EAP-AKA Forward Secrecy (draft-ietf-emu-aka-pfs-07)

Jari Arkko, John Mattsson, Karl Norrman, Vesa Torvinen

(+ many contributors in EMU and elsewhere)

Draft status

- The protocol has been technically ready for some time
  - Modulo discussion about encoding of the public values (slide 4)
- We believe there's an opportunity to deploy this and gain significant security improvement, particularly against pervasive surveillance activities
- For the -07 version John joined as an author
- Draft was improved in a number of ways (slide 3) and we went through quite a bit of background wrt the current choice of encoding (slide 4)
- Start WGLC at/after this meeting

Draft -07 changes

- The impact of forward secrecy explanation has been improved in the abstract and security considerations.
- The draft now more forcefully explains why the authors believe it is important to migrate existing systems to use forward secrecy, and makes a recommendation for this migration.
- The draft does no longer refer to issues within the smart cards but rather the smart card supply chain.
- The rationale for chosen algorithms is explained.

Public value encoding

Authors have gone through the discussion, references, other systems, and some open source cryptographic library implementations

Our observations are as follows:

- We checked the language relating to the public value encoding, and believe it is exactly according to the referenc ([RFC7748] Section 6.1 and [SEC2] Section 2.7.1)

```
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].
```

- The same arrangement is used elsewhere in 3GPP 5G specifications.
- Given this, we'd like to keep the current text and move forward
  - There are alternatives, such as allowing compressed and uncompressed form from SEC2
- Does anyone in the working group object?

WGLC

- This would be a good time to formally start the WGLC