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

Jari Arkko, John Mattsson, Karl Norrman, Vesa Torvinen

(+ many contributors in EMU and elsewhere)

Draft status

- Revised after IETF 114
- Now ready for WGLC

Draft -08 changes

- Support for the NIST P-256 group has been made mandatory in Section 6.4
  - Aligns the requirements with 3GPP SUCI encryption requirements
- The interaction between AT_KDF and AT_KDF_FS has been clarified
  - This becomes relevant if later specs add new values for either
  - Now we say how future specifications need to specify the treatment combinations
- Further clarification of key calculation in Section 6.3
  - Validation requirements & keeping the two algorithm requirements separate
- Impacts of potential future quantum computing attacks described
- Addition of a discussion about metadata in Section 7.4
- Various editorial improvements, reference updates