draft-lear-eap-teap-brski-01

Eliot Lear, Owen Friel, Nancy-Cam-Winget

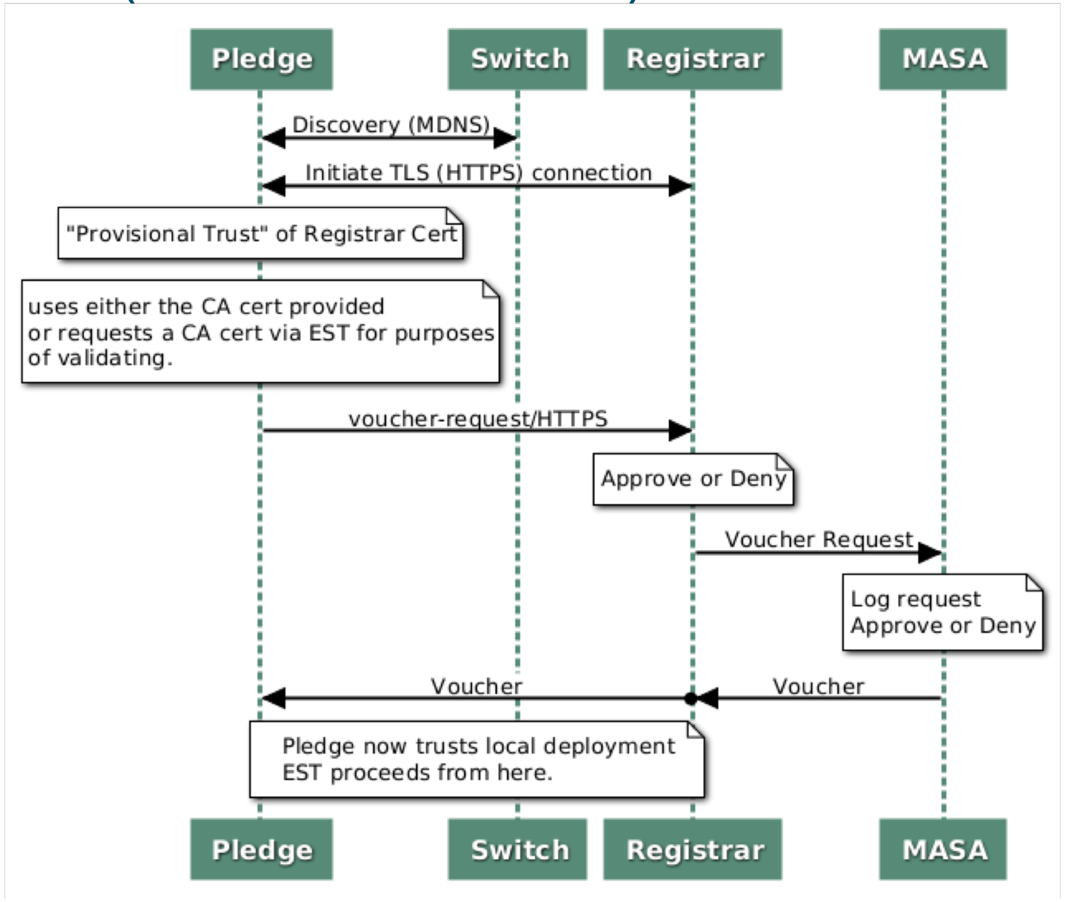
5. Nov 2018

Problem Statement and Goals

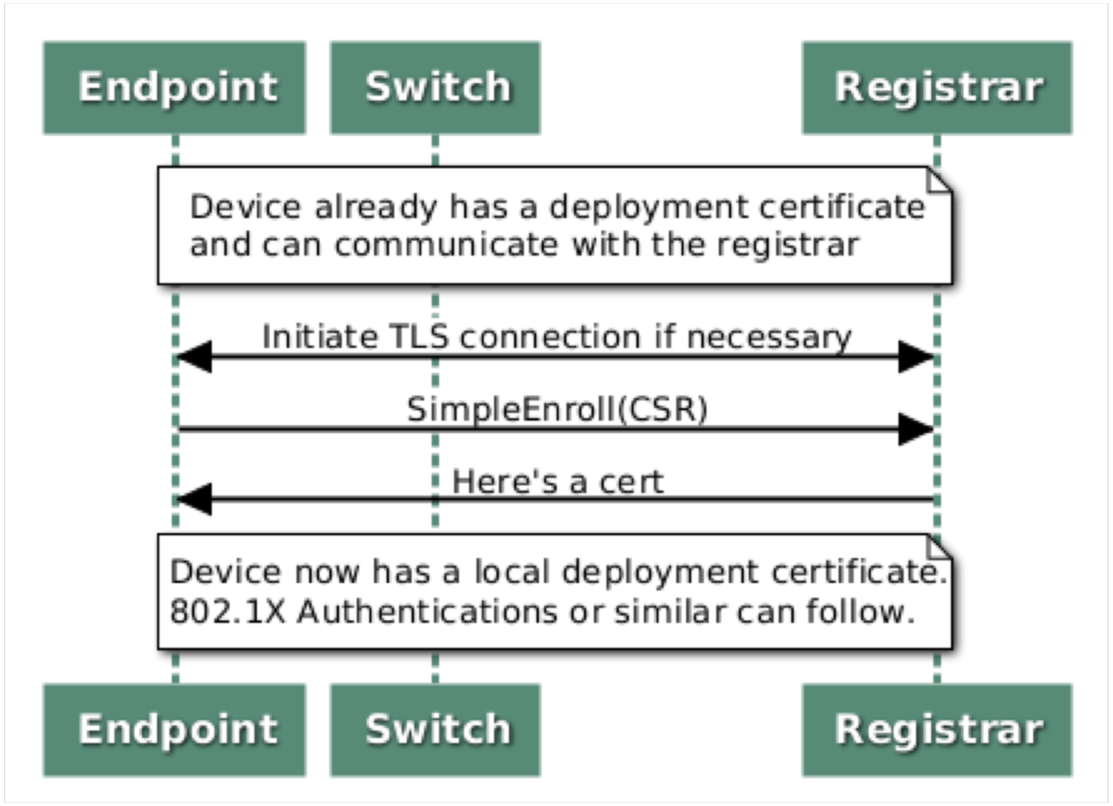
- Devices need trusted introduction to a local deployment
- ANIMA BRSKI provides that trusted introduction
  - Certificate-based trust anchor installation
- EST provides the means to enroll a deployment certificate
- BRSKI and EST assume some level of network connectivity
- Not the case with 802.11 (and other) networks
- EAP provides a tunnel mechanism prior to network admission control
- TEAP has many of the TLVs we already need to implement much of this

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)


Endpoint
Switch
Registrar
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.
Endpoint
Switch
Registrar

Overview

```
+---------+            +-------------+     +-------+
| Client  |            | TEAP-Server |     | MASA  |
+---------+            +-------------+     +-------+
    |                         |                |
    |       ClientHello       |                |
    |------------------------>|                |
    |   ServerHello, etc.(1)  |                |
    |<------------------------|                |
    |      etc., Finished     |                |
    |------------------------>|                |
    |      etc., Finished     |                |
    |<------------------------|                |
    | BRSKI-RequestAction(2)  |                |
    |<------------------------|                |
    | BRSKI-RequestVoucher(3) |                |
    |------------------------>| RequestVoucher |
    |                         |--------------->|
    |                         |    Voucher     |
    |      BRSKI-Voucher(4)   |<---------------|
    |<------------------------|                |
```

Overview

```
+--------+             +-------------+     +------+
| Client |             | TEAP-Server |     | MASA |
+--------+             +-------------+     +------+
    |<-------------------------|                |
    |  Trusted-Server-Root     |                |
    |------------------------->|                |
    |  Trusted-Server-Root     |                |
    |<-------------------------|                |
    |     CSR-Attributes       |                |
    |<-------------------------|                |
    |         PKCS#10          |                |
    |------------------------->|                |
    |         PKCS#7           |                |
    |<-------------------------|                |
    |  Crypto-Binding TLV      |                |
    |<-------------------------|                |
    |  Crypto-Binding TLV      |                |
    |------------------------->|                |
    |  Result TLV              |                |
    |<-------------------------|                |
    |  Result TLV              |                |
    |------------------------->|                |
    |      EAP-Success         |                |
    |<-------------------------|                |
```

Changes since -00

- TLVs documented
- IANA considerations section added
- Several “request” messages removed (they can be implied)
- Flows updated

Issues that need to be addressed

- Security Considerations
- Can we further develop the voucher mechanism to address non-MASA cases?
- Can we further develop to use proof other than a certificate (PSK or other)?

Next Steps

- Consider those questions
- Work on the underlying architecture
- Consider EAP-NOOB use case as well
- Not asking for WG adoption at this time
- May need some interim discussions on the broader issues
- More about those broader issues at OPSAWG
- “Side Meeting” Tuesday at 18:00