Constrained voucher

Michael Richardson, Peter van der Stok, Panos Kampanakis

IETF 102 - ANIMA Working Group
Constrained voucher

BRSKI uses EST, HTTP and TLS

This draft proposes
• constrained voucher additions to voucher and use of SIDs
• CoAP, CBOR, CMS, and COSE
to support voucher transport for constrained devices

EST: Enrollment over Secure Transport
BRSKI: Bootstrapping of Remote Secure Key Infrastructures
SID: YANG Schema Item iDentifier
COSE: CBOR Signing and Encryption (RFC 8152)
CMS: Cryptographic message Syntax (RFC 5652)
CBOR: Concise Binary Object Representation (RFC 7049)
Major progress

- CMS and COSE media types
- SID definition
- YANG modules
## 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 Join proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EST with coap/dtls</td>
<td></td>
</tr>
<tr>
<td>EST-coaps</td>
<td>ACE</td>
<td>CoAP/DTLS EST</td>
<td></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>To be defined</td>
<td>BRSKI with constrained IPIP proxy</td>
</tr>
</tbody>
</table>

CMS/CBOR used for SDOs with CMS/pkcsxx investment
COSE/CBOR used for 6tisch
CMS and COSE media types

IANA registry:
This draft specifies the media types and the content formats for coap

<table>
<thead>
<tr>
<th>Media type</th>
<th>mime type</th>
<th>Encoding</th>
<th>ID</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>application/voucher-cms+cbor</td>
<td>- -</td>
<td>CBOR</td>
<td>TBD2</td>
<td>[This RFC]</td>
</tr>
<tr>
<td>application/voucher-cose+cbor</td>
<td>&quot;COSE-Sign1&quot;</td>
<td>CBOR</td>
<td>TBD3</td>
<td>[This RFC]</td>
</tr>
</tbody>
</table>
SID definitions

SID is number assigned to YANG identifier
SIDs are registered (unique to YANG modules and identifiers)
They significantly reduce payload size

"assignment-ranges": [  
{  
   "entry-point": 1001100,  
   "size": 50  
  }  
],  
"module-name": "ietf-constrained-voucher",  
"module-revision": "2017-12-11",  
"items": [  
{  
   "namespace": "module",  
   "identifier": "ietf-constrained-voucher",  
   "sid": 1001100  
  },  
{  
   "namespace": "data",  
   "identifier": "/ietf-constrained-voucher:voucher",  
   "sid": 1001101  
  }
],

SID: YANG Schema Item iDentifier
TODO

- Update example payloads
- Prepare interop