Workgroup: EMU
Internet-Draft: draft-ar-emu-pqc-eapaka-00
Published: 4 March 2024
Intended Status: Standards Track
Expires: 5 September 2024
Authors: A. Banerjee T. Reddy
Nokia Nokia

Post-Quantum Cryptography enhancement in EAP-AKA prime

Abstract

Forward Secrecy for the Extensible Authentication Protocol Method for Authentication and Key Agreement (EAP-AKA' FS) is specified in [I-D.ietf-emu-aka-pfs], providing updates to [RFC9048] with an optional extension that offers ephemeral key exchange using the traditional Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) key agreement algorithm for achieving perfect forward secrecy (PFS). However, it is susceptible to future threats from Cryptographically Relevant Quantum Computers, which could potentially compromise a traditional ephemeral public key. If the adversary has also obtained knowledge of the long-term key and ephemeral public key, it could compromise session keys generated as part of the authentication run in EAP-AKA'.

This draft aims to enhance the security of EAP-AKA' FS making it quantum-safe.

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-ar-emu-pqc-eapaka/.

Discussion of this document takes place on the emu 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 5 September 2024.

Table of Contents

1. Introduction

Forward Secrecy for the Extensible Authentication Protocol Method for Authentication and Key Agreement (EAP-AKA' FS) defined in [I-D.ietf-emu-aka-pfs] updates the improved Extensible Authentication Protocol Method for 3GPP Mobile Network Authentication and Key Agreement (EAP-AKA') specified in [RFC9048], with an optional extension providing ephemeral key exchange. This prevents an attacker who has gained access to the long term key from

obtaining session keys established in the past, assuming these have been properly deleted. EAP-AKA' FS mitigates passive attacks (e.g., large scale pervasive monitoring) against future sessions.

Nevertheless, EAP-AKA' FS uses traditional algorithms public-key algorithms (e.g., ECDH) which will be broken by a Cryptographically Relevant Quantum Computer (CRQC) using Shor's algorithm. The presence of a CRQC would render state-of-the-art, traditional public-key algorithms deployed today obsolete and insecure, since the assumptions about the intractability of the mathematical problems for these algorithms that offer confident levels of security today no longer apply in the presence of a CRQC. A CRQC could recover the SHARED_SECRET from the ECDHE public keys (Section 6.3 of [I-D.ietf-emu-aka-pfs]). If the adversary has also obtained knowledge of the long-term key, it could then compute CK', IK', and the SHARED_SECRET, and any derived output keys. This means that the CRQC would disable the forward security capability provided by [I-D.ietf-emu-aka-pfs].

The migration to PQC is unique in the history of modern digital cryptography in that neither the traditional algorithms nor the post-quantum algorithms are fully trusted to protect data for the required data lifetimes. The post-quantum algorithms face uncertainty about the underlying mathematics, compliance issues, unknown vulnerabilities, hardware and software implementations that have not had sufficient maturing time to rule out classical cryptanalytic attacks and implementation bugs. During the transition from traditional to post-quantum algorithms, there is a desire or a requirement for protocols that use both algorithm types.

This specification defines Hybrid public-key encryption (HPKE) [RFC9180] for use with EAP-AKA' FS. HPKE offers a variant of public-key encryption of arbitrary-sized plaintexts for a recipient public key. HPKE works for any combination of an asymmetric key encapsulation mechanism (KEM), key derivation function (KDF), and authenticated encryption with additional data (AEAD) function. HPKE can be extended to support hybrid post-quantum Key Encapsulation Mechanisms (KEMs) as defined in [I-D.ietf-westerbaan-cfrg-hpke-xyber768d00].

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.

3. Terminology

This document makes use of the terms defined in [I-D.ietf-pquip-pqt-hybrid-terminology]. For the purposes of this document, it is helpful to be able to divide cryptographic algorithms into two classes:

"Traditional Algorithm": An asymmetric cryptographic algorithm based on integer factorisation, finite field discrete logarithms or elliptic curve discrete logarithms. In the context of JOSE, examples of traditional key exchange algorithms include Elliptic Curve Diffie-Hellman Ephemeral Static [RFC6090] [RFC8037]. In the context of COSE, examples of traditional key exchange algorithms include Ephemeral-Static (ES) DH and Static-Static (SS) DH [RFC9052].

"Post-Quantum Algorithm": An asymmetric cryptographic algorithm that is believed to be secure against attacks using quantum computers as well as classical computers. Examples of PQC key exchange algorithms include Kyber.

"Hybrid" key exchange, in this context, means the use of two key exchange algorithms based on different cryptographic assumptions, e.g., one traditional algorithm and one Post-Quantum algorithm, with the purpose of the final shared secret key being secure as long as at least one of the component key exchange algorithms remains unbroken. It is referred to as PQ/T Hybrid Scheme in [I-D.ietf-pquip-pqt-hybrid-terminology].

PQ/T Hybrid Key Encapsulation Mechanism: A Key Encapsulation mechanism (KEM) made up of two or more component KEM algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm.

4. Background on EAP-AKA' with perfect forward secrecy

In EAP-AKA', The authentication vector (AV) contains a random part RAND, an authenticator part AUTN used for authenticating the network to the USIM, an expected result part XRES, a 128-bit session key for integrity check IK, and a 128-bit session key for encryption CK.

As described in the draft [I-D.draft-ietf-emu-aka-pfs-11], the server has the EAP identity of the peer. The server asks the AD to run AKA algorithm to generate RAND, AUTN, XRES, CK and IK. Further it also derives CK’ and IK’ keys which are tied to a particular network name. The server now generates the ephemeral key pair and sends the public key of that key pair and the first EAP method message to the peer. In this EAP message, AT_PUB_ECDHE (carries public key) and the AT_KDF_FS(carries other FS related parameters). Both of these might be ignored of USIM doesn’t support the Forward Secrecy extension. The peer checks if it wants to have a Forward

extension in EAP AKA'. If yes, then it will eventually respond with AT_PUB_ECDHE and MAC. If not, it will ignore AT_PUB_ECDHE. If the peer wants to participate in FS extension, it will then generate its ECDH key pair, calculate a shared key based on its private key and server public key. The server will receive the RES from peer and AT_PUB_ECDHE. The shared key will be generated both in the peer and the server with key pairs exchanged, and later master key is also generated.

MK_ECDHE = PRF'(IK'| CK'|SHARED_SECRET,"EAP-AKA' FS"|Identity)

5. Hybrid Enhancements by Design

We suggest the following changes and enhancements:

*A new attribute, AT_PUB_HYBRID, is defined to carry the public key, which is the concatenation of traditional and PQC KEM public keys from the EAP server. The AT_PUB_HYBRID attribute will carry the encapsulated key, which is formed by concatenating the encapsulated key (enc) from the traditional KEM algorithm and the ciphertext (ct) from the PQC KEM Encapsulation function from the EAP peer.

*The AT_KDF_FS attribute is updated to indicate the HPKE KEM and HKDF for generating the Hybrid Master Key MK_HYBRID.

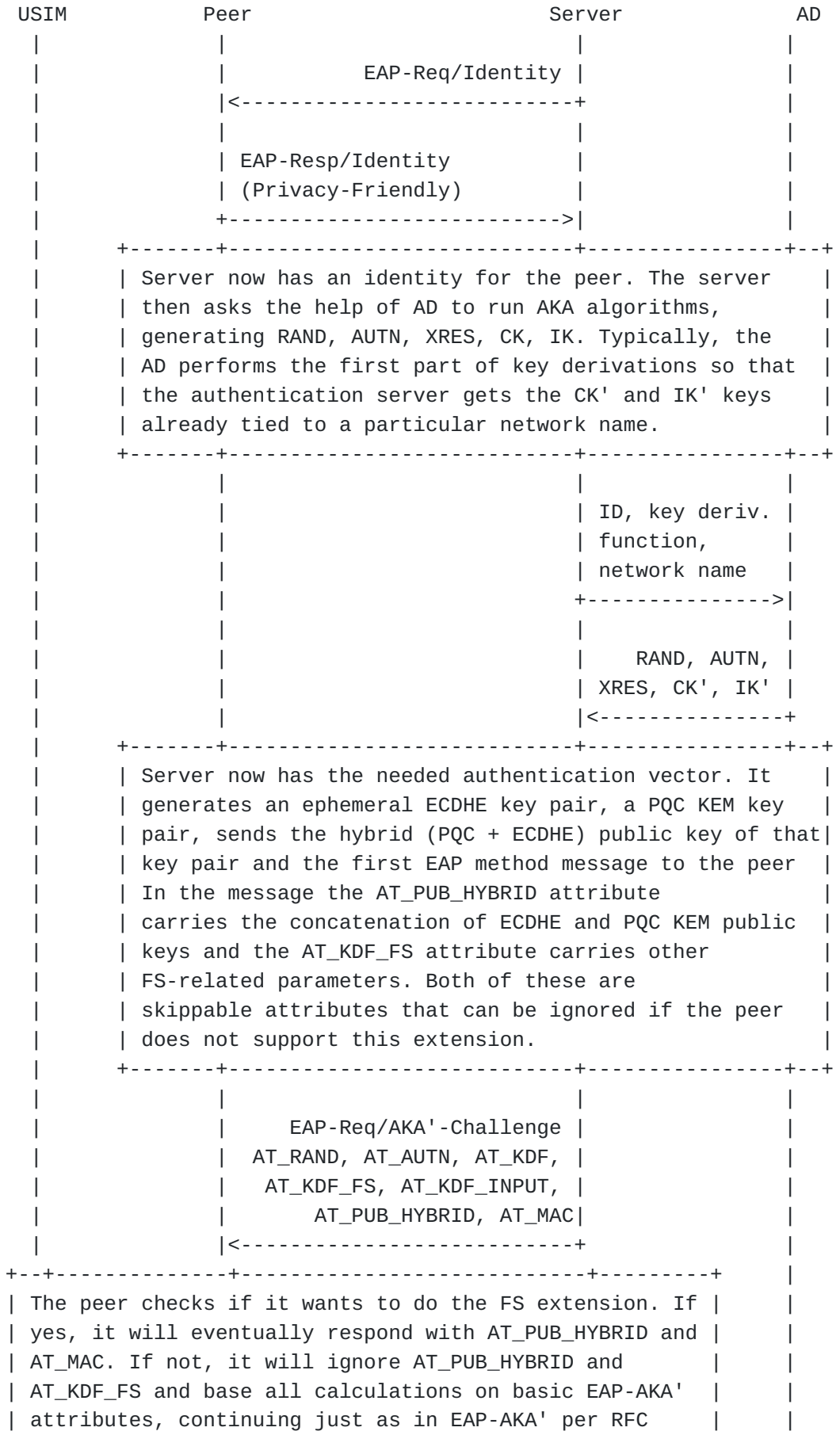
*Multiple AT_KDF_FS attributes is included in the EAP-Request to handle the EAP peer not supporting HPKE Hybrid KEM.

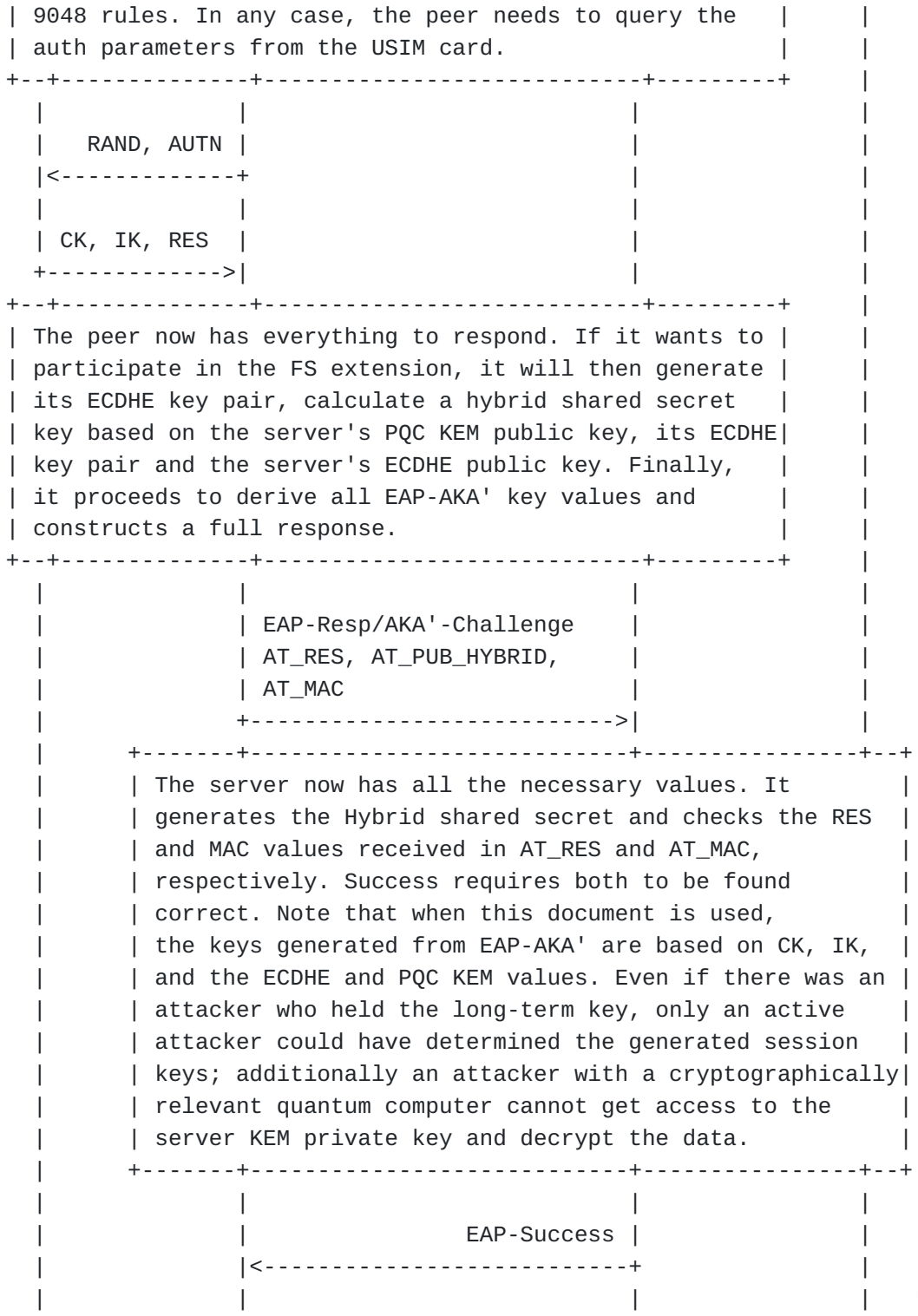
*The Hybrid key derivation function will be included first in the EAP-Request to indicate a higher priority than the traditional key derivation function.

6. Protocol Construction

This section defines the construction for hybrid key exchange in EAP-AKA' FS. Hybrid key exchange refers to using multiple key exchange algorithms simultaneously and combining the result with the goal of providing security even if all but one of the component algorithms is broken. It is motivated by transition to post-quantum cryptography.

6.1. Protocol Call Flow


USIM
Peer
Server
AD
EAP-Req/Identity
EAP-Resp/Identity
(Privacy-Friendly)
Server now has an identity for the peer. The server then asks the help of AD to run AKA algorithms, generating RAND, AUTN, XRES, CK, IK. Typically, the AD performs the first part of key derivations so that the authentication server gets the CK' and IK' keys already tied to a particular network name.
ID, key deriv. function, network name
RAND, AUTN, XRES, CK', IK'
Server now has the needed authentication vector. It generates an ephemeral ECDHE key pair, a PQC KEM key pair, sends the hybrid (PQC + ECDHE) public key of that key pair and the first EAP method message to the peer In the message the AT_PUB_HYBRID attribute carries the concatenation of ECDHE and PQC KEM public keys and the AT_KDF_FS attribute carries other FS-related parameters. Both of these are skippable attributes that can be ignored if the peer does not support this extension.
EAP-Req/AKA'-Challenge
AT_RAND, AT_AUTN, AT_KDF, AT_KDF_FS, AT_KDF_INPUT, AT_PUB_HYBRID, AT_MAC
The peer checks if it wants to do the FS extension. If yes, it will eventually respond with AT_PUB_HYBRID and AT_MAC. If not, it will ignore AT_PUB_HYBRID and AT_KDF_FS and base all calculations on basic EAP-AKA' attributes, continuing just as in EAP-AKA' per RFC



6.2. Key Steps in protocol construction

We outline the following key steps in the protocol:

*Server generates the PQC KEM Public key(pk2), private key (sk2) pair and the ECDH public key (pk1), private key (sk1) pair. The server will generate the AKA challenge and sends the EAP AKA'

Authentication Vector (AV). As defined in section 3.3 of [I-D.ietf-westerbaan-cfrg-hpke-xyber768d00] the server PQC KEM and ECDH key pairs are derived as:

```
sk1, pk1 = DeriveKeyPair(DHKEM)
sk2, pk2 = DeriveKeyPair(Kyber768Draft00)
```

*The server will store the expected response XRES, the ECDH private key sk1 and the PQC KEM private key sk2. The server will forward the EAP AKA' AV to peer along with pk1 and pk2.

*The USIM will validate the AKA challenge received, also verifies the MAC-I. After the verification is successful and if the peer also supports the Forward secrecy, peer will invoke kemEncaps using concact(pk1,pk2) as defined in section 3.3 of [I-D.ietf-westerbaan-cfrg-hpke-xyber768d00]:

```
Encap (concat(pk1,pk2)) = (enc, ss)
```

"enc" is the concatenation of the encapsulated key from ECDH and ciphertext from PQC KEM whereas "ss" is hybrid shared secret key. Hybrid shared key ss is generated by the peer using the Encap ([I-D.ietf-westerbaan-cfrg-hpke-xyber768d00]). The KEM combiner is a "hash and concatenation" based approach to generate a “hybrid” shared secret (ss).

*The peer will send the Authentication response RES and enc to the server.

*The server will verify the RES with XRES. The server will use the enc, PQC KEM private key sk2 and ECDH private key sk1 to generate shared secret:

```
Decap(enc, concat(sk1,sk2)) = ss
```

The generated ss from Decap is the hybrid shared secret key derived from PQC KEM and traditional ECDH. The peer and the server first generate the MK_HYBRID and subsequently generate MSK, EMSK as shown below:

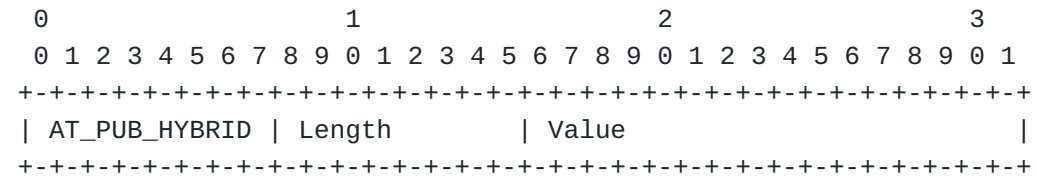
```
MK = PRF'(IK'|CK',"EAP-AKA'"|Identity)
HYBRID_SHARED_SECRET, enc = Encap(pKR)
MK_HYBRID = PRF'(IK'|CK'| HYBRID_SHARED_SECRET,"EAP-AKA' FS"| Identit
K_encr = MK[0..127]
K_aut = MK[128..383]
K_re = MK_HYBRID [0..255]
MSK = MK_HYBRID [256..767]
EMSK = MK_HYBRID [768..1279]
```

where, pkR is concatenation of traditional and PQC KEM public keys of the receiver, enc is concatenation of the encapsulated key from ECDH and the ciphertext from the PQC KEM and the Encap function is perfomed by the peer only.

7. Extensions to EAP-AKA' FS

7.1. AT_PUB_HYBRID

The format of the AT_PUB_HYBRID attribute is shown below.



The fields are as follows:

AT_PUB_HYBID:

This is set to TBA1 BY IANA.

Length:

The length of the attribute, set as other attributes in EAP-AKA [RFC4187]. The length is expressed in multiples of 4 bytes. The length includes the attribute type field, the Length field itself, and the Value field (along with any padding).

Value:

* EAP-Request: It contains the public key, which is the concatenation traditional and PQC KEM public keys from the EAP server.
* EAP-Response: It contains the encapsulated key, which is formed by concatenating the encapsulated key (enc) from the traditional KEM a and the ciphertext (ct) from the PQC KEM Encapsulation function fro EAP peer.

Because the length of the attribute must be a multiple of 4 bytes,the sender pads the Value field with zero bytes when necessary. To retain the security of the keys, the sender **SHALL** generate a fresh value for each run of the protocol.

8. IANA Considerations

One new value (TBA1) in the skippable range need to be assigned by IANA for AT_PUB_HYBRID (Section 7.1) in the "Attribute Types" registry under the "EAP-AKA and EAP-SIM Parameters" group.

IANA is requested to update the registry "EAP-AKA' AT_KDF_FS Key Derivation Function Values" with the Hybrid key derivation function entry:

Value	Description	Reference
TBA2	X25519Kyber768Draft00	[TBD BY IANA: THIS RFC]

9. References

9.1. Normative References

[I-D.ietf-emu-aka-pfs] Arkko, J., Norrman, K., 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-12, 19 February 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-emu-aka-pfs-12>.

[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>.

[RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, DOI 10.17487/RFC4187, January 2006, <https://www.rfc-editor.org/rfc/rfc4187>.

[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>.

[RFC9048] Arkko, J., Lehtovirta, V., Torvinen, V., and P. Eronen, "Improved Extensible Authentication Protocol Method for 3GPP Mobile Network Authentication and Key Agreement (EAP-AKA')", RFC 9048, DOI 10.17487/RFC9048, October 2021, <https://www.rfc-editor.org/rfc/rfc9048>.

[RFC9180] Barnes, R., Bhargavan, K., Lipp, B., and C. Wood, "Hybrid Public Key Encryption", RFC 9180, DOI 10.17487/RFC9180, February 2022, <https://www.rfc-editor.org/rfc/rfc9180>.

9.2. Informative References

[I-D.draft-ietf-emu-aka-pfs-11] Arkko, J., Norrman, K., 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-11, 10 July 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-emu-aka-pfs-11>.

[I-D.ietf-pquip-pqt-hybrid-terminology] D, F., "Terminology for Post-Quantum Traditional Hybrid Schemes", Work in Progress, Internet-Draft, draft-ietf-pquip-pqt-hybrid-terminology-02, 2 February 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqt-hybrid-terminology-02>.

[I-D.ietf-westerbaan-cfrg-hpke-xyber768d00] "*** BROKEN REFERENCE ***".

[RFC6090] McGrew, D., Igoe, K., and M. Salter, "Fundamental Elliptic Curve Cryptography Algorithms", RFC 6090, DOI 10.17487/RFC6090, February 2011, <https://www.rfc-editor.org/rfc/rfc6090>.

[RFC8037] Liusvaara, I., "CFRG Elliptic Curve Diffie-Hellman (ECDH) and Signatures in JSON Object Signing and Encryption (JOSE)", RFC 8037, DOI 10.17487/RFC8037, January 2017, <https://www.rfc-editor.org/rfc/rfc8037>.

[RFC9052] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <https://www.rfc-editor.org/rfc/rfc9052>.

Appendix A. Acknowledgements

This draft leverages text from [I-D.draft-ietf-emu-aka-pfs-11]

Authors' Addresses

Aritra Banerjee
Nokia
Munich
Germany

Email: aritra.banerjee@nokia.com

Tirumaleswar Reddy
Nokia
Bangalore
Karnataka
India

Email: kondtir@gmail.com