Constrained Voucher

BRSKI: Bootstrapping of Remote Secure Key Infrastructures

This draft proposes:

- Constrained voucher additions to voucher and use of SIDs
- Extends CoAP-EST draft with BRSKI extensions to EST
- 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 Identifier
COSE: CBOR Signing and Encryption (RFC 8152)
CMS: Cryptographic message Syntax (RFC 5652)
CBOR: Concise Binary Object Representation (RFC 7049)
Changes since IETF112

- Many small edits
  - IANA fixes
- Fixes to examples.
- Added table for mapping of assertion values to integers (not strings)
- Interop efforts
Hackathon Results

• IETF113 interop testing, online and via IETF VPN. In the weeks up to meeting.
  • Participants: Esko (IOT-Consultancy), Peter, Michael (Sandelman), Thomas (Siemens),
    - Will repeat at next Hackathon, but also participants want to continue between events.
    - IETF L2 VPN (used)
  • Same cats as last time, different bugs
List of Hackathon Issues (1)

• Still need **Early Allocation of TBD3** - previous efforts used 65502 (private use value) for Content-Format

• SNI must be used for Registrar/MASA connection
• still have to get AuthorityKeyIdentifier correct for IDevID

Much external distraction to participants
• in-room, right-now, right-here work is superior to vague on-line efforts
Discussion

Ready for WGLC!

Thanks to weekly discussions in BRSKI design team on Thursday
Will resume in April