Constrained join proxy

Michael Richardson, Peter van der Stok, Panos Kampanakis

IETF 103 - ANIMA Working Group
Constrained join proxy

BRISKI uses EST, HTTP and TLS

This draft proposes
- Replacement of circuit proxy, using
- CoAP to support EST connection between pledge and EST server

Based on stateless part of kumar-dice-dtls-relay

EST: Enrollment over Secure Transport (RFC7030)
BRISKI: Bootstrapping of Remote Secure Key Infrastructures
CBOR: Concise Binary Object Representation (RFC 7049)
Graphic explanation

Keyinfra-16

HTTP TLS

pledge \(\xrightarrow{\text{Link-local}}\) Circuit proxy \(\xrightarrow{\text{global}}\) EST server

Constrained devices

COAP DTLS

pledge

\(\xrightarrow{\text{Link-local}}\) Join proxy \(\xrightarrow{\text{global}}\) EST server
Transport format

- Pledge L-L address
- JP L-L address
- DTLS payload

- J-P global address
- EST global address
- Pledge L-L address
- DTLS payload

Ct=287; CBOR array: [ct=60, [L-L IPv6, port, ident], ct=281, <DTLS encoded>]

c\text{t}=287: \text{application/multipart-core}; \text{ct}=60: \text{application/cbor};
c\text{t}=281: \text{application/pkcs7-mime}; \text{smime-type=certs-only}
## Draft relations

<table>
<thead>
<tr>
<th>Draft</th>
<th>WG</th>
<th>uses</th>
<th>extends</th>
</tr>
</thead>
<tbody>
<tr>
<td>BRSKI</td>
<td>ANIMA</td>
<td>HTTP/TLS EST CMS</td>
<td>EST with Voucher requests MASA Circuit proxy</td>
</tr>
<tr>
<td>EST-coaps</td>
<td>ACE</td>
<td>CoAP/DTLS EST</td>
<td>EST with coap/dtls</td>
</tr>
<tr>
<td>Voucher</td>
<td>ANIMA</td>
<td>YANG/JSON CMS</td>
<td>BRSKI with voucher spec</td>
</tr>
<tr>
<td>Constrained voucher</td>
<td>ANIMA</td>
<td>YANG/CBOR Voucher COSE/CMS/CBOR</td>
<td>Voucher with 2 fields BRSKI with COSE/CBOR and SID BRSKI with CMS/CBOR and SID</td>
</tr>
<tr>
<td>Constrained Join-proxy</td>
<td>ANIMA?</td>
<td>CBOR multipart-ct draft</td>
<td>BRSKI with constrained join proxy</td>
</tr>
</tbody>
</table>
TODO

- Update example payloads
- Improve/extend discovery text
- Hope for comments

Question

Interesting to ANIMA?