long Certificate Chains in TLS-Based EAP Methods", RFC 9191, DOI 10.17487/RFC9191, February 2022, <https://www.rfc-editor.org/rfc/rfc9191>.

Author’s Address

Tirumaleswar Reddy
Nokia
Bangalore
Karnataka
India
Email: k.tirumaleswar_reddy@nokia.com