Constrained voucher

draft-ietf-anima-constrained-voucher-13

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

IETF 111
ANIMA Working Group

Constrained Voucher

BRSKI uses EST, HTTP and TLS

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 **S**chema **I**tem i**D**entifier

COSE: CBOR Signing and Encryption (RFC 8152)
CMS: Cryptographic message Syntax (RFC 5652)
CBOR: Concise Binary Object Representation (RFC 7049)

Constrained Voucher

BRSKI uses EST, HTTP and TLS

This draft proposes

- constrained voucher additions to
- Extends coap-est draft with BRSK
- CoAP, CBOR, CMS, and COSE

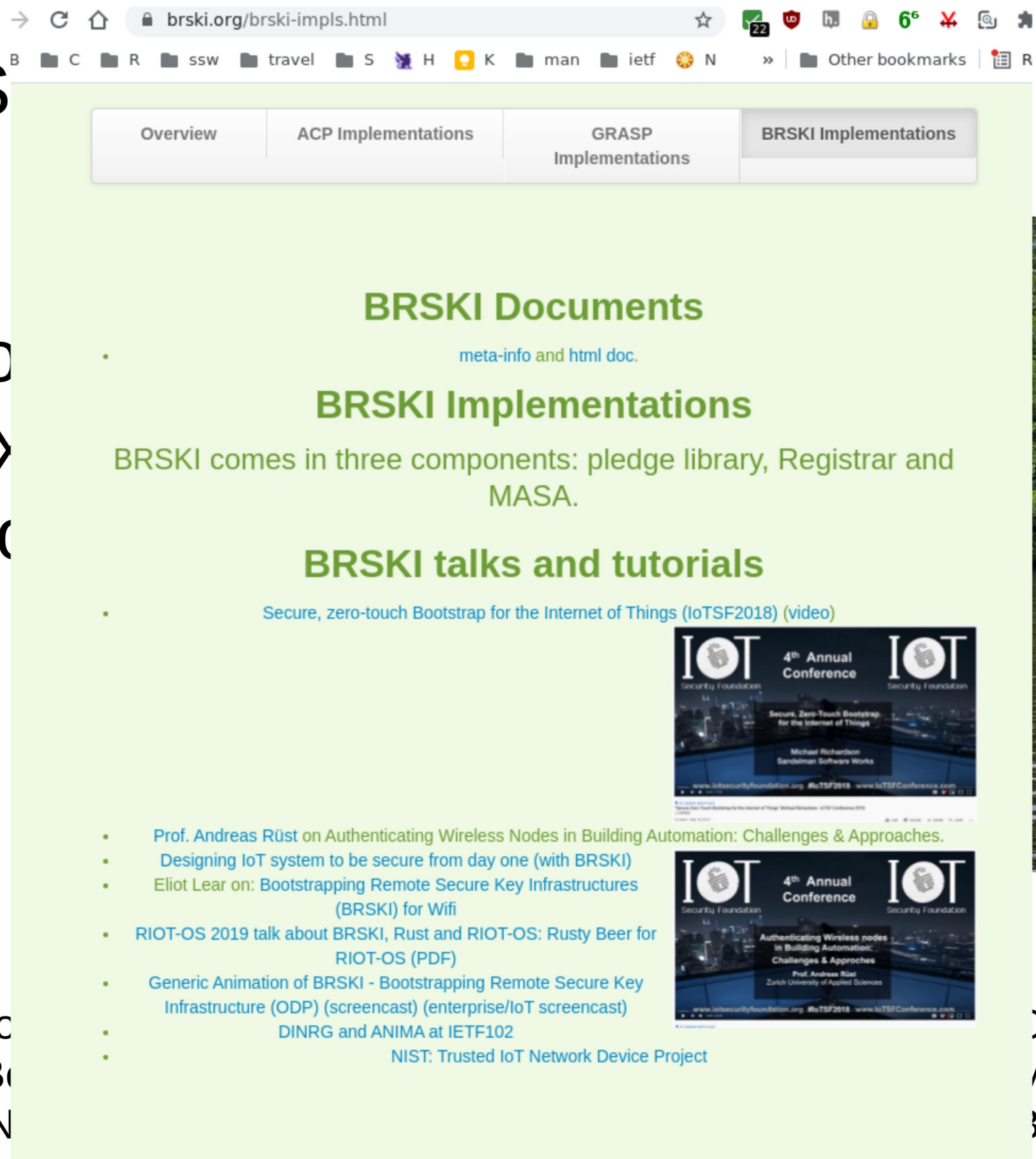
to support voucher transp s

EST: Enrollment over Secure Transport
BRSKI: Bootstrapping of Remote Secure Key Infrastructures
SID: YANG **S**chema **I**tem i**D**entifier

COSE: CBOR Signing and Encryption (RFC 8152)
CMS: Cryptographic message Syntax (RFC 5652)
CBOR: Concise Binary Object Representation (RFC 7049)

Constrained Voucher

BRS



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

This

- co
- Ex
- Co

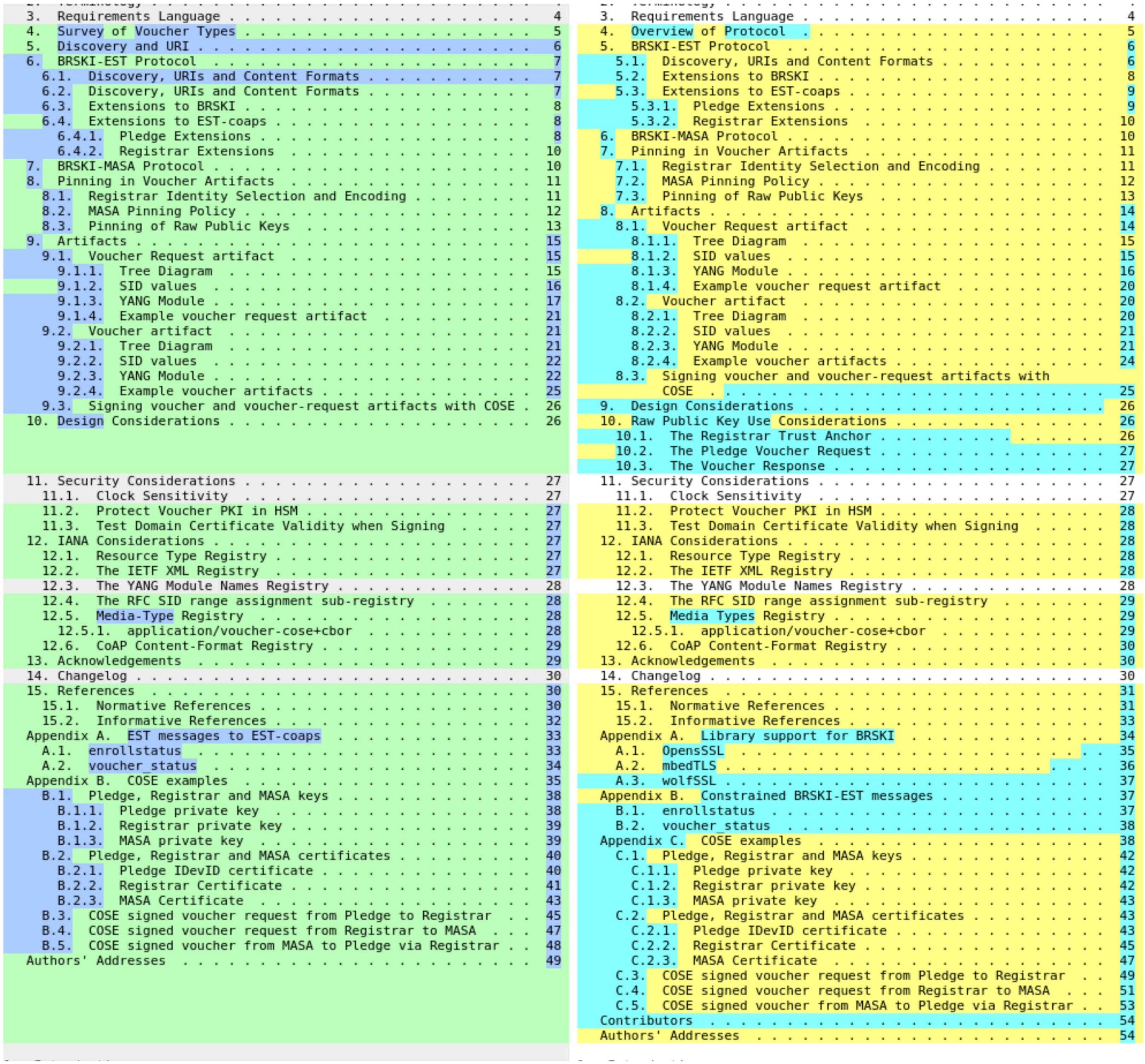
s

EST: Enro
BRSKI: Bo
SID: YAN

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

Changes since IETF110

- Changes since version 10.
- Raw Public Key Use Considerations
- Reference to published RFCs
- Three directorate reviews,
- 37 issues open
  - (47 closed)
- Hackathon IETF111
- Removed requirement to do Discovery.
- Removed requirement to get /cacerts if voucher pins needed trust anchor already
- More explanation of what to pin
  - Raw Public Key pinning
- Proximity-registrar-subject-public-key-info -> proximity-registrar-pubk
- Proposed to change module from ietf-cosntrained-voucher to ietf-voucher-constrained



```
   2.  Terminology . . . . . . . . . . . . . . . . . . . . . . . .
   3.  Requirements Language . . . . . . . . . . . . . . . . . . .   4
   4.  Survey of Voucher Types . . . . . . . . . . . . . . . . . .   5
   5.  Discovery and URI . . . . . . . . . . . . . . . . . . . . .   6
   6.  BRSKI-EST Protocol  . . . . . . . . . . . . . . . . . . . .   7
     6.1.  Discovery, URIs and Content Formats . . . . . . . . . .   7
     6.2.  Discovery, URIs and Content Formats . . . . . . . . . .   7
     6.3.  Extensions to BRSKI . . . . . . . . . . . . . . . . . .   8
     6.4.  Extensions to EST-coaps . . . . . . . . . . . . . . . .   8
       6.4.1.  Pledge Extensions . . . . . . . . . . . . . . . . .   8
       6.4.2.  Registrar Extensions  . . . . . . . . . . . . . . .  10
   7.  BRSKI-MASA Protocol . . . . . . . . . . . . . . . . . . . .  10
   8.  Pinning in Voucher Artifacts  . . . . . . . . . . . . . . .  11
     8.1.  Registrar Identity Selection and Encoding . . . . . . .  11
     8.2.  MASA Pinning Policy . . . . . . . . . . . . . . . . . .  12
     8.3.  Pinning of Raw Public Keys  . . . . . . . . . . . . . .  13
   9.  Artifacts . . . . . . . . . . . . . . . . . . . . . . . . .  15
     9.1.  Voucher Request artifact  . . . . . . . . . . . . . . .  15
       9.1.1.  Tree Diagram  . . . . . . . . . . . . . . . . . . .  15
       9.1.2.  SID values  . . . . . . . . . . . . . . . . . . . .  16
       9.1.3.  YANG Module . . . . . . . . . . . . . . . . . . . .  17
       9.1.4.  Example voucher request artifact  . . . . . . . . .  21
     9.2.  Voucher artifact  . . . . . . . . . . . . . . . . . . .  21
       9.2.1.  Tree Diagram  . . . . . . . . . . . . . . . . . . .  21
       9.2.2.  SID values  . . . . . . . . . . . . . . . . . . . .  22
       9.2.3.  YANG Module . . . . . . . . . . . . . . . . . . . .  22
       9.2.4.  Example voucher artifacts . . . . . . . . . . . . .  25
     9.3.  Signing voucher and voucher-request artifacts with COSE .  26
   10. Design Considerations . . . . . . . . . . . . . . . . . . .  26



   11. Security Considerations . . . . . . . . . . . . . . . . . .  27
     11.1.  Clock Sensitivity  . . . . . . . . . . . . . . . . . .  27
     11.2.  Protect Voucher PKI in HSM . . . . . . . . . . . . . .  27
     11.3.  Test Domain Certificate Validity when Signing  . . . .  27
   12. IANA Considerations . . . . . . . . . . . . . . . . . . . .  27
     12.1.  Resource Type Registry . . . . . . . . . . . . . . . .  27
     12.2.  The IETF XML Registry  . . . . . . . . . . . . . . . .  27
     12.3.  The YANG Module Names Registry . . . . . . . . . . . .  28
     12.4.  The RFC SID range assignment sub-registry  . . . . . .  28
     12.5.  Media-Type Registry  . . . . . . . . . . . . . . . . .  28
       12.5.1.  application/voucher-cose+cbor  . . . . . . . . . .  28
     12.6.  CoAP Content-Format Registry . . . . . . . . . . . . .  29
   13. Acknowledgements  . . . . . . . . . . . . . . . . . . . . .  29
   14. Changelog . . . . . . . . . . . . . . . . . . . . . . . . .  30
   15. References  . . . . . . . . . . . . . . . . . . . . . . . .  30
     15.1.  Normative References . . . . . . . . . . . . . . . . .  30
     15.2.  Informative References . . . . . . . . . . . . . . . .  32
   Appendix A.  EST messages to EST-coaps  . . . . . . . . . . . .  33
     A.1.  enrollstatus  . . . . . . . . . . . . . . . . . . . . .  33
     A.2.  voucher_status  . . . . . . . . . . . . . . . . . . . .  34
   Appendix B.  COSE examples  . . . . . . . . . . . . . . . . . .  35
     B.1.  Pledge, Registrar and MASA keys . . . . . . . . . . . .  38
       B.1.1.  Pledge private key  . . . . . . . . . . . . . . . .  38
       B.1.2.  Registrar private key . . . . . . . . . . . . . . .  39
       B.1.3.  MASA private key  . . . . . . . . . . . . . . . . .  39
     B.2.  Pledge, Registrar and MASA certificates . . . . . . . .  40
       B.2.1.  Pledge IDevID certificate . . . . . . . . . . . . .  40
       B.2.2.  Registrar Certificate . . . . . . . . . . . . . . .  41
       B.2.3.  MASA Certificate  . . . . . . . . . . . . . . . . .  43
     B.3.  COSE signed voucher request from Pledge to Registrar  . .  45
     B.4.  COSE signed voucher request from Registrar to MASA  . . .  47
     B.5.  COSE signed voucher from MASA to Pledge via Registrar . .  48
   Authors' Addresses  . . . . . . . . . . . . . . . . . . . . . .  49
```

```
   2.  Terminology . . . . . . . . . . . . . . . . . . . . . . . .
   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
```

https://www.ietf.org/rfcdiff?url1=draft-ietf-anima-constrained-voucher-10&url2=https://raw.githubusercontent.com/anima-wg/constrained-voucher/master/constrained-voucher-13.txt

Name of the module: ietf-voucher-constrained

ietf-constrained-voucher ->
ietf-voucher-constrained

No effect on running code
Because they are all encoded
Using SID values

ietf-constrained-voucher-request ->
ietf-voucher-request-constrained

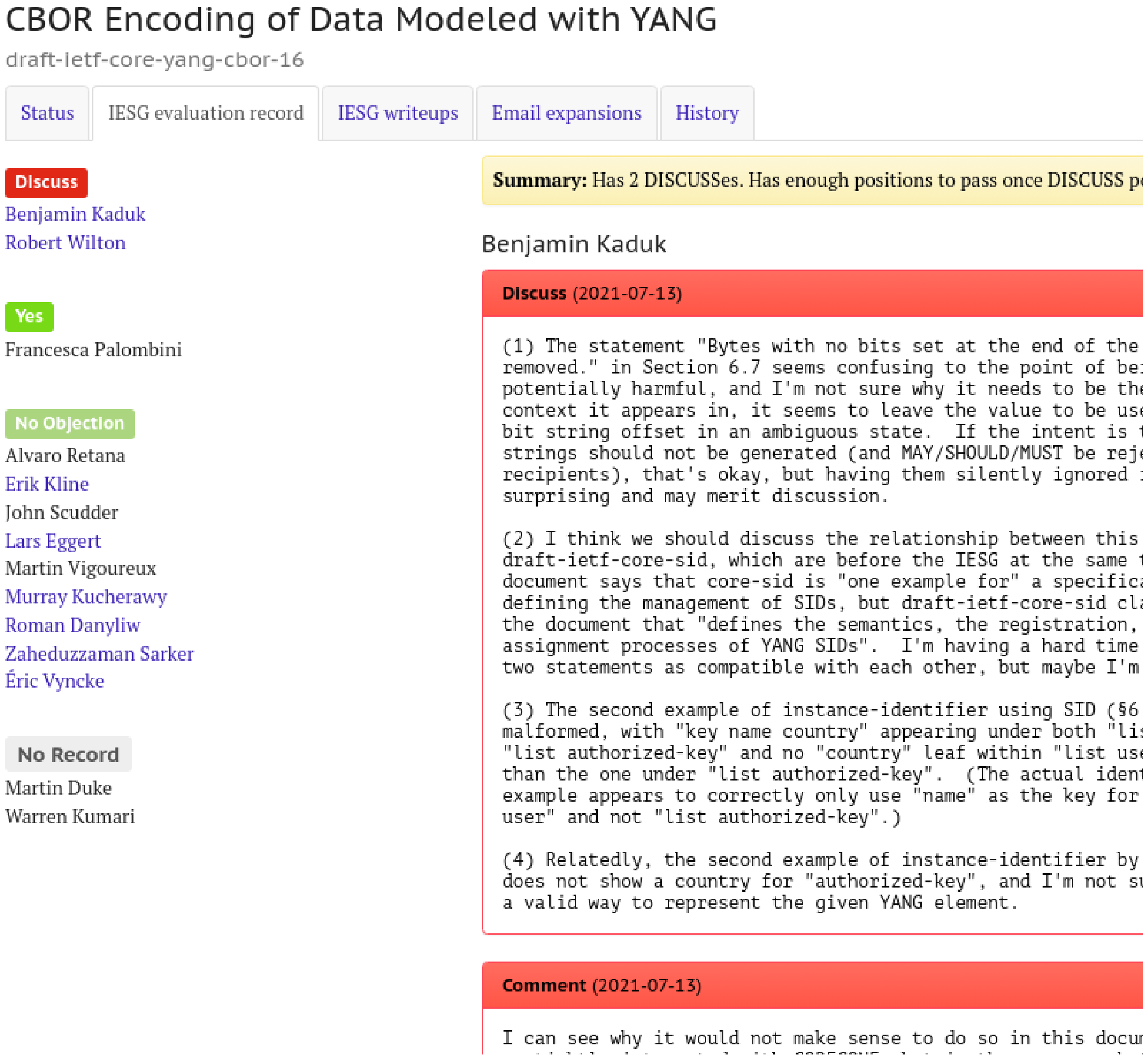
https://github.com/anima-wg/constrained-voucher/pull/127

Directorate Reviews

- Russ Housley GENART early review
  - Missing Security Considerations, pointed out some things
  - https://mailarchive.ietf.org/arch/msg/anima/87S9oAHrhRxMI03lRiutpClQRVc/
- Daniele Franke SECDIR early review
  - https://mailarchive.ietf.org/arch/msg/anima/UAGFHLMRmJ4cboyk4ONrhcdDfPo/
  - Issues #124, #125, #126.
    - About curve issue (#126), slide in Hackathon efforts coming
- Henk Birkholz IOTDIR early review
  - https://mailarchive.ietf.org/arch/msg/anima/EY4w20fWC5zYYly5JweHT1t5g8k/
  - Issues #132 to #141

- Media Types Review and Early Allocation Request
  - Carsten corrected sections 12.5, media types registry
  - We forgot to do early allocation for TBD3, had used value of 65502 in previous interop attempts (2019 era)

Dependent upon CORE WG drafts - now in IESG review



CBOR Encoding of Data Modeled with YANG

draft-ietf-core-yang-cbor-16

Summary: Has 2 DISCUSSes. Has enough positions to pass once DISCUSS p

Discuss
Benjamin Kaduk
Robert Wilton

Yes
Francesca Palombini

No Objection
Alvaro Retana
Erik Kline
John Scudder
Lars Eggert
Martin Vigoureux
Murray Kucherawy
Roman Danyliw
Zaheduzzaman Sarker
Éric Vyncke

No Record
Martin Duke
Warren Kumari

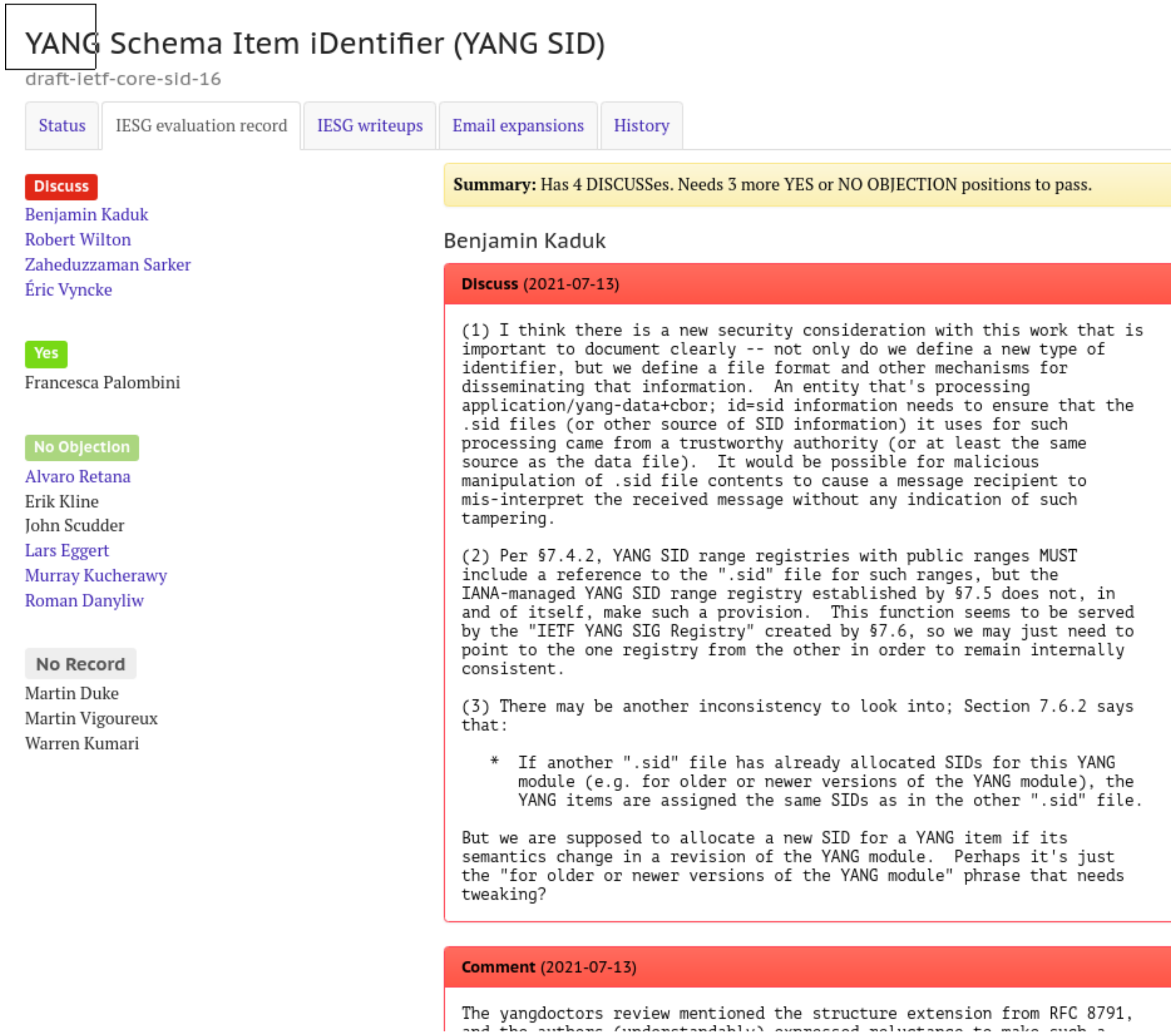
Benjamin Kaduk

Discuss (2021-07-13)

```
(1) The statement "Bytes with no bits set at the end of the
removed." in Section 6.7 seems confusing to the point of be:
potentially harmful, and I'm not sure why it needs to be the
context it appears in, it seems to leave the value to be use
bit string offset in an ambiguous state.  If the intent is t
strings should not be generated (and MAY/SHOULD/MUST be reje
recipients), that's okay, but having them silently ignored i
surprising and may merit discussion.

(2) I think we should discuss the relationship between this
draft-ietf-core-sid, which are before the IESG at the same t
document says that core-sid is "one example for" a specifica
defining the management of SIDs, but draft-ietf-core-sid cla
the document that "defines the semantics, the registration,
assignment processes of YANG SIDs".  I'm having a hard time
two statements as compatible with each other, but maybe I'm

(3) The second example of instance-identifier using SID (§6
malformed, with "key name country" appearing under both "lis
"list authorized-key" and no "country" leaf within "list use
than the one under "list authorized-key".  (The actual ident
example appears to correctly only use "name" as the key for
user" and not "list authorized-key".)

(4) Relatedly, the second example of instance-identifier by
does not show a country for "authorized-key", and I'm not su
a valid way to represent the given YANG element.
```

Comment (2021-07-13)

```
I can see why it would not make sense to do so in this docu
```



YANG Schema Item iDentifier (YANG SID)

draft-ietf-core-sid-16

Summary: Has 4 DISCUSSes. Needs 3 more YES or NO OBJECTION positions to pass.

Discuss
Benjamin Kaduk
Robert Wilton
Zaheduzzaman Sarker
Éric Vyncke

Yes
Francesca Palombini

No Objection
Alvaro Retana
Erik Kline
John Scudder
Lars Eggert
Murray Kucherawy
Roman Danyliw

No Record
Martin Duke
Martin Vigoureux
Warren Kumari

Benjamin Kaduk

Discuss (2021-07-13)

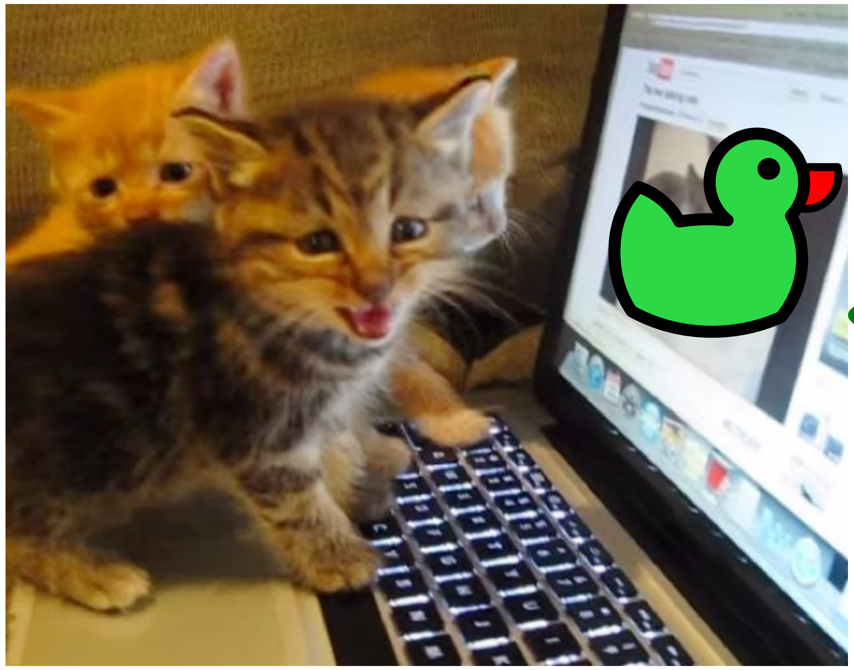
```
(1) I think there is a new security consideration with this work that is
important to document clearly -- not only do we define a new type of
identifier, but we define a file format and other mechanisms for
disseminating that information.  An entity that's processing
application/yang-data+cbor; id=sid information needs to ensure that the
.sid files (or other source of SID information) it uses for such
processing came from a trustworthy authority (or at least the same
source as the data file).  It would be possible for malicious
manipulation of .sid file contents to cause a message recipient to
mis-interpret the received message without any indication of such
tampering.

(2) Per §7.4.2, YANG SID range registries with public ranges MUST
include a reference to the ".sid" file for such ranges, but the
IANA-managed YANG SID range registry established by §7.5 does not, in
and of itself, make such a provision.  This function seems to be served
by the "IETF YANG SIG Registry" created by §7.6, so we may just need to
point to the one registry from the other in order to remain internally
consistent.

(3) There may be another inconsistency to look into; Section 7.6.2 says
that:

   *  If another ".sid" file has already allocated SIDs for this YANG
      module (e.g. for older or newer versions of the YANG module), the
      YANG items are assigned the same SIDs as in the other ".sid" file.

But we are supposed to allocate a new SID for a YANG item if its
semantics change in a revision of the YANG module.  Perhaps it's just
the "for older or newer versions of the YANG module" phrase that needs
tweaking?
```

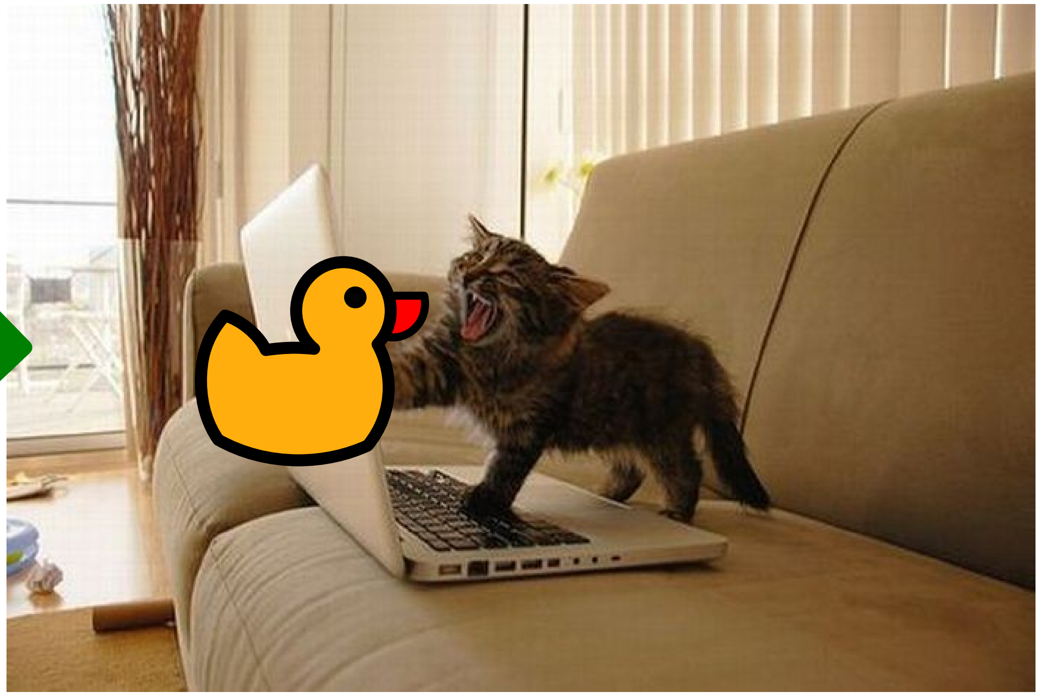
Comment (2021-07-13)

```
The yangdoctors review mentioned the structure extension from RFC 8791,
```

Hackathon Results

- IETF111 Hackathon July 19-23. Meet up in gather.town @ 14:00 UTC, at table A(NIMA).
- Participants: Esko (IOT-Consultancy), Peter (OCF?), Aurelio (ZHAW), Toerless (co-chair), Michael (Sandelman), Thomas (Siemens),
  - Will repeat at next Hackathon, but also participants want to continue between events.
  - IETF L2 VPN now available, which will help test join proxy parts
- NIST NCCoE IoT-onboarding presented Thursday, please see meeting materials
- Lost of work, but more smoke than fire
- Virtual event, so here are our feline likenesses at work:





List of Hackathon Issues (1)

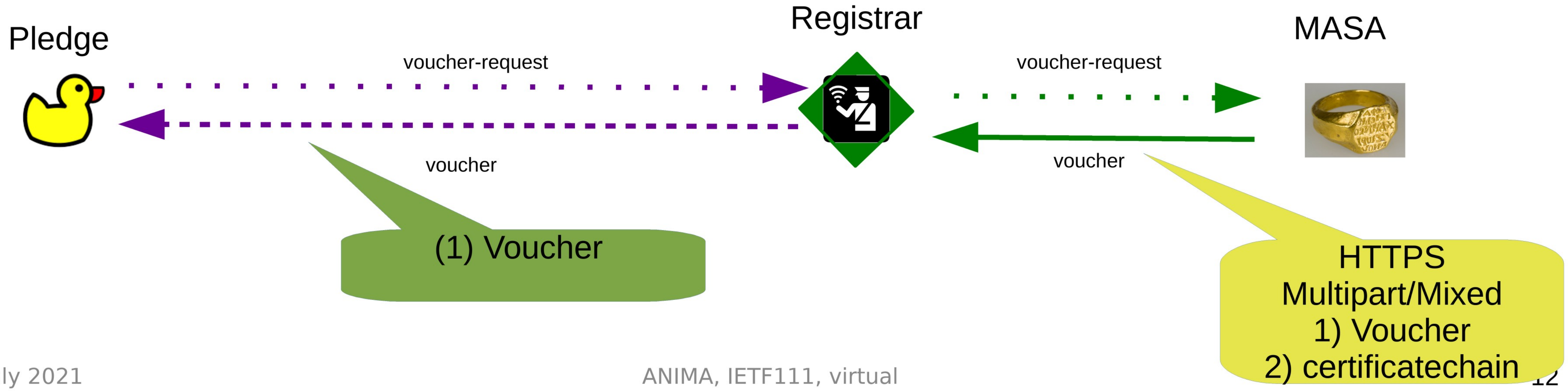
- Early Allocation of TBD3 - previous efforts used 65502 (private use value) for Content-Format
- Problems getting CCM_8 mode(s) enabled for OpenSSL
- What should Registrar/MASA have as mandatory to implement ciphers?
- SNI must be used for Registrar/MASA connection
  - SNI must be ignored to Pledge/Registrar (CN callback)

List of Hackathon Issues (2)

- is it allowed to omit x5bag on Voucher reply?
- is x5bag mandatory on Registar/MASA voucher-request?
  - Issue #142
- mbedTLS signature verification on voucher-request?
  - Unclear how to deal with preamble of public key with library
- Should we care about CN of MASA certificate? (Issue #144)
- IDevID Issuer in voucher, not using whole authority key.

X5BAG in voucher reply
auditing of MASA reply by Registrar

- Not transmitting x5bag with voucher to Pledge that already has it (or the RPK) saves at least 32-bytes, probably several hundred.
- Without x5bag with voucher, Registrar can not validate voucher. This creates a new code path to test, and also removes audit trail from Registrar.
- Two solutions are possible:
  - Always send x5bag or RPK equivalent (which would be?), but allow Registrar to remove it from COSE.
    - Involves “surgery” to COSE structure, which could result in a breaking something. Can not use COSE library.
  - Send needed certificates or public keys in a multipart/mixed.
    - This was proposed a few iterations ago, but not persued



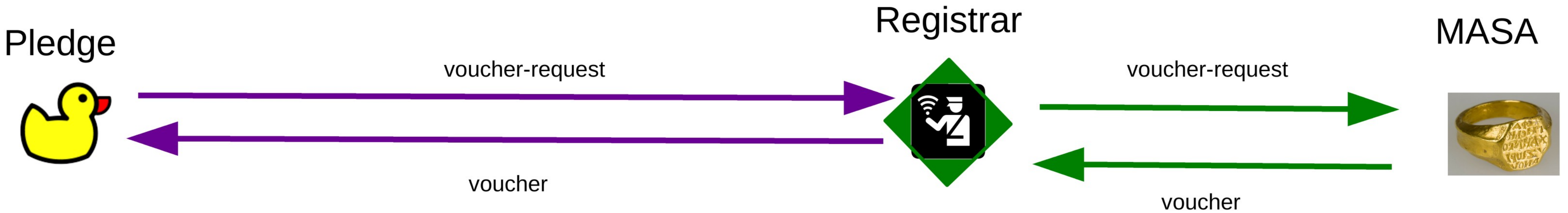
What should Registrar/MASA have as mandatory to implement ciphers?

- Pledge->Registrar, CoAPS, per RFC7252 has TLS_AES_128_CCM_8_SHA256 (DTLS1.3) and ECDHE-ECDSA-AES128-CCM8 (DTLS 1.2)
- These are not enabled by default as part of the **TLS** specification.
- Should Registrar->MASA be able to use only CCM_8 modes to talk to MASA? Should the Registrar use TLS MTI, or TLS MTI + CCM_8 modes?

We need to specify curve,
for signature on voucher request
And voucher.

So, we think secp256r1.
And an EdDSA ED25519?

CCM-8 is not standard TLS, so
MASA on common frameworks might
not support it. Do we force Registrar to
do normal public TLS list, or MASA to learn
CCM-8?



TLS_AES_128_CCM_8_SHA256
ECDHE-ECDSA-AES128-CCM8

?- CCM8 supported?

Should we care about CN of MASA certificate

- on Registrar, the TLS connection is made to MASA, and should the MASA’s certificate is verified to “match” the IDevID MASA extension.
  - Should we check the CN= in the SubjectDN?
  - Or should we use subjectAltName only, as per draft-rsalz-use-san-01
    - There is an mbedtls issue here with coding and constraints.
-

Should we care about CN of MASA certificate

- on Registrar, the TLS connection is made to MASA, and should the MASA’s certificate is verified to “match” the IDevID MASA extension.
  - Should we check the CN= in the SubjectDN?
  - Or should we use subjectAltName only, as per draft-rsalz-use-san-01
    - There is an mbedtls issue here with coding and constraints.
-

My preference is to ignore CN, and validate only subjectAltName as per draft-rsalz-use-san

IDevID Issuer, not using whole authority key

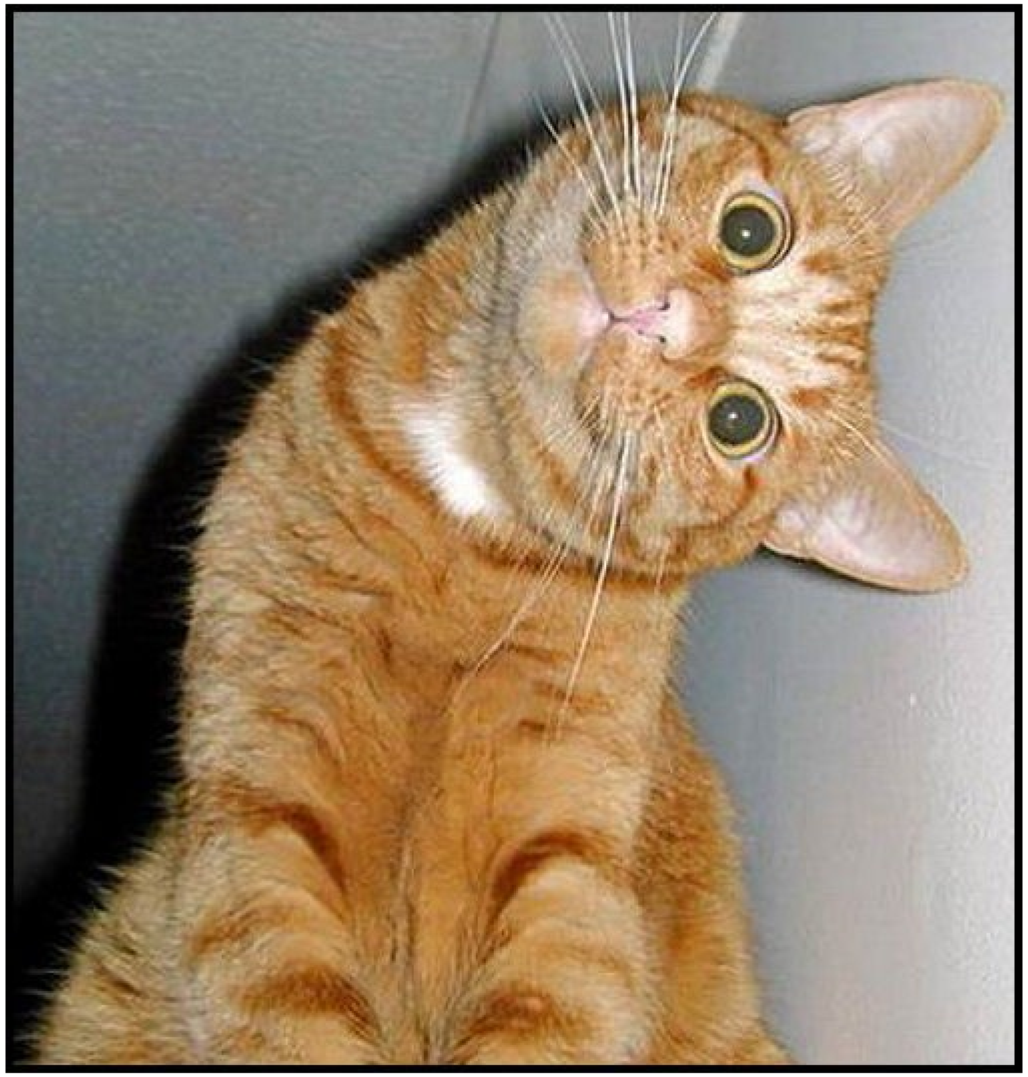
- In the voucher, we have the authority-key-identifier of IDevID issuer
  - (8366 section)
  - IDevID from Esko, processing by Thomas Registrar
- We may need clarification in RFC8366bis about this.

TLS Server Name Indicator (SNI) - RFC6066 clarification in RFC8995

- First errata against RFC8995:
  - https://www.rfc-editor.org/errata/eid6642
  - Section 5.4 says:
  - `Use of TLS 1.3 (or newer) is encouraged.  TLS 1.2 or newer is REQUIRED. TLS 1.3 (or newer) SHOULD be available.`
  - It should say:
  - `TLS 1.2 [RFC5246] with SNI support [RFC6066] is REQUIRED if TLS 1.3 is not available. The Server Name Indicator (SNI) is required when the Registrar communicates with the MASA in order for the MASA to be hosted in a modern multi-tenant TLS infrastructure.`
- Other one is about how the Pledge can not insert SNI, because it does not know the name of the Registrar, so any SNI found needs to be ignored by Registrar.
  - ... uhm.... Errata seems to be lost. Will refile.

Discussion

-



Thanks to weekly discussions in BRSKI design team on Thursday
Cancelled for August 5, but will resume on August 12.

Conclusions

Three directorate reviews occured
Security Considerations still needed
Applicability Statement needed!

(not ready for WGLC yet)