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”
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)

<table>
<thead>
<tr>
<th>Integer</th>
<th>Assertion Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>verified</td>
</tr>
<tr>
<td>1</td>
<td>logged</td>
</tr>
<tr>
<td>2</td>
<td>proximity</td>
</tr>
</tbody>
</table>

- 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

```java
@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).