7170bis

LAST CHANCE TO SEE
ALAN DEKOK IETF 117
TEAP

- Minor changes since IETF 116
- New diagrams from Eliot
- Reference RFC 9427
- Add error “Inner method not supported”
- Identity-Hint which makes it easier to select inner auth method
- PKCS still not implemented, might as well leave it in
MITM ATTACKS

› It is possible to use TEAP with inner methods that do not provide MSK
› Which means it is subject to MITM attacks
  › OK, don’t do that? Require at least one inner method with provides MSK
DEVolving To EAP-TLS

- Note that using TEAP with client certificate and no inner auth is allowed
- It still has to proceed to Phase 2 for inner Crypto-Binding, Result, etc.
- Which also serves as "protected success indication" as per RFC 9427
IMPLEMENTATION ISSUES

- Deployments with TEAP in real-world scenarios show difficulties
- Insufficient error messages and implementation issues
  - If everyone agrees on everything, it works fine
  - If supplicant has different configuration than what server expects...
- Probably need to recommend automated configuration
- TEAP is likely to have teething problems in deployments
Q&A

- There doesn’t seem to be anything else to do
- Any last-minute comments?