EST over coaps

Peter van der Stok, Sandeep Kumar, Panos Kampanakis
Martin Furuhed, Shahid Raza, Michael Richardson

IETF 100 - ACE Working Group
EST over coaps

Enrollment over Secure Transport (EST) [RFC7030] uses HTTP and TLS

This draft proposes CoAP and DTLS to support low resource devices

Application areas:
• Secure bootstrapping devices
• Distribution of identity (certificates) and keying material
Application areas

BRSKI also for 6tisch
Pledge and EST server exchange Certificates and Vouchers

BRSKI [anima]: Bootstrapping Remote Secure Key Infrastructures

Authenticated/authorized endpoint cert enrollment (and optionally key provisioning) through a CA or Registration Authority.
Current issues

- Proxying section too terse?
- Motivation of draft beyond BRSKI
- Many BRSKI extensions to support voucher transport
- Use of response codes 2.05 and 2.01
- Server side key generation using simple multipart encoding
- Combination of existing RFCs
- Content formats use binary encoding, no others
TODO

- Operational parameter values
- Change motivation section
- Add server-side key generation
- React to reviews
- And others.....
Next Steps

Ready for WG Draft?
Reminder
DTLS at transport is applied between pledge and EST server. Pledge and EST server exchange Certificates and Vouchers [ietf-anima-voucher].
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: e.g. /est
• Payload formats “pkcsxx” use binary
## Details

<table>
<thead>
<tr>
<th>Endpoints/Resources</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>/cacerts</td>
<td>pkcs7-mime</td>
</tr>
<tr>
<td>/simpleenroll</td>
<td>pkcs7-mime</td>
</tr>
<tr>
<td></td>
<td>pkcs10</td>
</tr>
<tr>
<td>/simplereenroll</td>
<td>pkcs7-mime</td>
</tr>
<tr>
<td></td>
<td>pkcs10</td>
</tr>
<tr>
<td>/csrattrs</td>
<td>csrattrs</td>
</tr>
<tr>
<td>/serverkeygen</td>
<td>pkcs7-mime</td>
</tr>
<tr>
<td></td>
<td>pkcs10</td>
</tr>
<tr>
<td></td>
<td>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