EAP-TEAP-BRKSI ▭ ????

Eliot Lear, Owen Friel, Dan Harkins, Na
Cam-Winget

IETF 106

Draft-lear-eap-teap-brski changes

- Diagrams have been simplified

- Rework of discussion around NAI

- Beginning of restructuring toward a different target:
  - Rather than focus just on BRSKI, focus on overall TEAP update

Goals: Go through RFC 7170 Errata

Erratum	Reported by	Topic	Proposed Action
5127	Tuure Vartiainen	Typo "|" intead of "," in TLS_PREF call	Accept
5128	Tuure Vartiainen	Typo "," instead of "|" in TLS_PREF	Accept
5765	Juoni Malinen	Authority TLV only required in outer	Accept
5767	Juoni Malinen	Clarify Intermediate-Result language within tunnel	Discuss
5768	Juoni Malinen	Incompatible field lengths, and TLS version issues	Discuss
5770	Juoni Malinen	S-IMCK[j] derivation confusion	Discuss
5775	Juoni Malinen	CMK derivation confusion	Discuss
5844	Juoni Malinen	Crypto binding used when Intermediate result should be used	Accept
5845	Juoni Malinen	Method completion text unclear	Discuss (but it's close)

New TLVs

- Voucher
- CSRATTRs
- Root certs
- NAI
- ???

Key issue

- How does TEAP interact with other 802.11 capabilities?
  - DPP
  - Other…

Next Steps

- Should we have a section that just accepts errata and update?

- Do we deal with TLS 1.3 or should that be in the TLS 1.3 doc?

- Proposal
  - Less focus on BRSKI, more focus on update
  - Roll it slow. Get some coding done
  - Maybe adopt draft as WG draft but not plan for approval until we nail above, plus any proposed new TLVs