EST over coaps

Peter van der Stok, Sandeep Kumar, Panos Kampanakis
Martin Furuhed, ShahidRaza

IETF 98 - ACE Working Group
EST over coaps

Bootstrapping of Remote Secure Key Infrastructures (BRSKI) [ietf-anima-bootstrapping-keyinfra] uses Enrollment over Secure Transport (EST) [RFC7030]

Where EST is currently based on HTTP and TLS
This draft proposes CoAP and DTLS

to support secure bootstrapping of low resource devices
DTLS at transport is applied between pledge and EST server. Pledge and EST server exchange Certificates and Vouchers [ietf-anima-voucher].
Motivation

When *anima* takes off, Boxes with EST server and Registrar will be available.

Adding the CoAP/UDP interface to box:
- enables secure bootstrapping in low resource networks,
- removes need for http/coap proxy,
- equalizes treatment of low-resource and regular devices.
Contents

• Specify use of DTLS and CoAP Block with examples
• Conformance with ACE profiles

Differences with EST:
• No human (password) intervention
• No full PKI messages
• Extensions needed for BRSKI
• Discovery of path base: /est
• Payload formats “pkcsxx” use CBOR

Ongoing:
• Comparison with 6tisch approach: EDHOC, OSCOAP
Details

endpoints/resources: /application/.....

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>/cacerts</td>
<td>pkcs7-mime</td>
</tr>
<tr>
<td>/simpleenroll</td>
<td>pkcs7-mime pkcs10</td>
</tr>
<tr>
<td>/simplereenroll</td>
<td>pkcs7-mime pkcs10</td>
</tr>
<tr>
<td>/csrattrs</td>
<td>csrattrs</td>
</tr>
<tr>
<td>/serverkeygen</td>
<td>pkcs7-mime pkcs10 pkcs8</td>
</tr>
<tr>
<td>/requestvoucher</td>
<td>voucherrequest</td>
</tr>
<tr>
<td>/voucher_status</td>
<td>json</td>
</tr>
<tr>
<td>/enrollstatus</td>
<td>json</td>
</tr>
</tbody>
</table>

BRSKI endpoint
TODO

- Operational parameter values
- Appendix examples for all endpoints
- Security considerations
- And others.....