

Forward Secure Reauthentication in EAP-AKA'

draft-wang-emu-fs-reauth-00

EMU, IETF 125 @ Shenzhen

19/3/2026

Guilin Wang and Zander Lei

FS Reauthentication in EAP-AKA'

□ Information of our draft

- Title: Forward Secure Reauthentication in EAP-AKA'
- draft-wang-emu-fs-reauth-00
- <https://datatracker.ietf.org/doc/draft-wang-emu-fs-reauth/>

□ A Brief History of EAP-AKA Series

- **RFC 4187: Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)**
 - for mobile devices connecting to networks using their credentials from SIM/USIM cards
 - reauthentication procedure is specified as an optional to enhance performance
- **RFC 5448: Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')**
 - It introduces a new key derivation function (KDF), SHA-256 instead of SHA-1
 - The KDF also binds the keys derived within the method to the name of the access network, for limiting the effects of compromised access network nodes and keys
- **RFC 9048: Improved Extensible Authentication Protocol Method for 3GPP Mobile Network Authentication and Key Agreement (EAP-AKA')**
 - specifies the protocol behavior for both 4G and 5G deployments using EAP-AKA'
 - How to construct the Network Name field
 - How EAP-AKA' use identifiers in 5G
 - How to define session identifiers and other exported parameters
 - How to update the requirements on generating pseudonym usernames and fast reauthentication identities to ensure identity privacy
- **RFC 9678: Forward Secrecy Extension to the Improved Extensible Authentication Protocol Method for Authentication and Key Agreement (EAP-AKA' FS)**
 - enhances the forward security (FS) for the session keys generated in EAP-AKA' by adding ECDH (ephemeral Diffie-Hellman key exchange)

FS Reauthentication in EAP-AKA'

□ Motivations

- As noted in Section 7.6 of [RFC9678], reauthentication pseudonym identities are encrypted under K_{encr} , a key without forward security, as it is generated before ephemeral DH.
- Once the long-term compromised, reauthentication protocol runs linkable.
- "If the pseudonym linkage risk is not acceptable, one way to avoid the linkage is to always require full EAP-AKA' authentication."
- So, this draft aims to update K_{encr} so that it is forward secure.

□ The proposed solution

- This draft specifies an update to EAP-AKA' FS and its predecessors above.
- **This update enables forward security (FS) of the Transient EAP Keys (TEKs) for protecting EAP packets, which are not in EAP-AKA' FS.**
- Based on this extension, reauthentication after a full authentication will be unlinkable to each other and then the privacy of end users is enhanced.
- This update is optional to the above standards

FS Reauthentication in EAP-AKA'

Fig. 1 EAP-AKA' FS Authentication Process (Section 5 of RFC 9678)

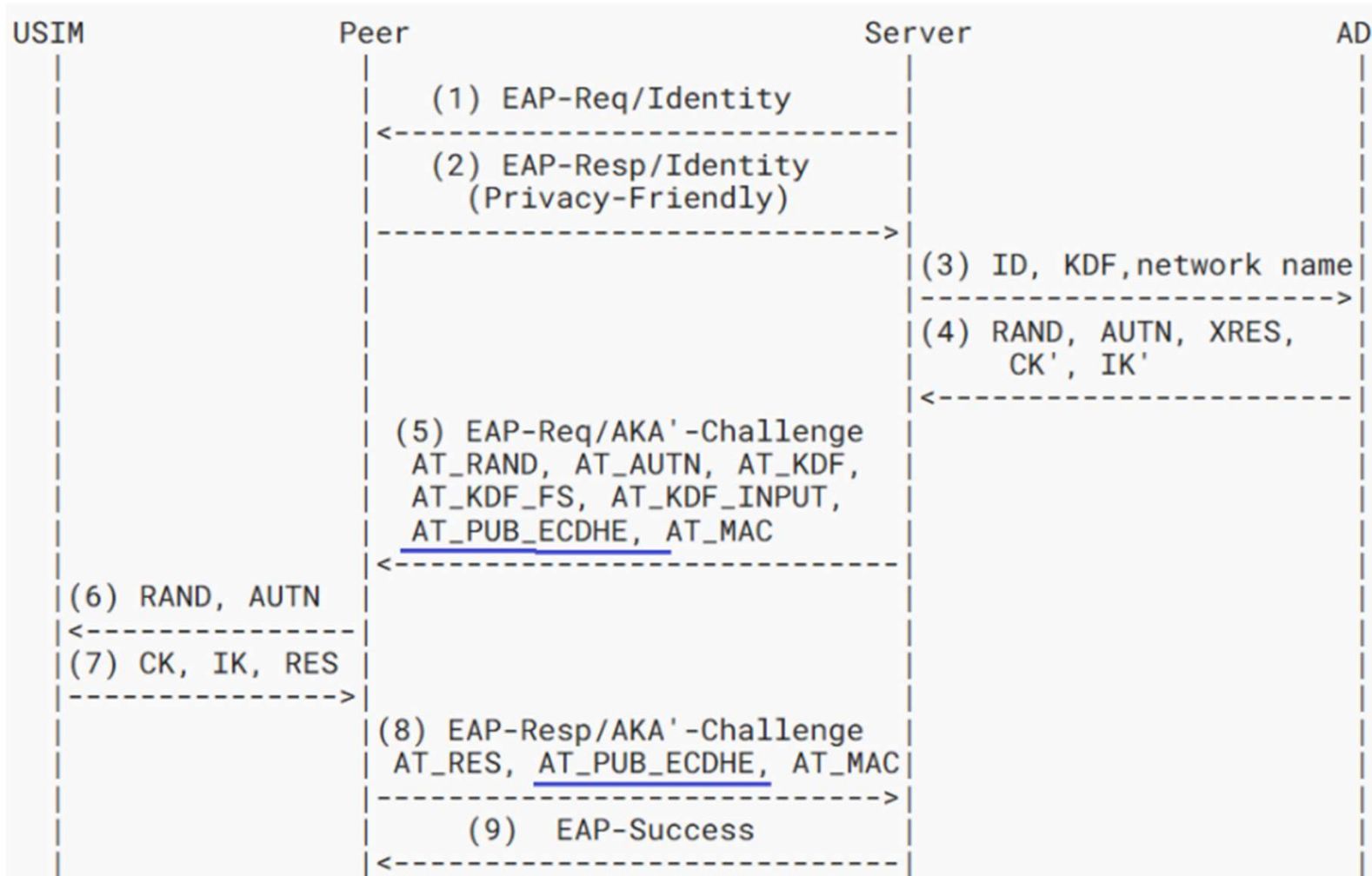


Fig. 2 Key Derivation in EAP-AKA' FS (Section 6.3 of RFC 9678)

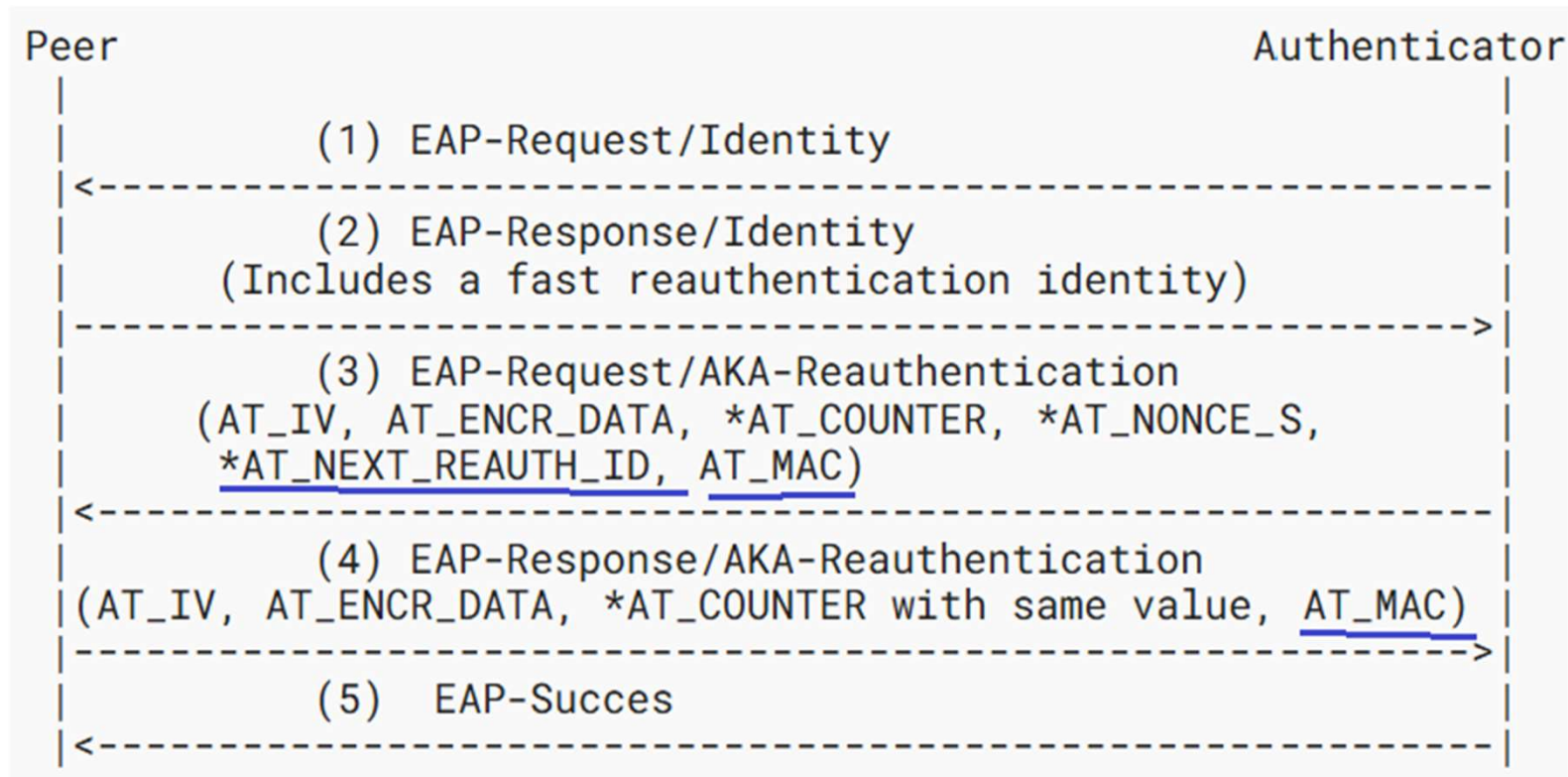
```

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

K_encr (reauth ID) not forward secure!

FS Reauthentication in EAP-AKA'

Fig. 3. Reauthentication Procedure (Section 5.4 of RFC 4187)



Linkage Attacks

- Once the long-term key is compromised, an attacker will know K_{encr} and K_{aut} .
- Then, the attacker can decrypt $AT_NEXT_REAUTH_ID$ and verify AT_MAC .
- So, multiple reauthentication runs can be linkable.

FS Reauthentication in EAP-AKA'

RFC 9678

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

Update
K_encr & K_aut



This Draft

```
MK      = PRF'(IK'|CK',"EAP-AKA'|Identity)
K_encr  = MK[0..127]
K_aut   = MK[128..383]
MK_ECDHE = PRF'(IK'|CK'|SHARED_SECRET,
               "EAP-AKA' FS"|Identity)
K_encr' = MK_ECDHE[0..127]
K_aut'  = MK_ECDHE[128..383]
K_re    = MK_ECDHE[384..639]
MSK     = MK_ECDHE[640..1060]
EMSK    = MK_ECDHE[1061..1633]
```

- ❑ So, no more linkage attacks, when the two keys are used to protect AT_NEXT_REAUTH_ID and AT_MAC.
- ❑ This update applies to the following PQ extensions to RFC 9678 as well.
 - [I-D.ietf-emu-hybrid-pqc-eapaka] Banerjee, A. and T. Reddy.K, "Enhancing Security in EAP-AKA' with Hybrid Post-Quantum Cryptography", draft-ietf-emu-hybrid-pqc-eapaka-01, 26 February 2026
 - [I-D.ietf-emu-pqc-eapaka] Reddy.K, T. and A. Banerjee, "Post-Quantum Key Encapsulation Mechanisms (PQ KEMs) in EAP-AKA prime", draft-ietf-emu-pqc-eapaka-01, 26 February 2026

FS Reauthentication in EAP-AKA'

Appreciate your you comments and reviews!

Thanks!