EAP-AKA Forward Secrecy (draft-ietf-emu-aka-pfs-06)

Jari Arkko, Karl Norrman, Vesa Torvinen (+ many contributors in EMU and elsewhere)

Draft status

- Been more or less ready, waiting for … some final details … opportunity to insert into use … author cycles
- But it does not make sense to wait forever, perhaps it is time to make this an RFC, and ready to be adopted for those that want to use it

Draft changes

- References updated
  E.g., RFCs 9048, 9190
- The draft now uses "forward secrecy" terminology
  Also references RFC 7624 per recommendations on mailing list discussion
  See https://mailarchive.ietf.org/arch/msg/emu/JIJizJcIOGwPHaiqgo2WohXFlkY/

Draft open questions

What's the conclusion on the encoding / public value length discussion?

- There's been a mailing list discussion
- I think the current text requires confirmation from the working group that it is sufficient – or a change
- John:
  - EDHOC and RFC 6090 use 32 bytes
  - Forcing 33 requires extra calculation
  - Referencing 186-4 and SEG is strange
- Rene:
  - Most implementations and standards use lossless (33 byte) representation
  - Encoding format matters, lets not create artificial differences
- Draft:

```
Value
   This value is the sender's ECDHE public value.  It is calculated
   as follows:

   *  For X25519/Curve25519, the length of this value is 32 bytes,
      encoded in binary as specified [RFC7748] Section 6.1.

   *  For P-256, the length of this value is 33 bytes, encoded in
      binary as specified in [FIPS186-4], using the compressed form
      from Section 2.7.1 of [SEC2].
```