Constrained join proxy
draft-vanderstok-anima-constrained-join-proxy-02

Michael Richardson, Peter van der Stok, Panos Kampanakis

IETF 105 - ANIMA Working Group
Constrained join proxy

BRSKI uses HTTP and TLS

This draft proposes
- Replacement of circuit proxy, using
- CoAP and DTLS to support connection between Pledge and Domain Registrar

Based on kumar-dice-dtls-relay

EST: Enrollment over Secure Transport (RFC7030)
BRSKI: Bootstrapping of Remote Secure Key Infrastructures
Graphic explanation

BRSKI-22

pledge

Link-local

Circuit proxy

Global/ANI

Domain Registrar

HTTP TLS

Constrained devices

pledge

Link-local

Join proxy

Global/ANI

Domain Registrar

COAP DTLS
State-full $\leftrightarrow$ State-less

Assumption:
Join Proxy discovers (knows) address of Domain Registrar
Pledge discovers address of Join Proxy

State-full:
Join Proxy stores link-local address and port of pledge
(a form of NAT66)

State-less:
Link-local address and port of pledge encapsulated in the request
Discovery

Pledge discovers Join Proxy

- Mesh: coap discovery
- 6tisch: enhanced beacon

Join Proxy discovers Domain Registrar

- ANI: GRASP
- NOT ANI: coap discovery
Packet Format

Stateless
State-less packet uses mediatype: application/multipart-core between Join Proxy and Domain Registrar

draft-ietf-core-multipart-ct-03

header

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

multpart-core

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

pledge

Link-local

Join proxy

Global/ANI

Domain Registrar

Diagnostic CBOR of Multipart-core payload:

[ 60, [IP_p, p_P, ident], cf-EST, h'DTLS-content']
## 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 CMSS</td>
<td>EST with Voucher requests MASA Circuit proxy</td>
</tr>
<tr>
<td>EST-coaps</td>
<td>ACE</td>
<td>CoAP/DTLS EST multipart-ct draft</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 and EST-coaps</td>
</tr>
</tbody>
</table>
TODO

• Hope for comments

Question

Interesting to ANIMA?