Forward Secure Reauthentication in EAP-AKA’

draft-ietf-emu-fs-reauth-00

EMU, IETF 127 @ San francisco

20/11/2026

Guilin Wang

FS Reauthentication in EAP-AKA’

❑ Information of our draft

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

❑ 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 TEKs (K_encr and K_aut) so that they are forward secure.**

❑ The proposed solution

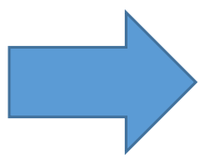
- This draft specifies an update to EAP-AKA' FS and its PQ followers.
- **This update enables forward security (FS) of the Transient EAP Keys (TEKs) for protecting EAP messages,** which are not in EAP-AKA' FS.
- Based on this extension, **reauthentication after a full authentication will be unlinkable 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’: Updates since 126 meeting

Adopted by the WG on 2026-11-11. Thanks!

❑ Version 03

- FS TEKs are taken from the tail of the output of key derivation functions, rather than the head part in version 02.
- Added exact formula for taking TEKs when applying to [I-D.ietf-emu-pqc-eapaka] and [I-D.ietf-emu-hybrid-pqc-eapaka].
- Described how to use TEKs in full authentication and fast reauthentication in Section 6.
- Added security considerations in Section 9.



❑ draft-ietf-emu-fs-reauth-00

- AT_NEXT_REAUTH_ID separated from message 9 in Figure 7, as suggested in the Call of Group Adoption.
- Updated Section 8 (IANA Considerations) with the skippable-range rationale.
- Formulas for key derivation in Figures 5 and 6 updated slightly by following new versions of [I-D.ietf-emu-pqc-eapaka] and [I-D.ietf-emu-hybrid-pqc-eapaka].

FS Reauthentication in EAP-AKA': Full Authentication

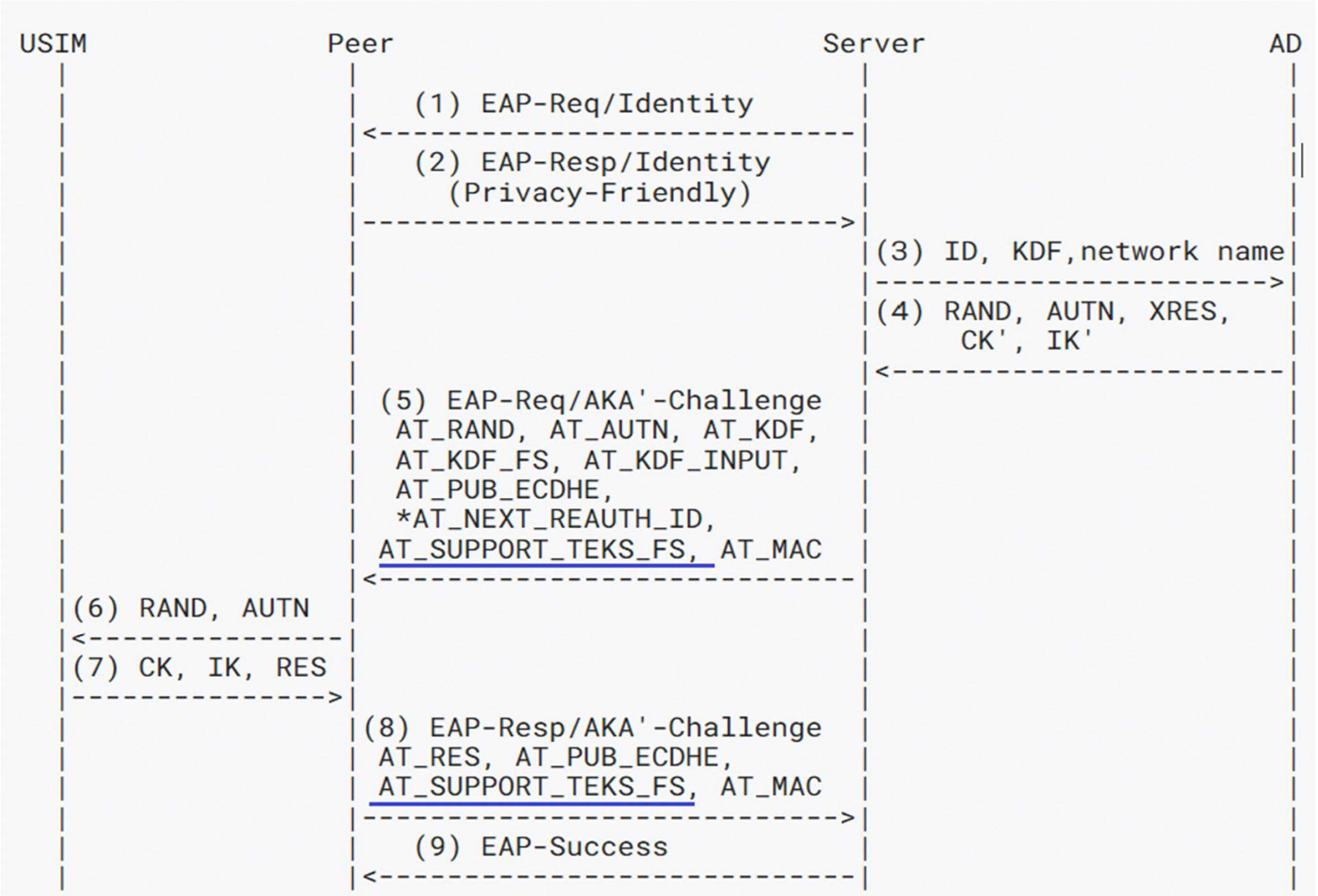
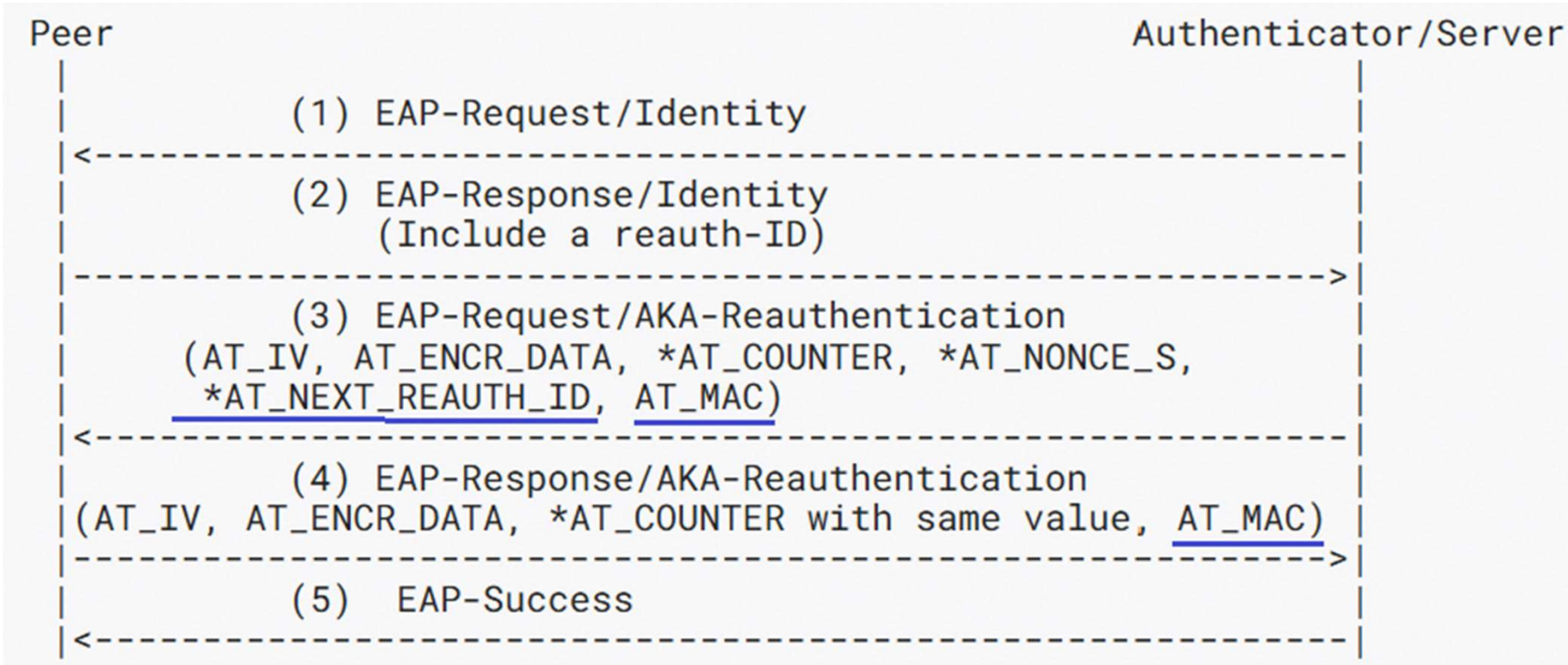


Figure 7. EAP-AKA' FS Authentication Process with TEKs Forward Security

- AT_NEXT_REAUTH_ID with FS was removed from mess. (9)
- AT_SUPPORT_TEKS_FS: notice to support this update.
- The first reauth-ID not FS: sent in mess. (5)
- So, the first fast authentication is not FS.
- But all followings are FS.

- **This choice achieves the best backward compatibility and the smallest change to EAP-AKA'.**

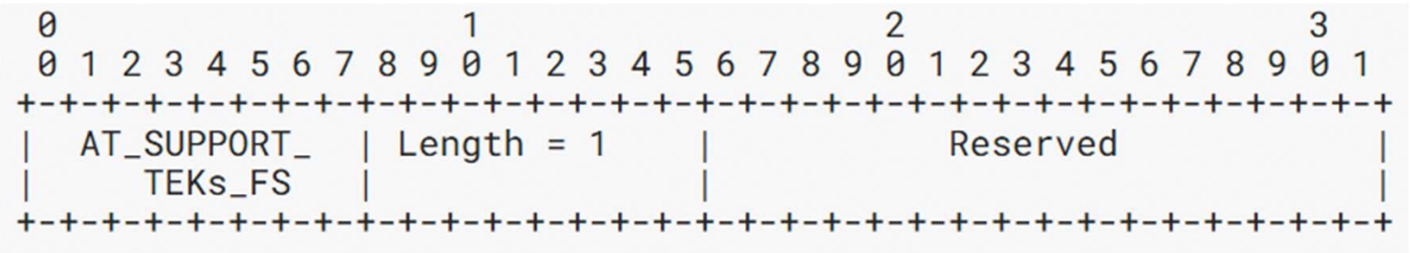
FS Reauthentication in EAP-AKA': Fast Reauthentication



- Highlighted values are still the same as messages specified by RFC 4187 & RFC 9678.
- However, they are protected with forward secure K_encr' and K_aut.
- However, note that when the first reauth-ID used in mess. (2), that rund is not FS.

FS Reauthentication in EAP-AKA': AT_SUPPORT_TEKS_FS

❑ Format of AT_SUPPORT_TEKS_FS



❑ IANA Considerations

Value	Description	Reference
TBA1 (128-255)	AT_SUPPORT_TEKS_FS	[This Document]

Table 1: IANA Attribute Type Allocation

- Requests IANA to allocate one new Attribute Type value (TBA1) from the skippable range (128-255) in the **"Attribute Types" registry** under the "Extensible Authentication Protocol (EAP) Registry" ("EAP-SIM/AKA/AKA' Attributes" subregistry)
- This is necessary to support this update as **an optional feature** to RFC 4187, RFC 9678, and the new PQ specifications.

FS Reauthentication in EAP-AKA': Security Considerations

- **Cryptographic Assumptions: without introducing new hardness assumptions**
  - PRF': HMAC-SHA-256
  - ephemeral key exchange: ECDHE, ML-KEM, or hybrid KEM
  - Symmetric primitives: AES-CBC-128 and HMAC-SHA-256-128.
- **Forward Security or Post-Compromise Unlinkability**
  - Long-term USIM compromise does not retroactively expose past sessions, if ephemeral keys and state (K_encr', K_aut', K_re) are zeroized immediately upon termination.
  - Compromise of runtime server memory limits exposure strictly to the active full authentication epoch.
- **Downgrade Attack Analysis**
  - Active MITM attempts to strip AT_SUPPORT_TEKS_FS fail during uncompromised handshakes because AT_MAC covers the entire EAP packet.
  - Post-compromise active impersonation remains out of scope as an adversary holding the long-term key can impersonate entities regardless of extension negotiation.
- **No change on the security state machine of EAP-AKA' FS**
  - The key is using the skippable AT_SUPPORT_TEKS_FS notice.

Thanks!