Using BRSKI with wireless

Eliot Lear, Owen Friel, Nancy Cam-Winget
Bootstrapping with wired (ANIMA BRSKI)

- Pledge=Device
- Registrar=Store of known devices (tied to AAA infrastructure)
- MASA="Manufacturer Authorized Signing Authority"
- EST -enrollment over secure transport
Client gets a certificate via EST (RFC 7030)

Device already has a deployment certificate and can communicate with the registrar

Initiate TLS connection if necessary

SimpleEnroll(CSR)

Here's a cert

Device now has a local deployment certificate. 802.1X Authentications or similar can follow.
Cramming that into EAP

```
+--------+        +--------+        +--------+
  Client  |        | TEAP-Server |        | MASA   |
  +--------+        +--------+        +--------+
  ClientHello
  +----------------->
  ServerHello,
  Certificate(1),
  ServerKeyExchange,
  CertificateRequest(2),
  ServerHelloDone,
  <----------------
  Certificate(3),
  ClientKeyExchange,
  CertificateVerify,
  ChangeCipherSpec,
  Finished
  +----------------->
  ChangeCipherSpec,
  Finished
  <----------------
  Crypto-Binding TLV
  <----------------
  Crypto-Binding TLV
  +----------------->
  Result TLV
  <----------------
  Result TLV
  +----------------->
  EAP-Success
```
Next steps

• We still don’t think we have the flow just quite right
  • So...
    • Code, code, code

• Need to include asynchronous onboarding draft work by Steffen Fries
  • “No soup for you, come back in 2 days”

• Need to address offline use case
  • ANIMA BRISKI assumes online use case; Michael Richardson has done some work on this. Also being discussed at IEEE

• Still need to solve the SSID selection problem