draft-ietf-bootstrapped-tls-01 (was draft-friel-tls-eap-dpp)

Dan Harkins & Owen Friel

EMU WG, IETF 115

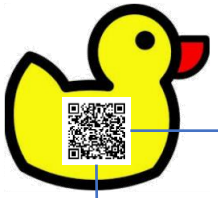
Summary

- Reuse Wi-Fi alliance Easy Connect / Device Provisioning Profile (DPP) bootstrap approach for wired bootstrap
- Reuse DPP EC bootstrap key pair and formats (e.g. QR code)
- Provides mutual authentication between bootstrapping client and server that knows client's bootstrap public key
- Use RFC 5869 HKDF to derive PSK from bootstrap key
- Use RFC 8773 Cert Based Auth with External PSK
- Use RFC 7250 TLS with raw public key using bootstrapping key
- Use RFC 9258 Importing External (PSKs) for TLS 1.3 to import derived PSK
- No new TLS extensions, changes or new funky crypto required

Changes since IETF 114

- Addressed mailer feedback
- Refactored to (hopefully) improve readability
- Clarified identity handling in EAP
- Defined an eap-dpp.arpa domain

TLS authentication w/DPP bootstrapping keys



RFC 5869 → RFC 9258

Client

ClientHello
RFC 8773 → **+ cert_with_extern_psk**
RFC 7250 → **+ client_cert_type=RawPublicKey**
+ key_share
RFC 5869 → RFC 9258 → **+ pre_shared_key** --------> ?

Server

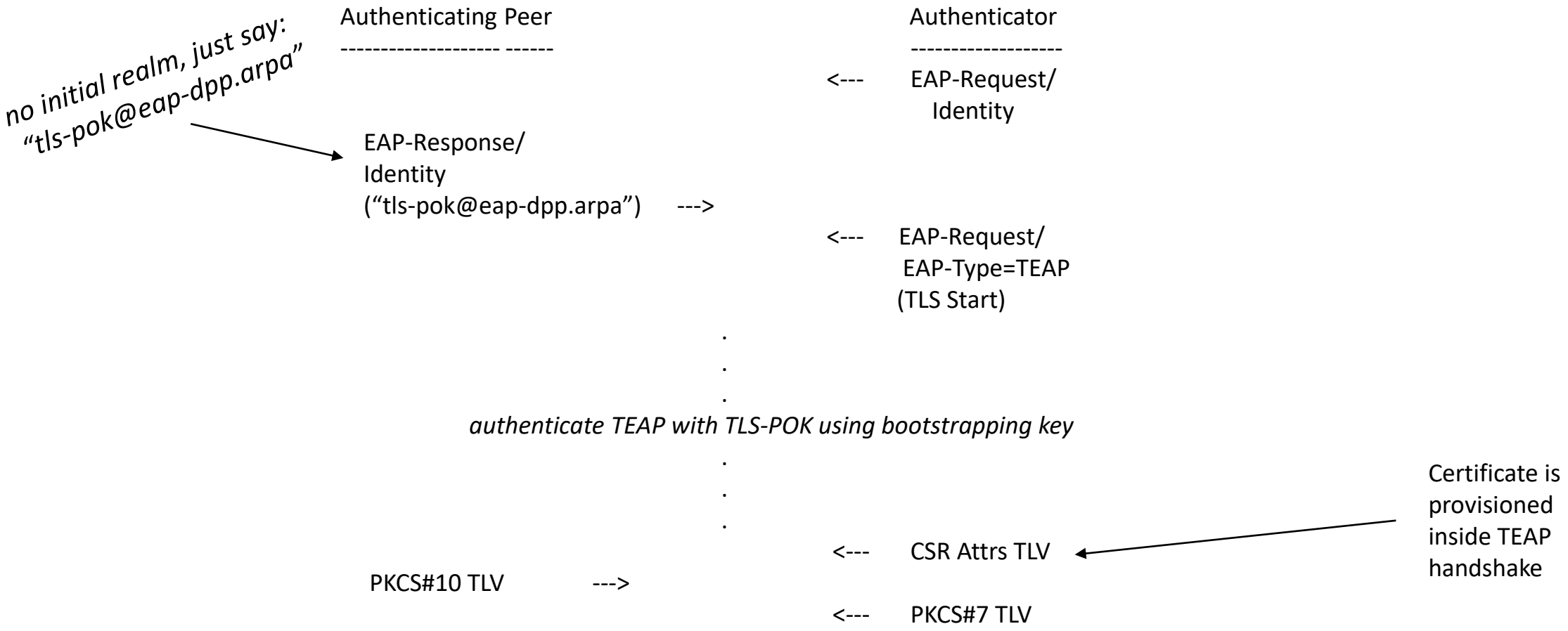
ServerHello
+ cert_with_extern_psk
+ client_cert_type=RawPublicKey
+ key_share
+ pre_shared_key
{EncryptedExtensions}
{CertificateRequest}
{Certificate}
{CertificateVerify}
{Finished}
<--------

Server uses RFC 9258 ImportedIdentity to lookup the bootstrap key

{Certificate}
{CertificateVerify}
{Finished} -------->
[Application Data] <-------> [Application Data]

Legend:
present for dpp
existing exchange

TEAP w/DPP bootstrapping keys



Supplicant's subsequent connection uses provisioned certificate

Questions and Next Steps?