RPKI Signed Checklists (RSC) update March 2022

Job Snijders
job@fastly.com / job@openbsd.org

Co-authors: Ben Maddison (Workonline), Tom Harrison (APNIC)

Agenda

- **What is RSC?**
  - Ability to construct a signature over one or more *arbitrary* digital objects
  - Exists outside the Core RPKI publication system for “Routing” – RSC has no impact to the BGP DFZ
  - Might be useful to BYOIP / BYOAS scenarios: PeeringDB, Cloud Providers
- **Testing & running code status**
  - Multiple Signers
  - Multiple Validators
- **Next steps**
  - Working Group Last Call?

IETF 111 SIDROPS – what happened since then?

Previous update at IETF 111:

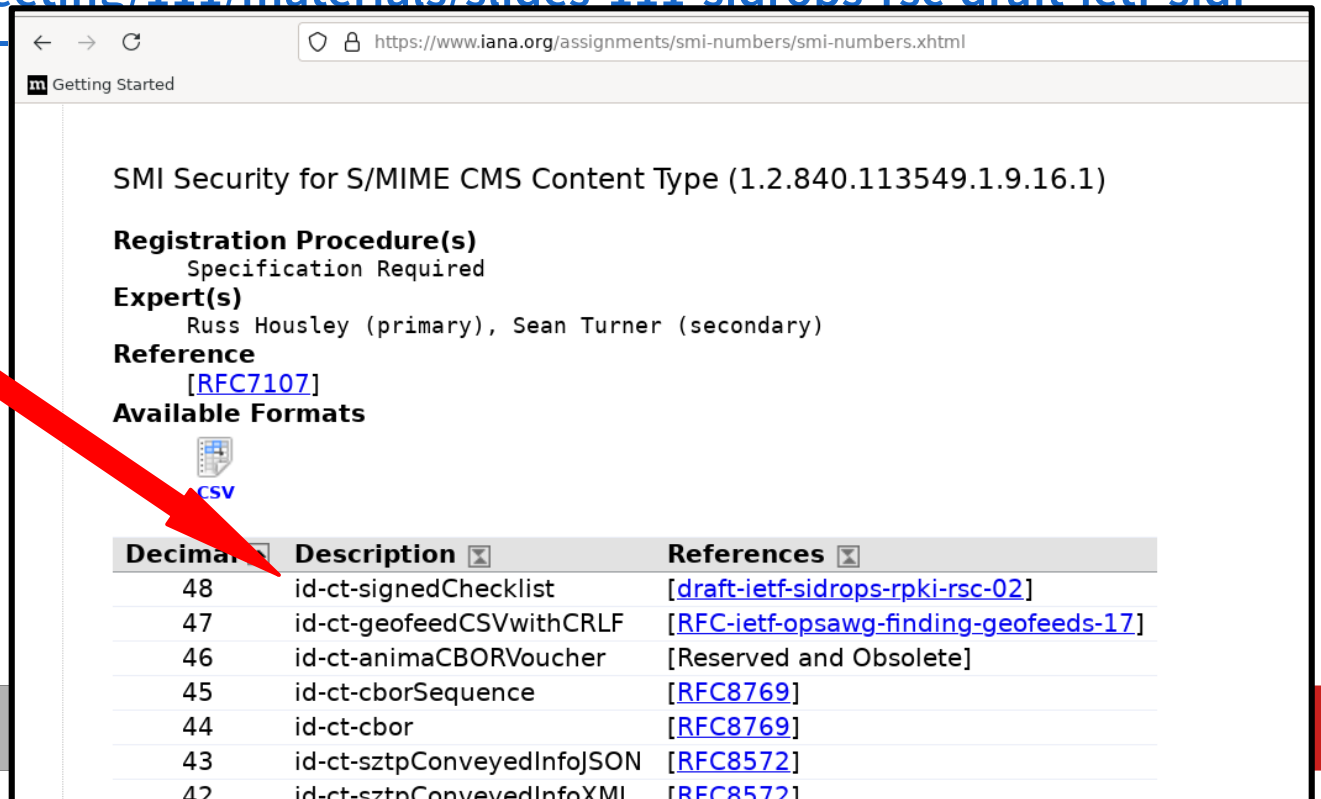
https://datatracker.ietf.org/meeting/111/materials/slides-111-sidrops-rsc-draft-ietf-sidrops-rpki-rsc-july-2021-update-

Renewed the IANA codepoint!

1.2.840.113549.1.9.16.1.48

Content-Type OID added to:

- OpenSSL 3.0
- LibreSSL 3.4.0



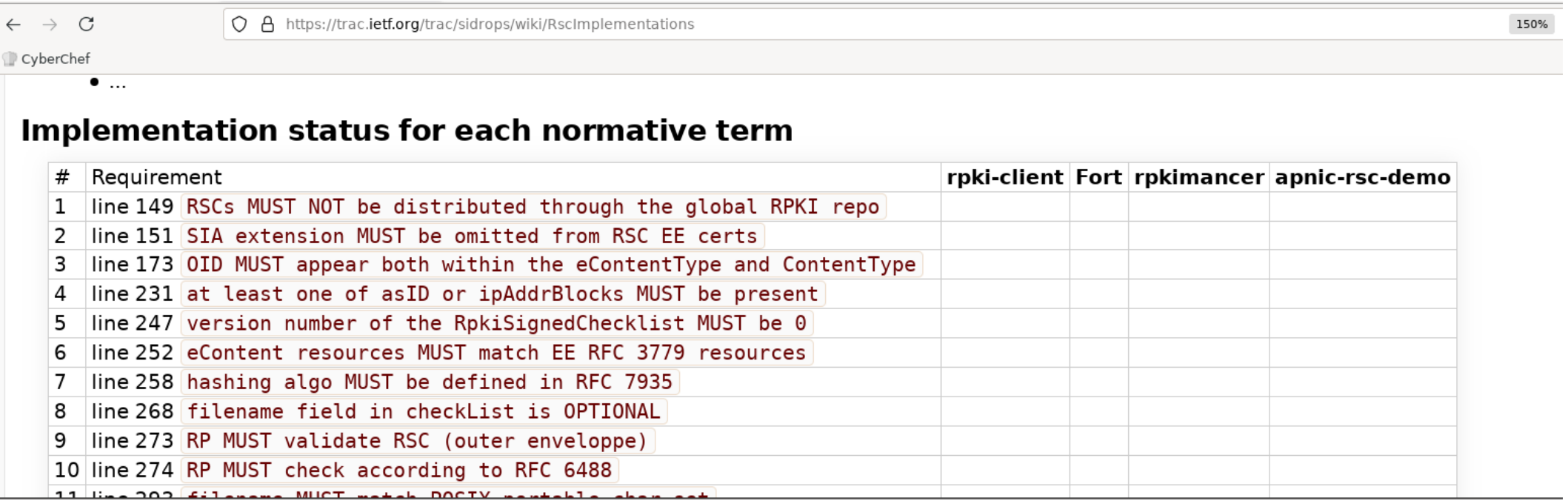
Example .sig file

https://github.com/job/draft-rpki-checklists/tree/main/example file “checklist.sig”

```
vurt$ openssl asn1parse -in checklist.sig -inform der -i -strparse 60
    0:d=0  hl=2 l= 126 cons: SEQUENCE
    2:d=1  hl=2 l=  19 cons:  SEQUENCE
    4:d=2  hl=2 l=  17 cons:   cont [ 1 ]
    6:d=3  hl=2 l=  15 cons:    SEQUENCE
    8:d=4  hl=2 l=  13 cons:     SEQUENCE
   10:d=5  hl=2 l=   2 prim:      OCTET STRING      [HEX DUMP]:0002
   14:d=5  hl=2 l=   7 prim:      BIT STRING
   23:d=1  hl=2 l=  11 cons:  SEQUENCE
   25:d=2  hl=2 l=   9 prim:   OBJECT            :sha256
   36:d=1  hl=2 l=  90 cons:  SEQUENCE
   38:d=2  hl=2 l=  52 cons:   SEQUENCE
   40:d=3  hl=2 l=  16 prim:    IA5STRING         :b42_ipv6_loa.png
   58:d=3  hl=2 l=  32 prim:    OCTET STRING      [HEX DUMP]:9516DD64BE7C1725B9FCA117120E58E8D842A5206873399B3DDFFC91C4B6ACF0
   92:d=2  hl=2 l=  34 cons:   SEQUENCE
   94:d=3  hl=2 l=  32 prim:    OCTET STRING      [HEX DUMP]:0AE1394722005CD92F4C6AA024D5D6B3E2E67D629F11720D9478A633A117A1C7
```

Implementation reporting: both high level & detailed

https://trac.ietf.org/trac/sidrops/wiki/RscImplementations



Request to the Big Five™ Trust Anchors and NIRs?

Can you implement a RSC signing service via your Web Portals / APIs?

```
-----BEGIN RSC REQUEST-----
1|1627391997|My First RSC|15562|27-07-2021|27-07-2022|F2ca1bb6c7e907…
-----END RSC REQUEST-----
-----BEGIN SIGNATURE-----
RGWqTwh/z7+mC/R9VJIcb…
1eUgTTihwlAdejOykIsviQ==
-----END SIGNATURE-----
```

Don’t forget a RSC REVOKE tool! :-)

Or as Web Form in a Portal?

Resource	[AS 15562]
SHA256 hash	F2ca1bb6c7e907...
Optional filename	test
RSC Validity Period	NOW() - NOW()+1year

Cancel | Generate & Download RSC!

Next steps?

- Wrap it up … WG Last Call?