7170bis

ARE WE THERE YET?

ALAN DEKOK IETF 116
TEAP

› Many, many changes since IETF 115.
› We now have interoperable implementations
   ‣ Windows, wpa_supplicant, FreeRADIUS, ISE, ...
› Many clarifications and fixes
› All errata have been addressed
› Thanks to the WG members for much feedback and corrections
OPEN ISSUES

‣ It looks like no one has implemented PKCS portions
‣ Keep or remove?
‣ Request-Action issue raised by Eliot
OPEN ISSUES - SIGNALLING

- No way to select auth mechanisms based on provided identity
  - for EAP, Identity comes before selection of EAP type
  - For inner TEAP, server has to choose EAP / password before it knows identity!
- No way to signal supported auth types (machine / user)
  - Must ask, and then return an error
- Client cannot send “I have X and Y”, or server sends “I want X and/or Y”
IMPLEMENTATION ISSUES

- Windows client when configured only for a single authentication whilst the server is for chained authentication you end up with:

- server: please do machine authentication (Identity-Type-TLV) and tell me your identity (EAP-Payload-TLV[EAP-Identity])

- notice that these are done simultaneously we cannot get the identity and then pick the type of authentication

- client: my identity is "host/bobs-workstation" and I am doing EAP-TLS to authenticate

- server: please now do user authentication

- server does not know the clients configuration

- client: my identity is "" (empty string)....stall, instead of ?? Error
Q&A

› Who has read the document in detail?
› Who has implemented it?
› Does anyone have operational experience with it?