Constrained BRSKI

draft-ietf-anima-constrained-voucher-18

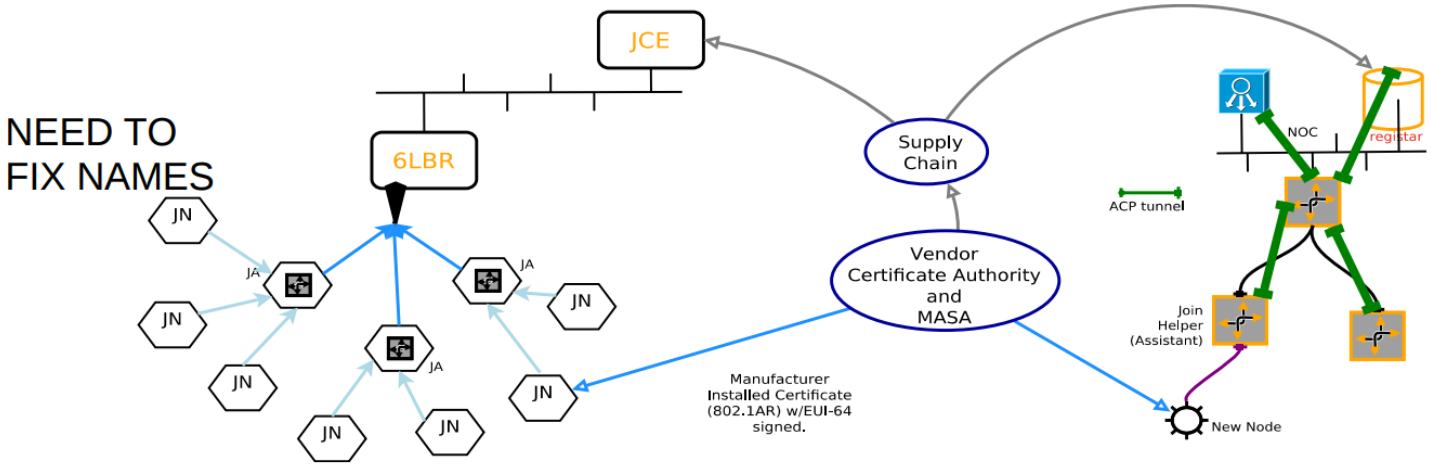
IETF 115, London, November 2022

M. Richardson
P. van der Stok
P. Kampanakis
E. Dijk (presenting)

Recap

- **Once upon a time, in London ...**
  - IETF 101 meeting – March 2018 – ANIMA WG

- **... there was a request for WG adoption of “Constrained Voucher”**



Recap

- **Goal: BRSKI device bootstrap solution for constrained devices & networks**
  - Suitable for wireless 6LoWPAN (802.15.4) mesh networks and other constrained networks.
  - CoAP and DTLS (instead of HTTPS)
  - COSE-signed CBOR (instead of CMS-signed JSON)
  - Constrained EST-coaps (instead of classic EST)
  - Minimize overhead of messages & options

Updates in version -16 (2022-02)

› **Clarified values for the "assertion" field** (derives from YANG enum)

Integer	Assertion Type
0	verified
1	logged
2	proximity

› **Editorial updates** (author review, consistent table formatting, ...)

› **Update of BRSKI Well-Known URI Sub-Registry** – adding a new column for 'short URI'

Updates in version -17 (2022-04)

- **Clarify how RFC 8995 is Amended**

- **Pledge IDevID security section added** in Security Considerations

Updates in version -18 (2022-07)

- **"application/voucher-cose+cbor“** Content Format assigned

- **Section 10 on discovery extensions added**
  - GRASP and CoAP discovery
  - DNS-SD discovery is kept for future work! (see list discussions)

- **Editorial updates** (e.g. reference updates, moving text around)

Implementations & Interop

- **Minerva.sandelman.ca**
  - Registrar – Fountain
  - MASA – Highway
  - Pledge (simulated) – Reach
- **IoTconsultancy.nl OpenThread Registrar fork**
  - includes Registrar, MASA, Pledge (simulated)
  - code for OpenThread embedded Pledge (not public)
  - aims for integration into an automated testing framework ~ also testing “out of spec” cases
  - using **Github issue tracker**
- **petervanderstok BRSKI**
  - and test MASA
- **Siemens-BT Registrar & MASA**

Demo

```
18:32:23.862 [:CoapEndpoint-DTLS-0.0.0.0:0#1] DEBUG org.eclipse.califo
removing Exchange[L3, complete] for token KeyToken[masa.iotconsultancy
18:32:23.862 [:CoapEndpoint-DTLS-0.0.0.0:0#1] DEBUG org.eclipse.califo
removing Exchange[L3, complete] for MID KeyMID[masa.iotconsultancy.nl:
18:32:23.863 [:CoapEndpoint-DTLS-0.0.0.0:0#1] DEBUG org.eclipse.califo
e] completed CON-POST   MID=39539, Token=F0CF11D1E2EC41FF, OptionSet={
known","est","sen"], "Content-Format":"unknown/286"},
30 81 ef 30 81 97 02 01 00 30 35 31 1e 30 1c 06 03 55 04 03 0c 15 54 65
20 49 6f 54 20 64 65 76 69 63 65 31 13 30 11 06 03 55 04 05 13 0a 41 38
30 59 30 13 06 07 2a 86 48 ce 3d 02 01 06 08 2a 86 48 ce 3d 03 01 07 03
c4 51 56 df 08 db 2b 0c 69 79 5a 65 bd 95 d5 5d 26 9b 33 aa 02 2f 9c 84
59 38 54 67 7a f2 86 a5 45 a1 5b 4c 83 ea 12 60 b3 cd 89 87 be f3 f2 a0
08 2a 86 48 ce 3d 04 03 02 03 47 00 30 44 02 20 40 cc fb de da 2a 88 08
7e 6d 64 95 9c e4 ec 63 9d 02 5c c1 1b 40 5b 2b 02 20 09 89 a6 46 c5 b4
98 f2 12 41 27 f7 2e f8 8b 51 0c 40 24 cf ba 82 d2 6b !
18:32:23.871 [main] INFO com.google.openthread.pledge.Pledge - enrolle
383644333330303031,CN=TestVendor IoT device
18:32:23.878 [main] INFO com.google.openthread.pledge.Pledge - operati
-----BEGIN CERTIFICATE-----
MIIBzjCCAXSgAwIBAgIBBDAKBggqhkjOPQQDAjBTMREwDwYDVQQDDAhkb21haW5j
YTETMBEGA1UECwwKT3BlblRocmVhZDEPMA0GA1UECgwGR29vZ2xlMQswCQYDVQQH
DAJTSDELMAkGA1UEBhMCQ04wHhcNMjIxMTAyMTczMjI0WhcNMjcxMTAxMTczMjI0
WjA1MR4wHAYDVQQDDBVUZXN0VmVuZG9yIElvVCBkZXZpY2UxEzARBgNVBAUTCkE4
NkQzMzAwMDEwwTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARNjWjDXcRRVt8I2ysM
aXlaZb2V1VOmmzOqAi+cjpU9zwxqTzJGWThUZ3ryhqVFoVtMg+oSYLPNiYe+8/Kg
CodzolcwVTAJBgNVHRMEAjAAMB8GA1UdIwQYMBaAFNUU4axOeBdnlnLWtSogECTz
GQveMCcGA1UdEQQgMB6gHAYJKwYBBAGC3yoBoA8WDVRlc3REb21haW5UQ0UwCgYI
KoZIzj0EAwIDSAAwRQIgSqrBTGHyY/YGGcplnW8KPqk1e2HKdpHZARzkk/iiWDYC
IQChg5KfRl+VJJhkZsmcXCBvmGB2BvSpds1WEC5mAcjKtA==
-----END CERTIFICATE-----

18:32:23.882 [main] INFO com.google.openthread.pledge.Pledge - operati
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIMlybVWVthxHj6naBmsn6vEsTwRbhx9ssiqFN6bhxFQ+oAoGCCqGSM49
AwEHoUQDQgAETY1ow13EUVbfCNsrDGl5WmW9ldVdJpszqgIvnI6VPc8Mak8yRlk4
VGd68oalRaFbTIPqEmCzzYmHvvPyoAqHcw==
-----END EC PRIVATE KEY-----

done
```

```
@Test
public void testMultiPledges() throws Exception {
  PledgeThread[] threads = new PledgeThread[12];

  // create multiple PledgeThreads, each with own Pledge and own credentials.
  for (int i = 0; i < threads.length; ++i) {
    threads[i] = new PledgeThread();
  }

  // run the Pledges
  for (PledgeThread thread : threads) {
    thread.start();
    Thread.sleep(20);
  }

  // wait for each Pledge to finish
  for (PledgeThread thread : threads) {
    try {
      thread.join();
      if (thread.errorState != null) {
        String msg =
            "Pledge [" + thread.getId() + "] had an exception/error: " + thread.errorState;
        logger.error(msg, thread.errorState);
        Assert.fail();
      }
    } catch (InterruptedException e) {
      Assert.fail("join failed: " + e.getMessage());
    }
  }
}
```

Open Issues aka Next Steps

- **https://github.com/anima-wg/constrained-voucher/issues**

- **12 document issues open**
  - (Issues labeled “future” or “interop” are not for the document)

- **Most important open issues**
  - Check all examples against interop running code! #237
  - Update discovery section to match new *draft-ietf-anima-constrained-join-proxy* #236
  - Optimize data size by excluding IDevID root CA cert? #239
    Open for discussion

Thank you!

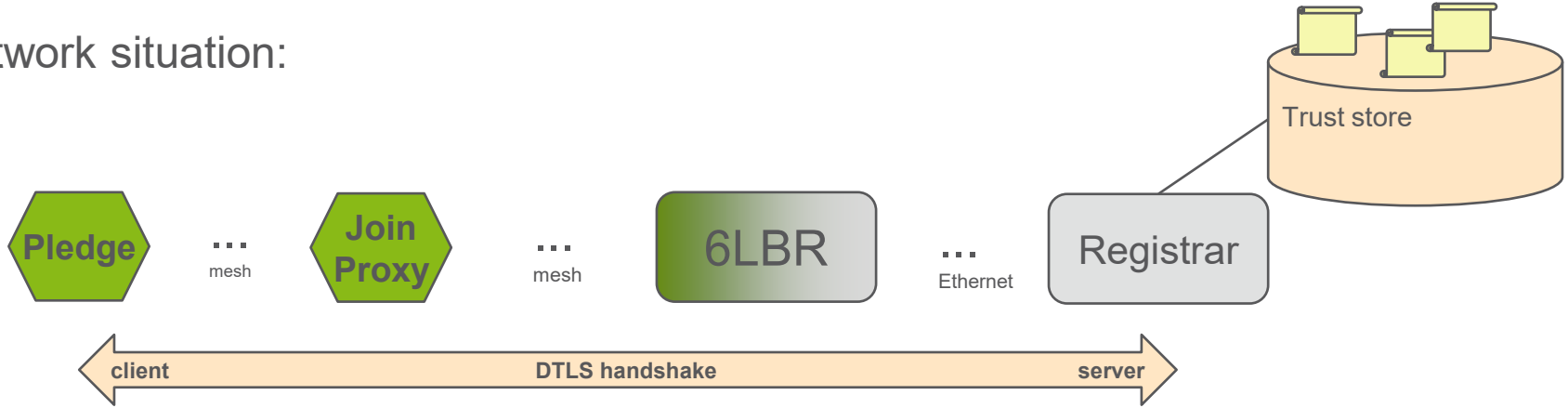
Comments/questions?

https://github.com/anima-wg/constrained-voucher/

Backup slides

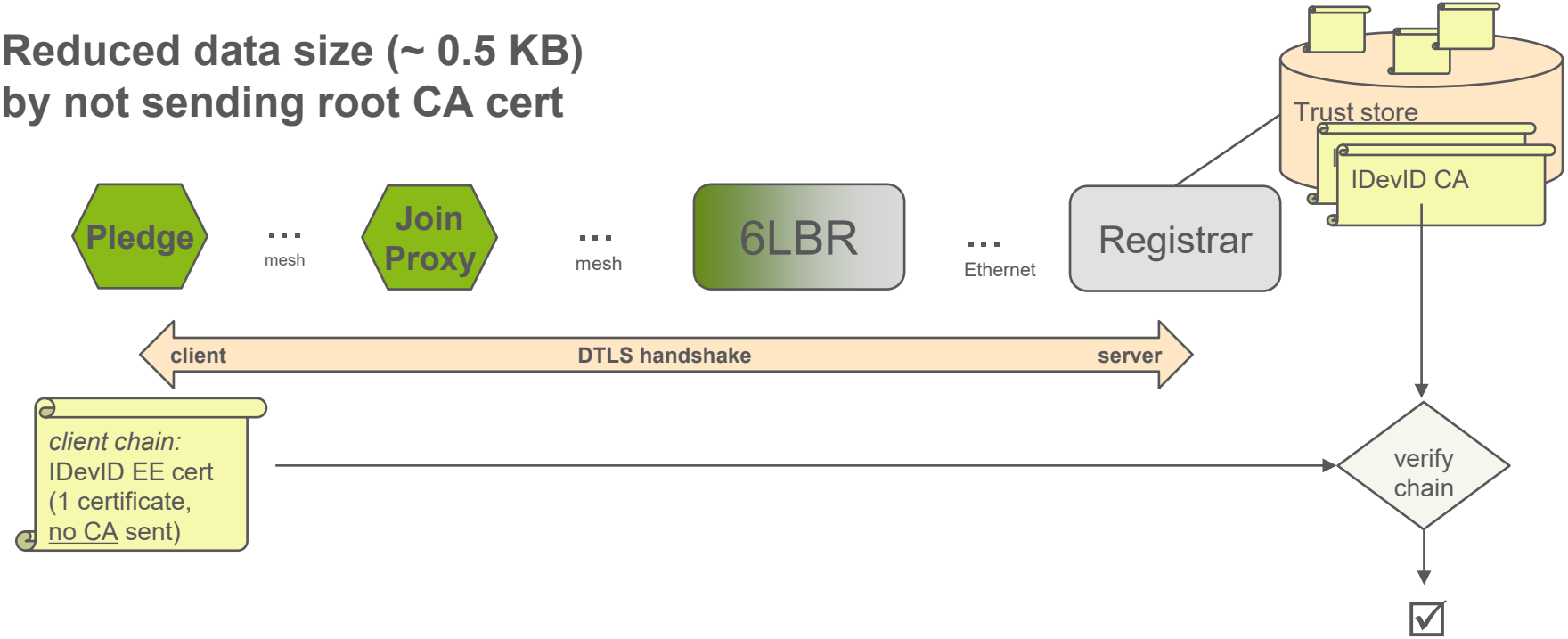
Optimize data size - exclude root CA cert?

› Network situation:



Optimize data size - exclude root CA cert?

› **Reduced data size (~ 0.5 KB) by not sending root CA cert**



› **BRSKI assumes Registrar has it already (to verify Pledge may join the Domain).**