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

Draft	WG	uses	extends
BRSKI	ANIMA	HTTP/TLS EST CMS	EST with Voucher requests MASA Join proxy
EST-coaps	ACE	CoAP/DTLS EST	EST with coap/dtls
Voucher	ANIMA	YANG/JSON CMS	BRSKI with voucher spec
Constrained voucher	ANIMA	YANG/CBOR Voucher COSE/CMS/CBOR	Voucher with 2 fields BRSKI with COSE/CBOR and SID BRSKI with CMS/CBOR and SID
Constrained Join-proxy	ANIMA?	To be defined	BRSKI with constrained IPIP proxy

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

Media type	mime type	Encoding	ID	Reference
application/voucher-cms+cbor	- -	CBOR	TBD2	[This RFC]
application/voucher-cose+cbor	"COSE-Sign1"	CBOR	TBD3	[This RFC]

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