EAP-AKA Forward Secrecy
(draft-ietf-emu-aka-pfs-08)

Jari Arkko, John Mattsson, Karl Norrman

(slides version 2)
Draft status

• Revised after AD and IETF LC comments
• Now in 2nd IETF LC, which ends on August 1st
Draft -11 changes

Addressed IETF Last Call comments from directorates, Security AD, Meiling Cheng, and a detailed pass from the author Karl:

• Replaced the reference to the deprecated FIPS 186-4 with SP 800-186
• Changed HSS to Authentication Database (AD) as HSS is not used in all 3GPP generations
• Explained difference between EAP-AKA and EAP-AKA'
• Explained how DH ephemeral key exchange provides more than FS and how this is important mitigating pervasive monitoring
• Included links for the zero trust principles
• Explained why $K_{enr}$ and $K_{auth}$ not being protected by the ECDHE addition
• Added that a future introduction of KEM might require additional changes
• Changed SIM to USIM everywhere. A USIM is required for the AKA used here
• Changed to long-term key instead of long-term secret or long-term shared secret
• Reference updates
• Various editorial improvements
K_encr and K_auth protection via ECDHE

The purpose of this extension is to provide FS for the keys resulting from an EAP-AKA’ authentication run

• This is useful, e.g., for traffic protection keys

Last call raised a question about FS within EAP-AKA’ itself, specifically when K_encr is used with AT_ENCR

• Version -11 now explains this is no issue for K_auth but data encrypted with K_encr is not

Is this an issue?

• One case where this may matter is with pseudonyms for next reauth

• Current draft takes action 1: Explain what protection is or is not provided.

• We could go beyond this, say, action 2: Recommend avoiding pseudonyms if this is an issue.

• Or even action 3: Mandate a delayed exchanged of pseudonyms or other sensitive data exchanged via AT_ENCR (details to be designed)

• Does the WG have an opinion?