EMU PQC for 802.1

Date: 2025-07-29

Authors:

Name	Affiliation	Address	Phone	Email
Peter Yee	NSA-CSD	Mountain View, CA 94043, USA		peter@akayla.com

EAP Method Update (EMU)

- **See https://datatracker.ietf.org/wg/emu/**
  - This working group has been chartered to provide updates to some commonly used Extensible Authentication Protocol methods including of EAP-TLS, EAP-AKA, EAP-AKA' (for 5G), EAP-SIM, etc.
  - The group should document any recently gained new knowledge on vulnerabilities or the possible implications of pervasive surveillance or other new concerns.
- **Updates**
  - New: Post-Quantum Key Encapsulation Mechanisms (PQ KEMs) in EAP-AKA prime: https://datatracker.ietf.org/doc/draft-ietf-emu-pqc-eapaka/ (July 2025)
  - New: Enhancing Security in EAP-AKA' with Hybrid Post-Quantum Cryptography: https://datatracker.ietf.org/doc/draft-ietf-emu-hybrid-pqc-eapaka/ (July 2025)
  - Not yet adopted: Post-Quantum Enhancements to EAP-TLS and EAP-TTLS: https://datatracker.ietf.org/doc/draft-reddy-emu-pqc-eap-tls/ (July 2025)

PQC for EAP-TLS and EAP-TTLS

- Presentation to the EMU WG at IETF 123: https://datatracker.ietf.org/meeting/123/materials/slides-123-emu-post-quantum-enhancements-to-eaptls-and-eapttls-00
- Builds on RFC 9191 (Handling Large Certificates and Long Certificate Chains in TLS-Based EAP Methods)
- Recommendations:
  - Mandate Hybrid/PQ for key exchange in EAP-TLS/TTLS
  - Mandate PQ or hybrid certificates for authentication
  - Use cert chain optimization to avoid fragmentation
- Leverages key exchange optimizations in draft-reddy-uta-pqc-app
- Modifies EST (RFC 7030) to support EAP client and server intermediate cert chain retrieval