# draft-ietf-bootstrapped-tls-07
# TLS-POK

Dan Harkins & Owen Friel

EMU WG, IETF 121

# Summary

- Reuse Wi-Fi alliance Easy Connect / Device Provisioning Profile (DPP) bootstrap approach and DPP Elliptic Curve keypair for wired bootstrap
- Provides mutual authentication between bootstrapping client and server that knows client's bootstrap public key
- Depends on these key RFCs
  - RFC 9258 Importing External (PSKs) for TLS 1.3 to import derived PSK
  - RFC 8773 Cert Based Auth with External PSK
  - RFC 7250 TLS with raw public key using bootstrapping key
  - RFC 5869 HKDF to derive External PSK ID from bootstrap key
  - draft-ietf-emu-eap-arpa-03 for indicating TLS-POK bootstrapping to EAP server
- No new TLS extensions, changes or new funky crypto required
  - But does use 2 relatively new TLS RFCs that are not widely supported yet

# Draft Status

- WGLC
- All comments to date addressed
- TODO: add test vectors

# Implementation Status

- No E2E implementation on a commercial TLS stack with a commercial AAA server
- TLS Status

| TLS Stack | Status |
|---|---|
| golang mint (Richard Barnes *et al*) | End to end TLS implementation<br>Not integrated with any EAP / AAA server |
| OpenSSL | RFC9258: No<br>RFC8773: Implemented on Owen's fork but not merged yet |
| GnuTLS | RFC8773: No |

- EAP Status

| RFC | Status |
|---|---|
| draft-ietf-emu-eap-arpa-03 | FreeRADIUS status? |

# Questions and Next Steps?