Onboarding

DRAFT-RICHARDSON-EMU-EAP-ONBOARDING-01
IETF 114
DEVICE ONBOARDING

- Unconfigured device needs to be onboarded, but has no credentials
  
- Solution: use unauthenticated EAP-TLS, and join a captive portal network
  
- Problem: RFC 5216 allows for unauthenticated EAP-TLS, but offers no further help
  
- Solution: use explicit signalling via NAI of onboarding@eap.arpa
  
  - NAI is local only, and cannot be forwarded / proxied
  
  - device can access a limited network for onboarding
  
  - Once on a captive portal network, use RFC8995(BRSKI) to get credentials
    
    - this avoids trying to stuff BRSKI into EAP, and reuses existing captive portal infrastructure
FURTHER WORK

- The device can still authenticate the server (e.g. subjectAltName)
  - If a CA root is good enough for web browsing, it’s good enough for onboarding
- The behavior of the local network is “captive portal + TBD”
- ...@eap.arpa can be used to signal different kinds of desired access
RELATED WORK

- Similar work being done elsewhere (Hotspot 2.0 onboarding, etc.)
  - SDO-specific
- WBA has “unauth EAP-TLS” using vendor-specific EAP method.
  - It would be good for the IETF to define standard methods for this
    - Avoids fragmentation in the technology
DISCUSSION
DRAFT-RICHARDSON-EMU-EAP-ONBOARDING-01