RFC8366bis voucher

draft-ietf-anima-rfc8366bis

was ADOPTED: January 2022

Michael Richardson,

(+Kent Watsen, Qiufang Ma, Max Pritiken, Toerless Eckert)

IETF 122
ANIMA Working Group

RFC8366bis: The storey so far

1) Tried to do extensions (see auxiliary slide for history). Failed.
    1) Moved all YANG extensions from: brski-cloud, cBRSKI, brski-prm into RFC8633bis into this document.
    2) Moved all YANG-CBOR (SID) work from cBRSKI into this document, verified that we things worked, tooling (pyang) was okay.
    3) waited for other documents to all become stable (equilibrium)
2) Noticed how RFC8520 (MUD) did extensions via draft-ietf-opsawg-mud-ol document, using “extensions”
3) Wrote draft-richardson-netmod-atrest-extensions, have not yet presented it or socialized it with netconf group. Implemented this. See next slides.

RFC8366bis: Reviews and changes

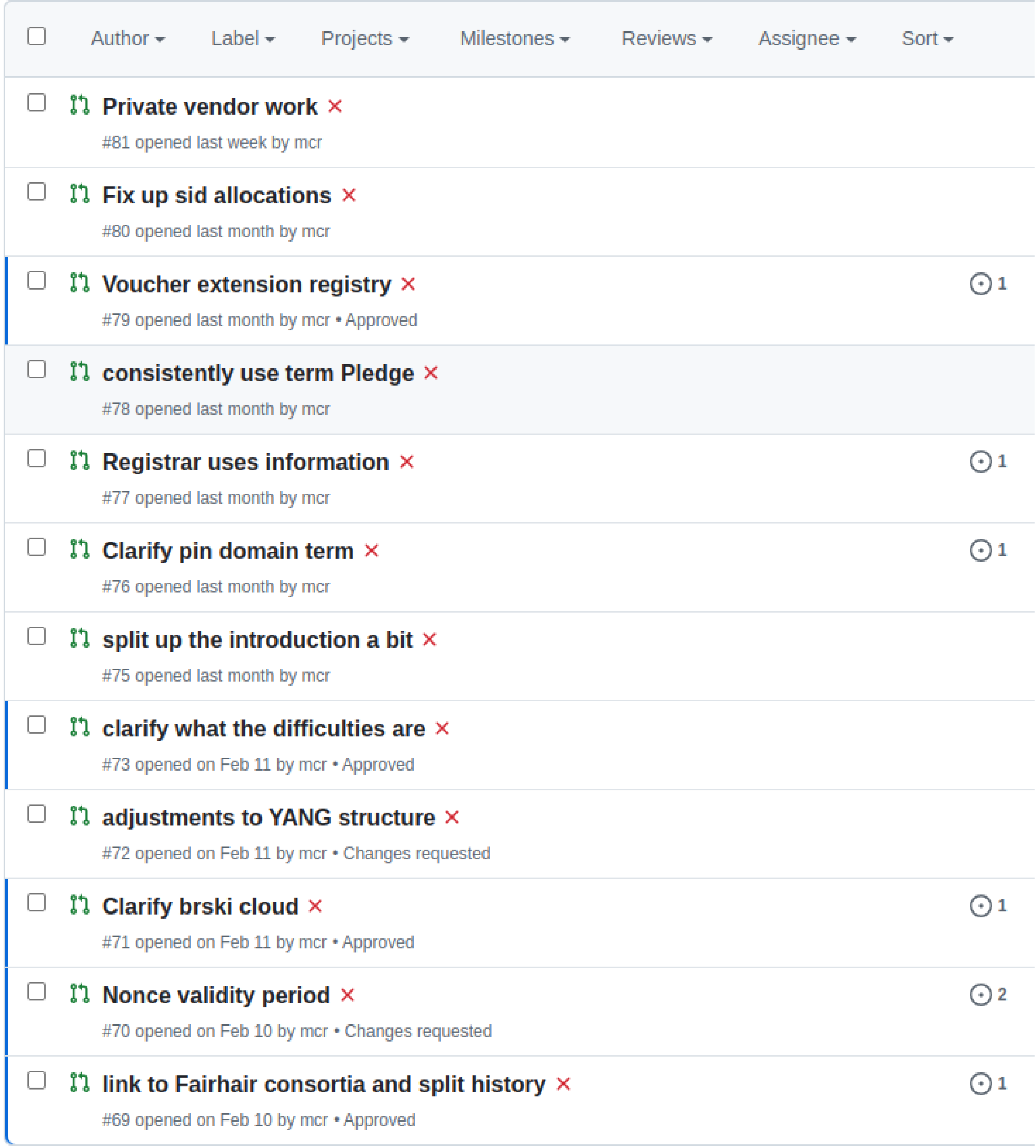
1) Processed Document review from Alexander Clemm.

2) Other comments accumulated.

3)These pull requests are **not** yet merged, but new document is based upon accumulation of patches.

4)**Please** go comment/read the pull requests.

Merge them all April 4, 2025.



□ Author ▾ Label ▾ Projects ▾ Milestones ▾ Reviews ▾ Assignee ▾ Sort ▾

□ **Private vendor work** ×
#81 opened last week by mcr

□ **Fix up sid allocations** ×
#80 opened last month by mcr

□ **Voucher extension registry** × ⊙ 1
#79 opened last month by mcr • Approved

□ **consistently use term Pledge** ×
#78 opened last month by mcr

□ **Registrar uses information** × ⊙ 1
#77 opened last month by mcr

□ **Clarify pin domain term** × ⊙ 1
#76 opened last month by mcr

□ **split up the introduction a bit** ×
#75 opened last month by mcr

□ **clarify what the difficulties are** ×
#73 opened on Feb 11 by mcr • Approved

□ **adjustments to YANG structure** ×
#72 opened on Feb 11 by mcr • Changes requested

□ **Clarify brski cloud** × ⊙ 1
#71 opened on Feb 11 by mcr • Approved

□ **Nonce validity period** × ⊙ 2
#70 opened on Feb 10 by mcr • Changes requested

□ **link to Fairhair consortia and split history** × ⊙ 1
#69 opened on Feb 10 by mcr • Approved

Extension Process (PR #79)

- Avoid having to wrap up documents again for simple extensions in the future.
- Support vendor (MASA) <-> Pledge extensions.
- Possible to just abuse JSON dictionaries to add anything you like
  - (not the YANG way!)
- not possible/easy when using CBOR (cBRSKI) due to need to allocate SIDs

```
leaf-list extensions {

   type string {

      length "1..40";

   }

   description "A list of extension names that are
used in this Voucher file.  Each name is
registered with the IANA and described in an
RFC.";

}
```

Extension JSON view

- In JSON, new YANG extension creates a new module name, e.g., “ietf-voucher-delegated”

```
{
  "ietf-voucher:voucher": {
    "created-on": "2016-10-07T19:31:42Z",
    "assertion": "logged",
    “extensions” : [ “ietf-voucher-delegated” ],
    "serial-number": "JADA123456789",
    "idevid-issuer": "base64encodedvalue==",
    "pinned-domain-cert": "base64encodedvalue==",
    "nonce": "base64encodedvalue=="
    “ietf-voucher-delegated”: {
        “delegation-enabled-flag”: “true”,
         “delegation-countdown” : 12,
    }
  }
}
```

Extension CBOR view

- In CBOR, new YANG extension creates requires a new SID allocation.
  - standard extensions get this from IANA
  - or from alternate Mega-Range (see RFC9595 section 6.3)
  - Vendor proprietary extensions could use draft-bormann-core-yang-sid-pen (still WIP)

```
{
  2451: {                    / SID = 2451, ietf-voucher:voucher|voucher /
    1: 2,                    / SID = 2452, assertion "proximity" /
    2: "2022-12-05T19:19:23Z", / SID = 2453, created-on   /
    3: false,                / SID = 2454, domain-cert-revocation-checks    /
    17: [ 61000 ],           / SID = 2468, extensions /
    7: h'831D5198A6CA2C7F',  / SID = 2508, nonce              /
    8: h'308201' ... '8CFF',    / SID = 2459, pinned-domain-cert
/
   11: "JADA123456789"      / SID = 2462, serial-number       /
   Tag<47>61000: {
     1: true,      / SID=61001, delegation-enabled-flag /
     2: 12,        / SID=61002, delegation-countdown /
   }
  }
}
```

CBOR diagnostic Format

Simple Extension

- Previous system might be too much for simple vendor/pledge extension

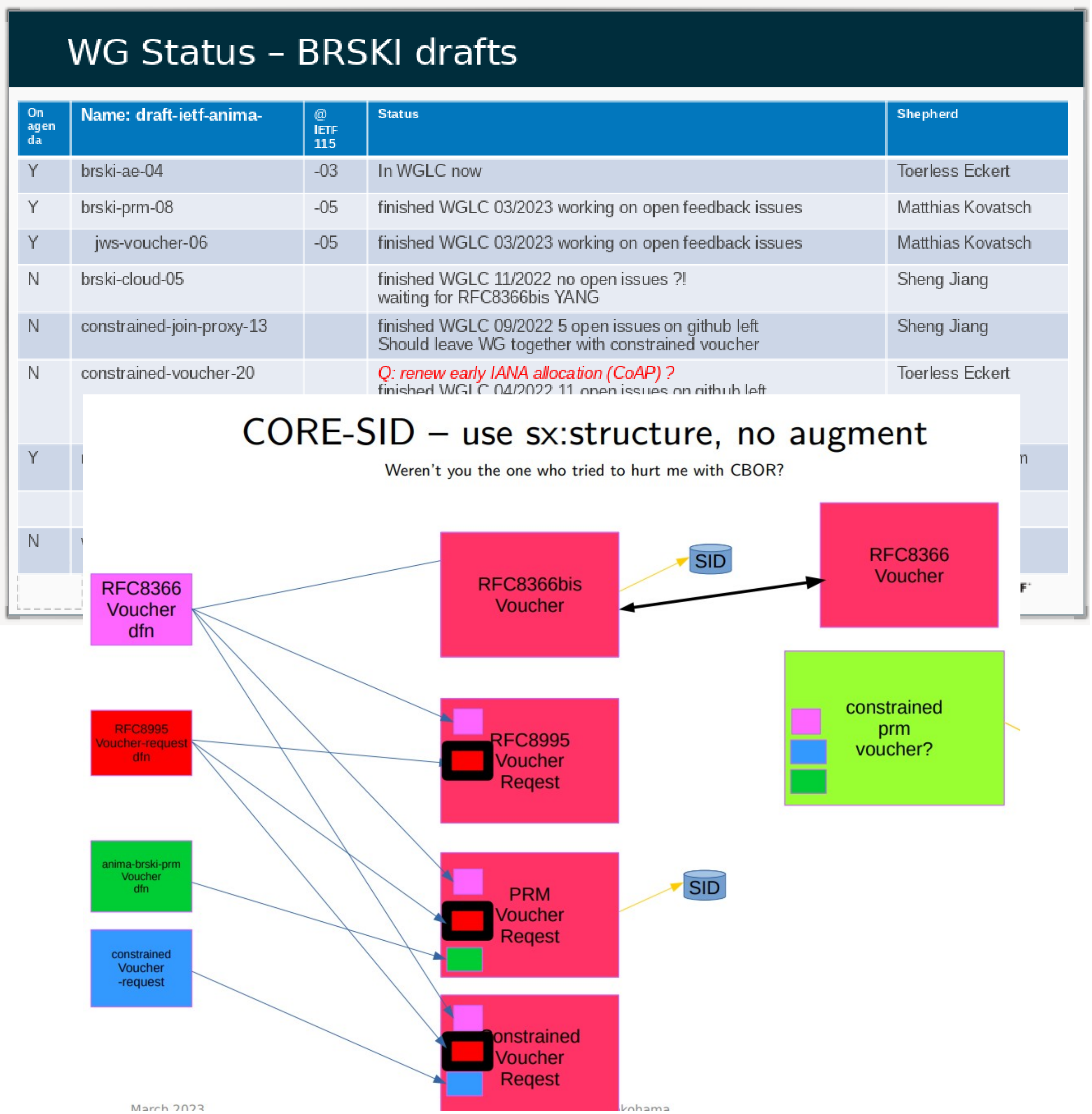
- `manufacturer-private`
  - `Is a one-time, non-interoperable way to insert stuff.`
  - `Must be bstr encoded because otherwise it would be delta encoded.`

```
{
   2451: {                     / SID = 2451, ietf-voucher:voucher|voucher /
     1: 2,                     / SID = 2452, assertion "proximity" /
     2: "2022-12-05T19:19:23Z", / SID = 2453, created-on   /
     3: false,                 / SID = 2454, domain-cert-revocation-checks    /
     18: <<[                   / SID = 2469, manufacturer-private /
        87: “potato”     / bstr encoded! /
     ]>>,
     7: h'831D5198A6CA2C7F', / SID = 2508, nonce                 /
     8: h'308201' ... '8CFF',    / SID = 2459, pinned-domain-cert
/
    11: "JADA123456789"     / SID = 2462, serial-number        /
   }
  }
```

CBOR diagnostic Format

Aux Slide: Discussions at IETF116 and before

- If you didn’t see the discussion and situation, then please visit: https://play.conf.meetecho.com/Playout/?session=IETF116-NETMOD-20230331-0030 Start at 1:53:00.
- Working through WGLC on documents that now depend upon RFC8366bis.
- draft-ietf-anima-brski-cloud draft-ietf-anima-constrained-join-proxy draft-ietf-anima-jws-voucher are still not in WGLC.
-



WG Status – BRSKI drafts

On agenda	Name: draft-ietf-anima-	@ IETF 115	Status	Shepherd
Y	brski-ae-04	-03	In WGLC now	Toerless Eckert
Y	brski-prm-08	-05	finished WGLC 03/2023 working on open feedback issues	Matthias Kovatsch
Y	jws-voucher-06	-05	finished WGLC 03/2023 working on open feedback issues	Matthias Kovatsch
N	brski-cloud-05		finished WGLC 11/2022 no open issues ?! waiting for RFC8366bis YANG	Sheng Jiang
N	constrained-join-proxy-13		finished WGLC 09/2022 5 open issues on github left Should leave WG together with constrained voucher	Sheng Jiang
N	constrained-voucher-20		*Q: renew early IANA allocation (CoAP) ?* finished WGLC 04/2022 11 open issues on github left	Toerless Eckert
Y				
N				

CORE-SID – use sx:structure, no augment

Weren’t you the one who tried to hurt me with CBOR?

Next Step?

Get the other documents out of the WG, as if they need changes to YANG, then 8366bis can be revised