Constrained voucher

draft-ietf-anima-constrained-voucher-14

Michael Richardson, Peter van der Stok,
Panos Kampanakis, Esko Dijk

IETF 112
ANIMA Working Group

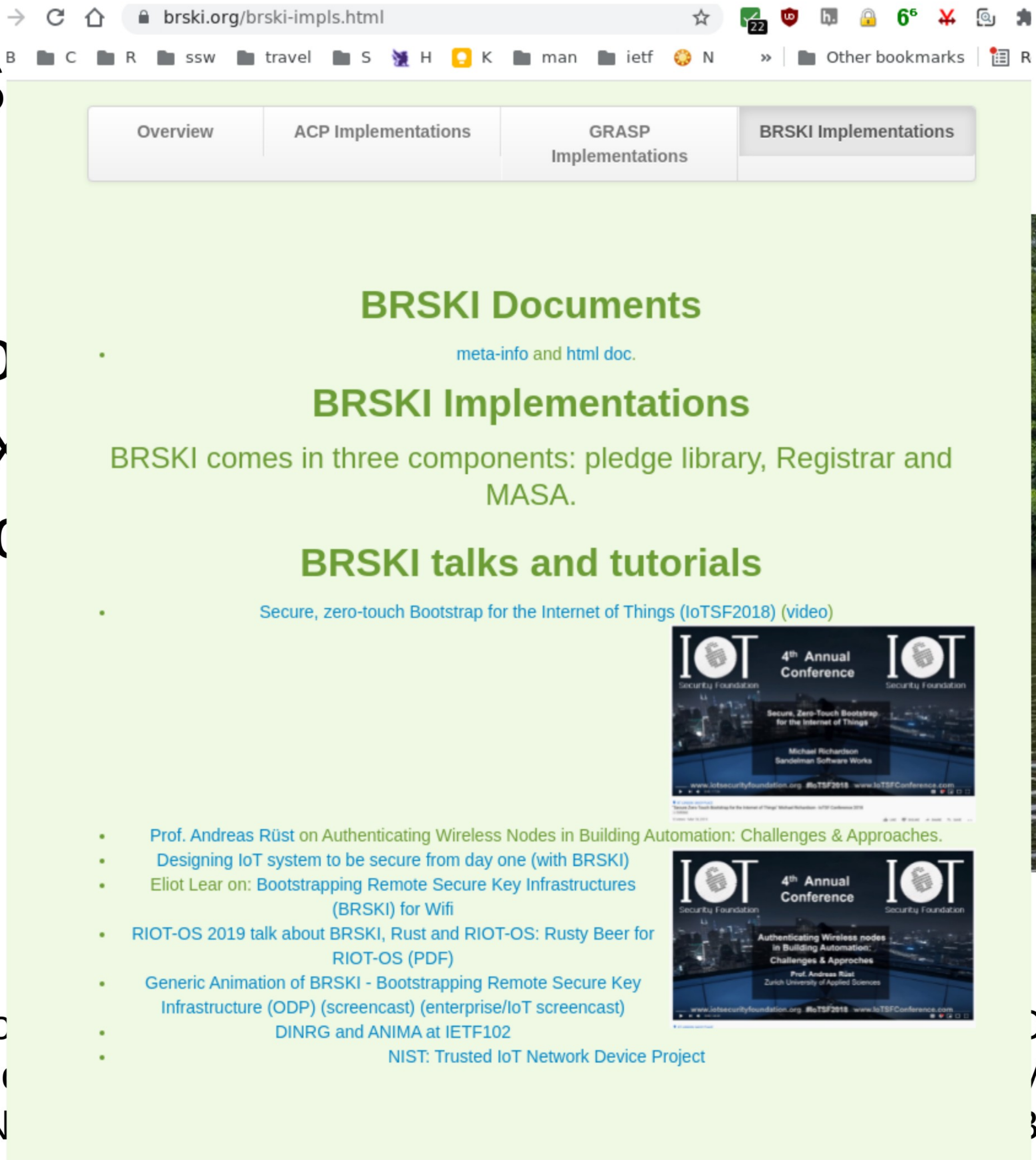
Constrained Voucher

BRS

This

- co
- Ex
- Co

s



BRSKI Documents

- meta-info and html doc.

BRSKI Implementations

BRSKI comes in three components: pledge library, Registrar and MASA.

BRSKI talks and tutorials

- Secure, zero-touch Bootstrap for the Internet of Things (IoTSF2018) (video)

- Prof. Andreas Rüst on Authenticating Wireless Nodes in Building Automation: Challenges & Approaches.
- Designing IoT system to be secure from day one (with BRSKI)
- Eliot Lear on: Bootstrapping Remote Secure Key Infrastructures (BRSKI) for Wifi
- RIOT-OS 2019 talk about BRSKI, Rust and RIOT-OS: Rusty Beer for RIOT-OS (PDF)
- Generic Animation of BRSKI - Bootstrapping Remote Secure Key Infrastructure (ODP) (screencast) (enterprise/IoT screencast)
- DINRG and ANIMA at IETF102
- NIST: Trusted IoT Network Device Project

IoT Security Foundation
4th Annual Conference
Authenticating Wireless nodes in Building Automation: Challenges & Approches
Prof. Andreas Rüst
Zurich University of Applied Sciences

EST: Enro
BRSKI: B
SID: YAN

SE: CBOR Signing and Encryption (RFC 8152)
MS: Cryptographic message Syntax (RFC 5652)
BOR: Concise Binary Object Representation (RFC 7049)

Changes since IETF111

- Changes since version 13
- Clarify what the Updates are
- Much expanded BRSKI-EST section
- Some errors in SID allocation
- 17 issues open
  - (83 closed)
  - All review comments closed
- Security Considerations completed
- Added section on what to implement in specific Deployments
- Considered what to do if yang-cbor documents do not progress

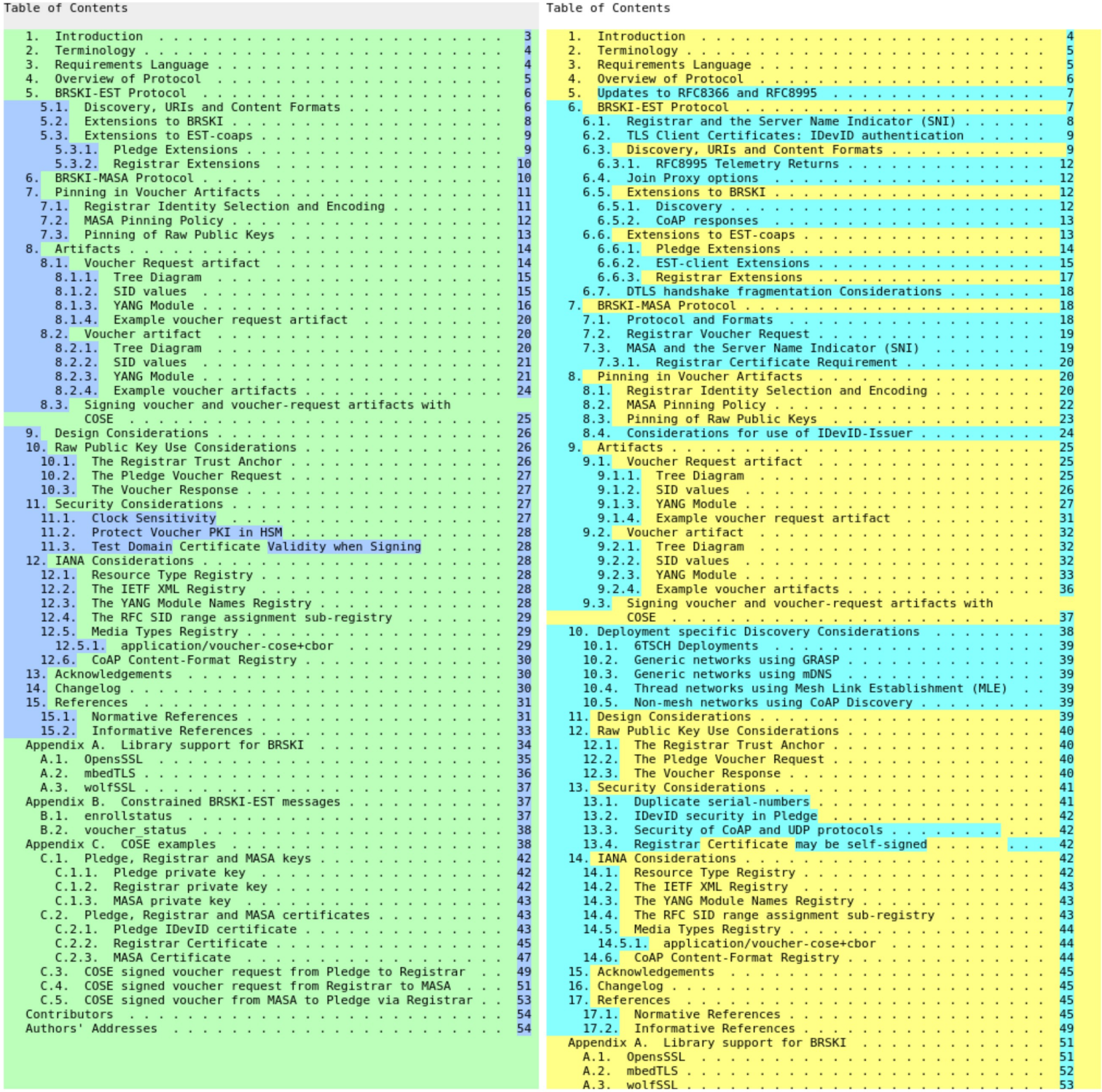


Table of Contents

```
   1.  Introduction  . . . . . . . . . . . . . . . . . . . . . . .   3
   2.  Terminology . . . . . . . . . . . . . . . . . . . . . . . .   4
   3.  Requirements Language . . . . . . . . . . . . . . . . . . .   4
   4.  Overview of Protocol  . . . . . . . . . . . . . . . . . . .   5
   5.  BRSKI-EST Protocol  . . . . . . . . . . . . . . . . . . . .   6
     5.1.  Discovery, URIs and Content Formats . . . . . . . . . .   6
     5.2.  Extensions to BRSKI . . . . . . . . . . . . . . . . . .   8
     5.3.  Extensions to EST-coaps . . . . . . . . . . . . . . . .   9
       5.3.1.  Pledge Extensions . . . . . . . . . . . . . . . . .   9
       5.3.2.  Registrar Extensions  . . . . . . . . . . . . . . .  10
   6.  BRSKI-MASA Protocol . . . . . . . . . . . . . . . . . . . .  10
   7.  Pinning in Voucher Artifacts  . . . . . . . . . . . . . . .  11
     7.1.  Registrar Identity Selection and Encoding . . . . . . .  11
     7.2.  MASA Pinning Policy . . . . . . . . . . . . . . . . . .  12
     7.3.  Pinning of Raw Public Keys  . . . . . . . . . . . . . .  13
   8.  Artifacts . . . . . . . . . . . . . . . . . . . . . . . . .  14
     8.1.  Voucher Request artifact  . . . . . . . . . . . . . . .  14
       8.1.1.  Tree Diagram  . . . . . . . . . . . . . . . . . . .  15
       8.1.2.  SID values  . . . . . . . . . . . . . . . . . . . .  15
       8.1.3.  YANG Module . . . . . . . . . . . . . . . . . . . .  16
       8.1.4.  Example voucher request artifact  . . . . . . . . .  20
     8.2.  Voucher artifact  . . . . . . . . . . . . . . . . . . .  20
       8.2.1.  Tree Diagram  . . . . . . . . . . . . . . . . . . .  20
       8.2.2.  SID values  . . . . . . . . . . . . . . . . . . . .  21
       8.2.3.  YANG Module . . . . . . . . . . . . . . . . . . . .  21
       8.2.4.  Example voucher artifacts . . . . . . . . . . . . .  24
     8.3.  Signing voucher and voucher-request artifacts with
           COSE  . . . . . . . . . . . . . . . . . . . . . . . . .  25
   9.  Design Considerations . . . . . . . . . . . . . . . . . . .  26
   10. Raw Public Key Use Considerations . . . . . . . . . . . . .  26
     10.1.  The Registrar Trust Anchor . . . . . . . . . . . . . .  26
     10.2.  The Pledge Voucher Request . . . . . . . . . . . . . .  27
     10.3.  The Voucher Response . . . . . . . . . . . . . . . . .  27
   11. Security Considerations . . . . . . . . . . . . . . . . . .  27
     11.1.  Clock Sensitivity  . . . . . . . . . . . . . . . . . .  27
     11.2.  Protect Voucher PKI in HSM . . . . . . . . . . . . . .  28
     11.3.  Test Domain Certificate Validity when Signing  . . . .  28
   12. IANA Considerations . . . . . . . . . . . . . . . . . . . .  28
     12.1.  Resource Type Registry . . . . . . . . . . . . . . . .  28
     12.2.  The IETF XML Registry  . . . . . . . . . . . . . . . .  28
     12.3.  The YANG Module Names Registry . . . . . . . . . . . .  28
     12.4.  The RFC SID range assignment sub-registry  . . . . . .  29
     12.5.  Media Types Registry . . . . . . . . . . . . . . . . .  29
       12.5.1.  application/voucher-cose+cbor  . . . . . . . . . .  29
     12.6.  CoAP Content-Format Registry . . . . . . . . . . . . .  30
   13. Acknowledgements  . . . . . . . . . . . . . . . . . . . . .  30
   14. Changelog . . . . . . . . . . . . . . . . . . . . . . . . .  30
   15. References  . . . . . . . . . . . . . . . . . . . . . . . .  31
     15.1.  Normative References . . . . . . . . . . . . . . . . .  31
     15.2.  Informative References . . . . . . . . . . . . . . . .  33
   Appendix A.  Library support for BRSKI  . . . . . . . . . . . .  34
     A.1.  OpensSSL  . . . . . . . . . . . . . . . . . . . . . . .  35
     A.2.  mbedTLS . . . . . . . . . . . . . . . . . . . . . . . .  36
     A.3.  wolfSSL . . . . . . . . . . . . . . . . . . . . . . . .  37
   Appendix B.  Constrained BRSKI-EST messages . . . . . . . . . .  37
     B.1.  enrollstatus  . . . . . . . . . . . . . . . . . . . . .  37
     B.2.  voucher_status  . . . . . . . . . . . . . . . . . . . .  38
   Appendix C.  COSE examples  . . . . . . . . . . . . . . . . . .  38
     C.1.  Pledge, Registrar and MASA keys . . . . . . . . . . . .  42
       C.1.1.  Pledge private key  . . . . . . . . . . . . . . . .  42
       C.1.2.  Registrar private key . . . . . . . . . . . . . . .  42
       C.1.3.  MASA private key  . . . . . . . . . . . . . . . . .  43
     C.2.  Pledge, Registrar and MASA certificates . . . . . . . .  43
       C.2.1.  Pledge IDevID certificate . . . . . . . . . . . . .  43
       C.2.2.  Registrar Certificate . . . . . . . . . . . . . . .  45
       C.2.3.  MASA Certificate  . . . . . . . . . . . . . . . . .  47
     C.3.  COSE signed voucher request from Pledge to Registrar  .  49
     C.4.  COSE signed voucher request from Registrar to MASA  . .  51
     C.5.  COSE signed voucher from MASA to Pledge via Registrar .  53
   Contributors  . . . . . . . . . . . . . . . . . . . . . . . . .  54
   Authors' Addresses  . . . . . . . . . . . . . . . . . . . . . .  54
```

Table of Contents

```
   1.  Introduction  . . . . . . . . . . . . . . . . . . . . . . .   4
   2.  Terminology . . . . . . . . . . . . . . . . . . . . . . . .   5
   3.  Requirements Language . . . . . . . . . . . . . . . . . . .   5
   4.  Overview of Protocol  . . . . . . . . . . . . . . . . . . .   6
   5.  Updates to RFC8366 and RFC8995  . . . . . . . . . . . . . .   7
   6.  BRSKI-EST Protocol  . . . . . . . . . . . . . . . . . . . .   7
     6.1.  Registrar and the Server Name Indicator (SNI) . . . . .   8
     6.2.  TLS Client Certificates: IDevID authentication  . . . .   9
     6.3.  Discovery, URIs and Content Formats . . . . . . . . . .   9
       6.3.1.  RFC8995 Telemetry Returns . . . . . . . . . . . . .  12
     6.4.  Join Proxy options  . . . . . . . . . . . . . . . . . .  12
     6.5.  Extensions to BRSKI . . . . . . . . . . . . . . . . . .  12
       6.5.1.  Discovery . . . . . . . . . . . . . . . . . . . . .  12
       6.5.2.  CoAP responses  . . . . . . . . . . . . . . . . . .  13
     6.6.  Extensions to EST-coaps . . . . . . . . . . . . . . . .  13
       6.6.1.  Pledge Extensions . . . . . . . . . . . . . . . . .  14
       6.6.2.  EST-client Extensions . . . . . . . . . . . . . . .  15
       6.6.3.  Registrar Extensions  . . . . . . . . . . . . . . .  17
     6.7.  DTLS handshake fragmentation Considerations . . . . . .  18
   7.  BRSKI-MASA Protocol . . . . . . . . . . . . . . . . . . . .  18
     7.1.  Protocol and Formats  . . . . . . . . . . . . . . . . .  18
     7.2.  Registrar Voucher Request . . . . . . . . . . . . . . .  19
     7.3.  MASA and the Server Name Indicator (SNI)  . . . . . . .  19
       7.3.1.  Registrar Certificate Requirement . . . . . . . . .  20
   8.  Pinning in Voucher Artifacts  . . . . . . . . . . . . . . .  20
     8.1.  Registrar Identity Selection and Encoding . . . . . . .  20
     8.2.  MASA Pinning Policy . . . . . . . . . . . . . . . . . .  22
     8.3.  Pinning of Raw Public Keys  . . . . . . . . . . . . . .  23
     8.4.  Considerations for use of IDevID-Issuer . . . . . . . .  24
   9.  Artifacts . . . . . . . . . . . . . . . . . . . . . . . . .  25
     9.1.  Voucher Request artifact  . . . . . . . . . . . . . . .  25
       9.1.1.  Tree Diagram  . . . . . . . . . . . . . . . . . . .  25
       9.1.2.  SID values  . . . . . . . . . . . . . . . . . . . .  26
       9.1.3.  YANG Module . . . . . . . . . . . . . . . . . . . .  27
       9.1.4.  Example voucher request artifact  . . . . . . . . .  31
     9.2.  Voucher artifact  . . . . . . . . . . . . . . . . . . .  32
       9.2.1.  Tree Diagram  . . . . . . . . . . . . . . . . . . .  32
       9.2.2.  SID values  . . . . . . . . . . . . . . . . . . . .  32
       9.2.3.  YANG Module . . . . . . . . . . . . . . . . . . . .  33
       9.2.4.  Example voucher artifacts . . . . . . . . . . . . .  36
     9.3.  Signing voucher and voucher-request artifacts with
           COSE  . . . . . . . . . . . . . . . . . . . . . . . . .  37
   10. Deployment specific Discovery Considerations  . . . . . . .  38
     10.1.  6TSCH Deployments  . . . . . . . . . . . . . . . . . .  39
     10.2.  Generic networks using GRASP . . . . . . . . . . . . .  39
     10.3.  Generic networks using mDNS  . . . . . . . . . . . . .  39
     10.4.  Thread networks using Mesh Link Establishment (MLE)  .  39
     10.5.  Non-mesh networks using CoAP Discovery . . . . . . . .  39
   11. Design Considerations . . . . . . . . . . . . . . . . . . .  39
   12. Raw Public Key Use Considerations . . . . . . . . . . . . .  40
     12.1.  The Registrar Trust Anchor . . . . . . . . . . . . . .  40
     12.2.  The Pledge Voucher Request . . . . . . . . . . . . . .  40
     12.3.  The Voucher Response . . . . . . . . . . . . . . . . .  40
   13. Security Considerations . . . . . . . . . . . . . . . . . .  41
     13.1.  Duplicate serial-numbers . . . . . . . . . . . . . . .  41
     13.2.  IDevID security in Pledge  . . . . . . . . . . . . . .  42
     13.3.  Security of CoAP and UDP protocols . . . . . . . . . .  42
     13.4.  Registrar Certificate may be self-signed . . . . . . .  42
   14. IANA Considerations . . . . . . . . . . . . . . . . . . . .  42
     14.1.  Resource Type Registry . . . . . . . . . . . . . . . .  42
     14.2.  The IETF XML Registry  . . . . . . . . . . . . . . . .  43
     14.3.  The YANG Module Names Registry . . . . . . . . . . . .  43
     14.4.  The RFC SID range assignment sub-registry  . . . . . .  43
     14.5.  Media Types Registry . . . . . . . . . . . . . . . . .  44
       14.5.1.  application/voucher-cose+cbor  . . . . . . . . . .  44
     14.6.  CoAP Content-Format Registry . . . . . . . . . . . . .  44
   15. Acknowledgements  . . . . . . . . . . . . . . . . . . . . .  45
   16. Changelog . . . . . . . . . . . . . . . . . . . . . . . . .  45
   17. References  . . . . . . . . . . . . . . . . . . . . . . . .  45
     17.1.  Normative References . . . . . . . . . . . . . . . . .  45
     17.2.  Informative References . . . . . . . . . . . . . . . .  49
   Appendix A.  Library support for BRSKI  . . . . . . . . . . . .  51
     A.1.  OpensSSL  . . . . . . . . . . . . . . . . . . . . . . .  51
     A.2.  mbedTLS . . . . . . . . . . . . . . . . . . . . . . . .  52
     A.3.  wolfSSL . . . . . . . . . . . . . . . . . . . . . . . .  53
```

Dependent upon CORE WG drafts - still in IESG review

yang-cbor/yang-sid design team formed to deal with review comments has had four meetings

- 18 issues still open (including a bunch of wontfix)
- 34 issues closed
- Design team includes Andy Bierman

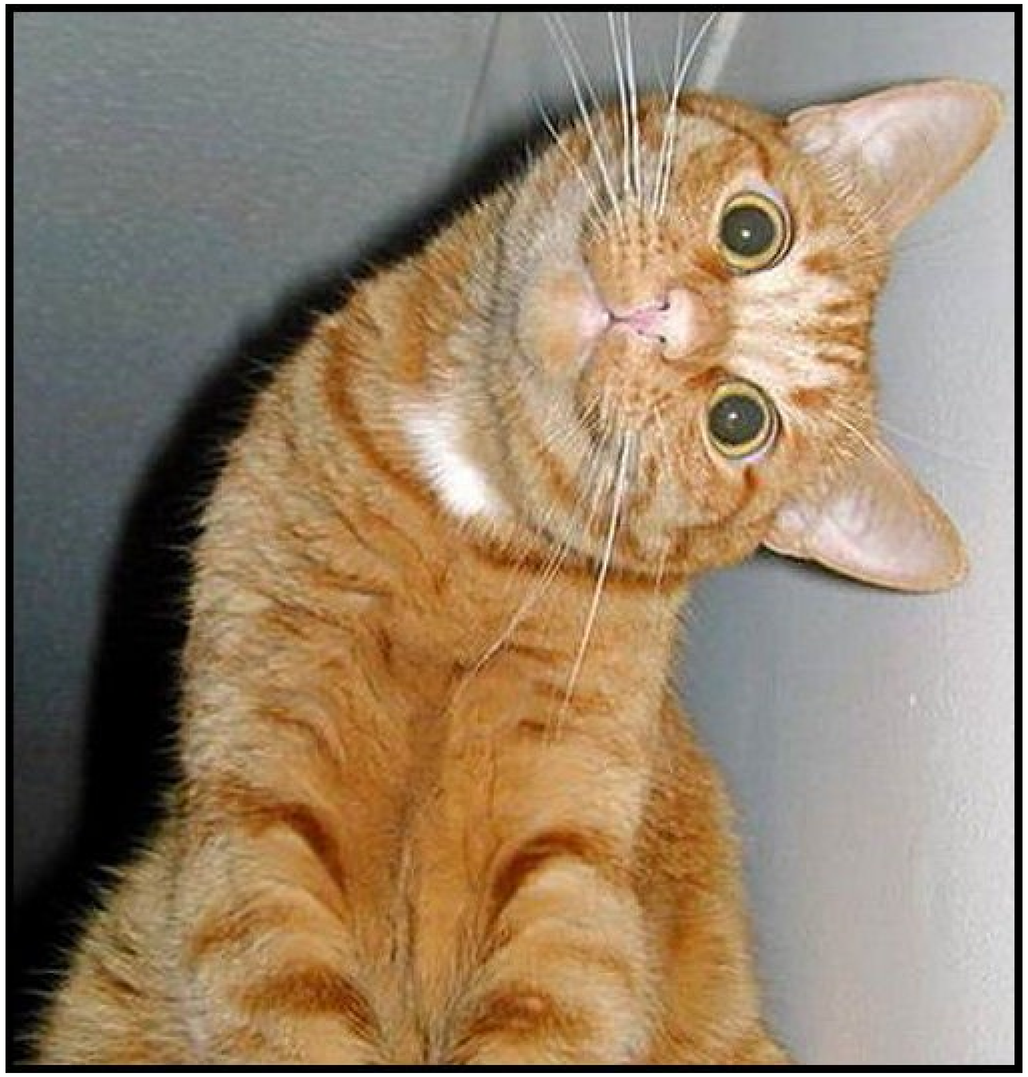
My recommendation to ANIMA constrained-voucher team is that the SID documents will get through IESG review before Xmas break

Hackathon Results

- IETF112 Hackathon Nov 1-5. Meet up in gather.town @ 14:00 UTC, at table A(NIMA).
- Not really any participants. I think people (me included!) are exhausted.
  - BUT: L2 VPN now working, and we will test asynchronously.
- NIST NCCoE IoT-onboarding
  - https://www.federalregister.gov/documents/2021/10/26/2021-23293/national-cybersecurity-center-of-excellence-nccoe-trusted-internet-of-things-iot-device

Discussion

-



Thanks to weekly discussions in BRSKI design team on Thursday
Next meeting Nov. 25

Conclusions

Three directorate reviews occurred and were reacted to.
Security Considerations is done.
Applicability Statement is done.

Ready for WGLC!

- no major issues
- Only minor issues remain, many of which are wishes