RPKI Signed Checklists (RSC) update July 2021

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

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
- **Testing & running code status**
  - Multiple Signers
  - Multiple Validators
- **Next steps**
  - Wait for more feedback from *RSC issuers* (RIRs)?
  - Wait for more Relying Party implementation reports?
  - Last Call?

IETF 110 SIDROPS – what happened since then?

Previous update at IETF 110:
https://datatracker.ietf.org/meeting/110/materials/slides-110-sidrops-job-snijders-rsc-00.pdf

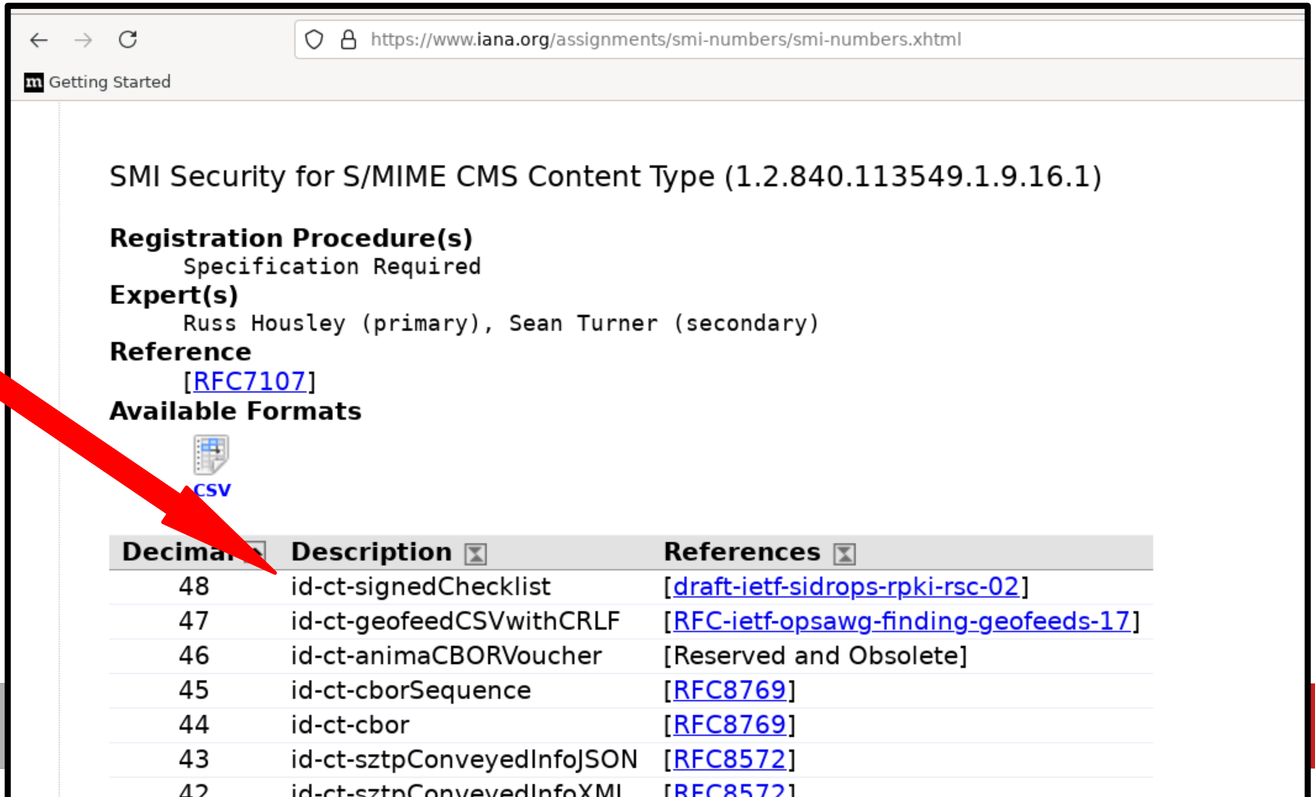
Since then:

Got the IANA codepoint!

1.2.840.113549.1.9.16.1.48

Content-Type OID added to:

- OpenSSL 3.0.0 beta1
- LibreSSL 3.4.0



https://www.iana.org/assignments/smi-numbers/smi-numbers.xhtml
Getting Started

SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1)

Registration Procedure(s)

Specification Required

Expert(s)

Russ Housley (primary), Sean Turner (secondary)

Reference

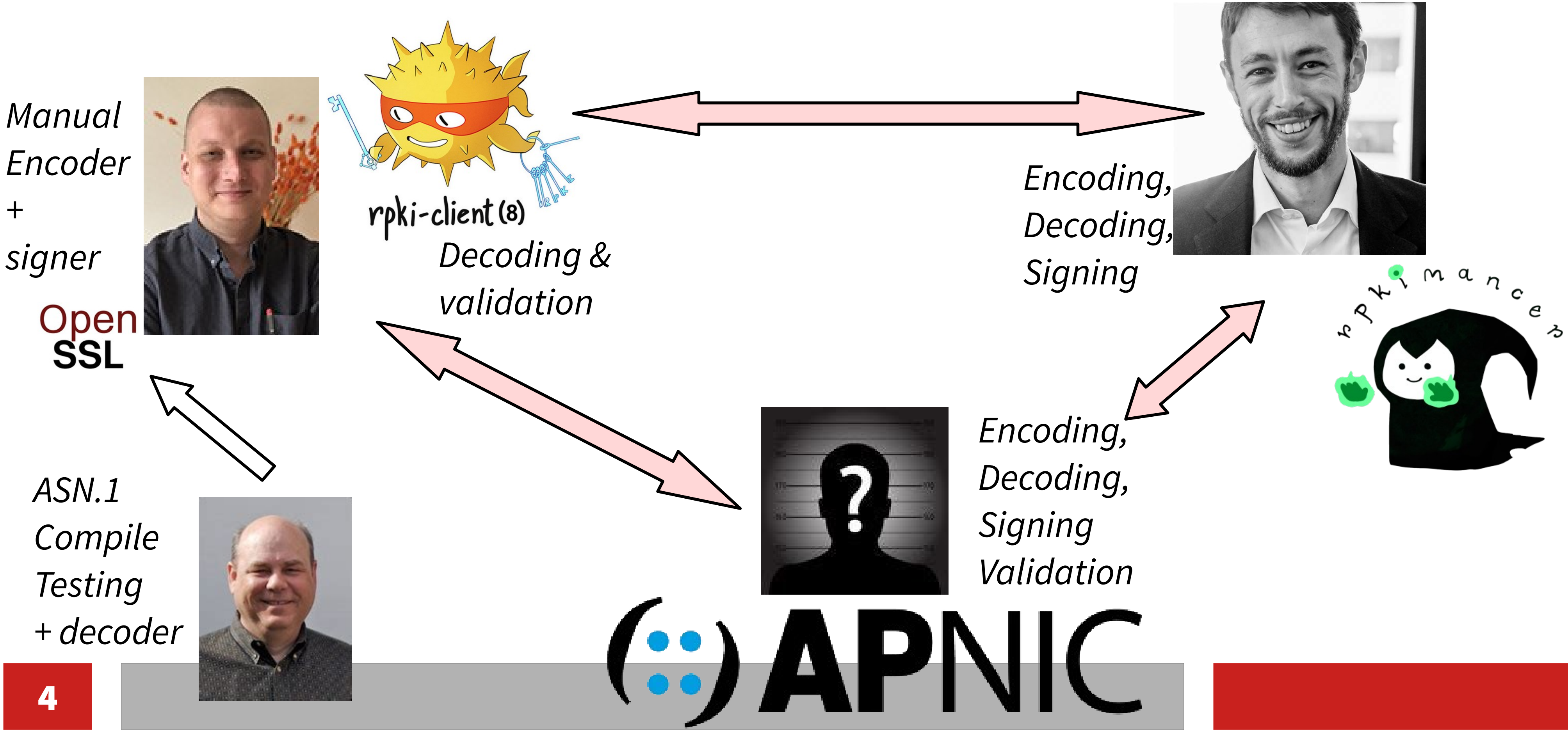
[RFC7107]

Available Formats

CSV

Decimal	Description	References
48	id-ct-signedChecklist	[draft-ietf-sidrops-rpki-rsc-02]
47	id-ct-geofeedCSVwithCRLF	[RFC-ietf-opsawg-finding-geofeeds-17]
46	id-ct-animaCBORVoucher	[Reserved and Obsolete]
45	id-ct-cborSequence	[RFC8769]
44	id-ct-cbor	[RFC8769]
43	id-ct-sztpConveyedInfoJSON	[RFC8572]
42	id-ct-sztpConveyedInfoXML	[RFC8572]

Double checking & confirming each other’s work – a triangle



Manual Encoder
+
signer

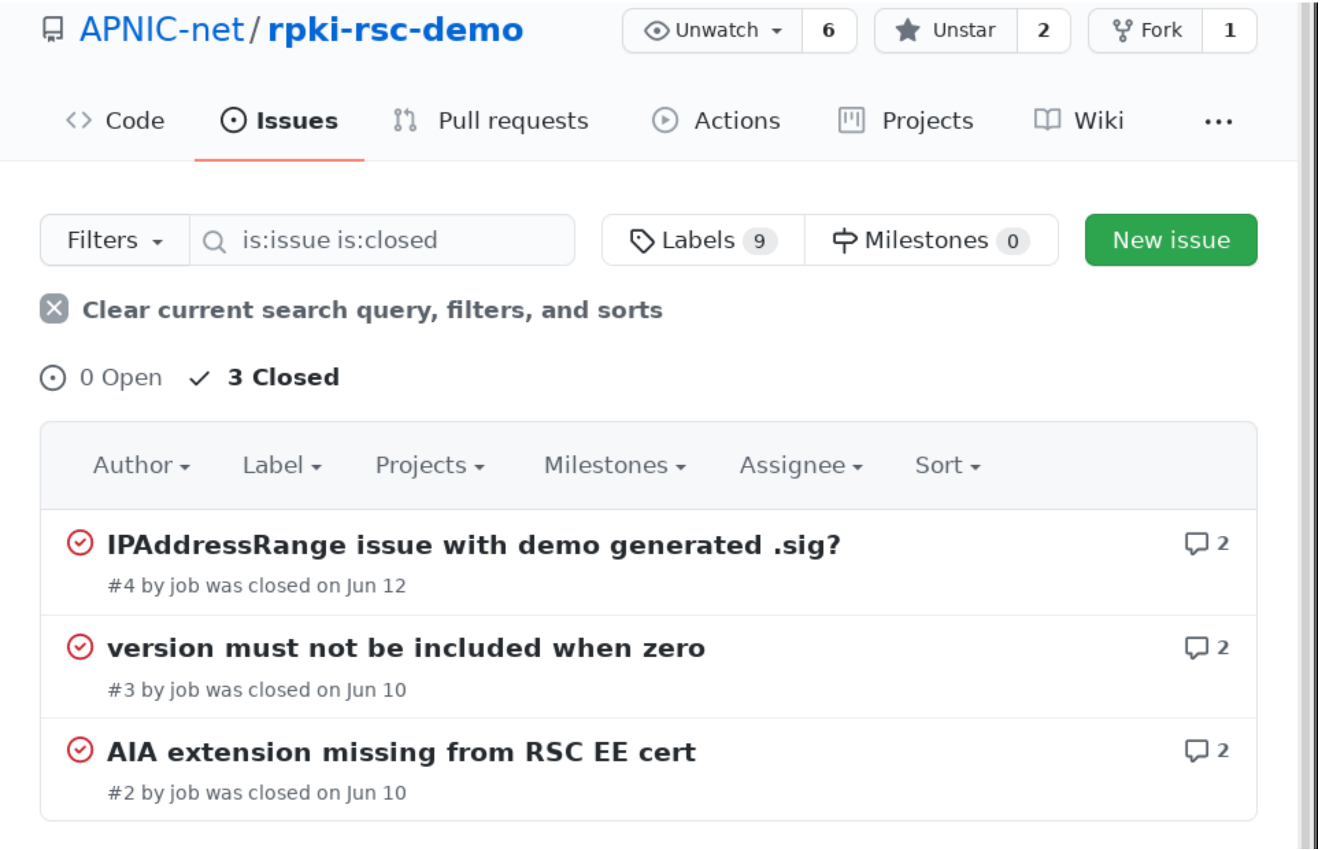
Decoding & validation

Encoding,
Decoding,
Signing

ASN.1
Compile
Testing
+ decoder

Encoding,
Decoding,
Signing
Validation

(Tinkering with) Running Code proved to be invaluable



is:issue is:closed

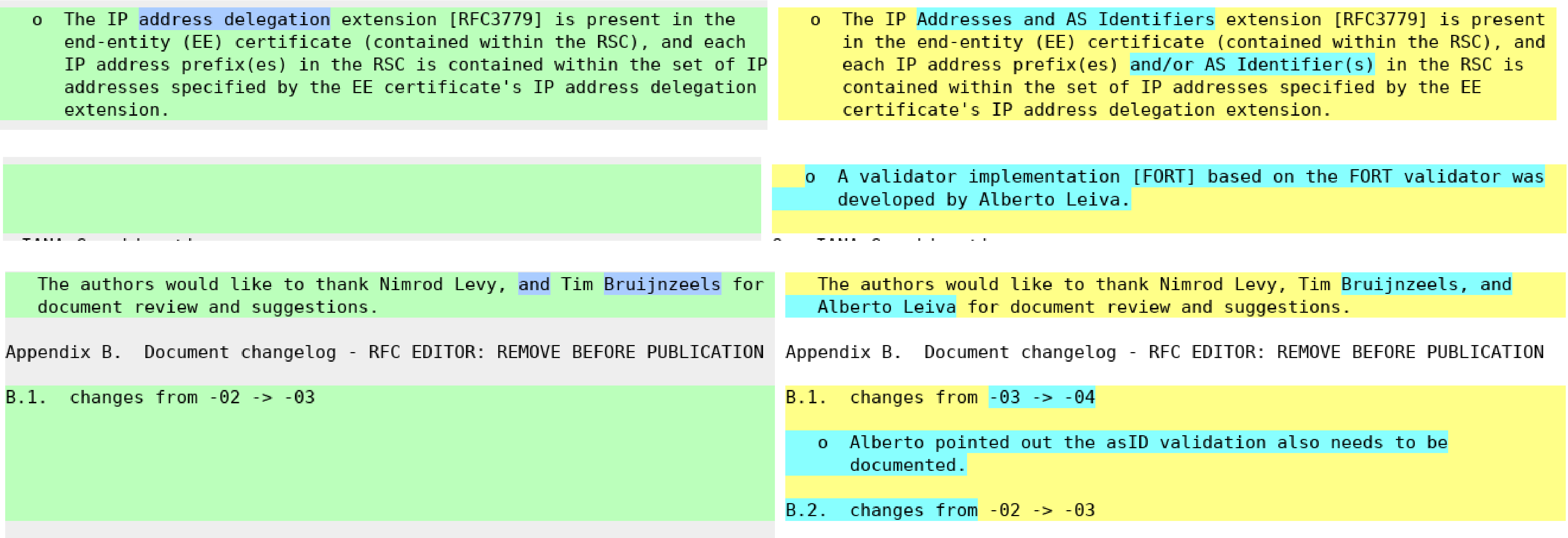
IPAddressRange issue with demo generated .sig? 2
#4 by job was closed on Jun 12

version must not be included when zero 2
#3 by job was closed on Jun 10

AIA extension missing from RSC EE cert 2
#2 by job was closed on Jun 10

Software developers provide the best possible feedback

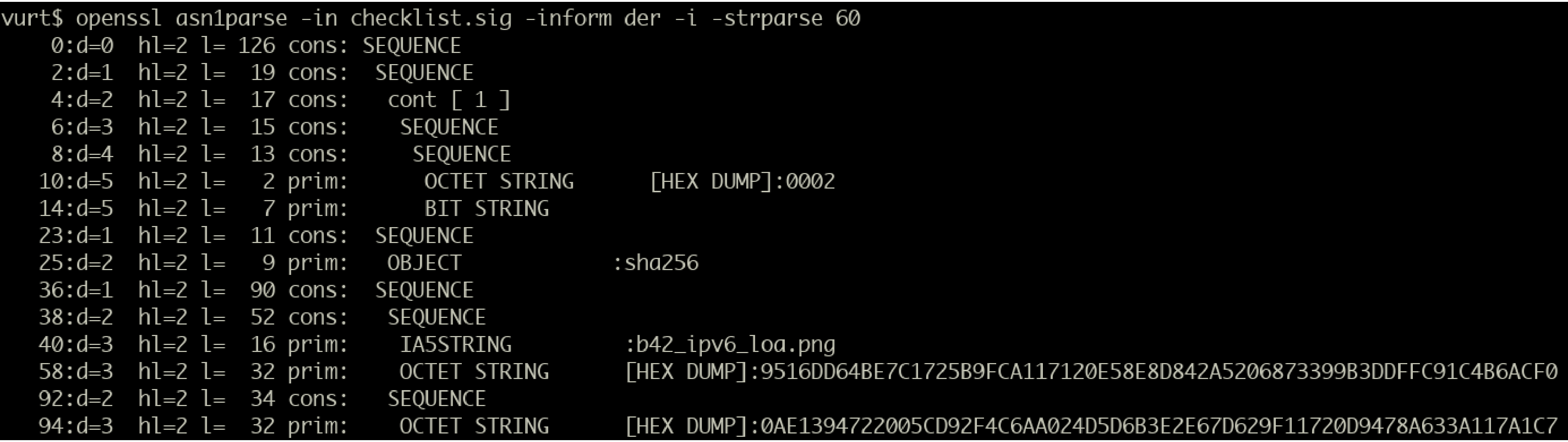
https://www.ietf.org/rfcdiff?url2=draft-ietf-sidrops-rpki-rsc-04.txt



o The IP address delegation extension [RFC3779] is present in the end-entity (EE) certificate (contained within the RSC), and each IP address prefix(es) in the RSC is contained within the set of IP addresses specified by the EE certificate's IP address delegation extension.	o The IP Addresses and AS Identifiers extension [RFC3779] is present in the end-entity (EE) certificate (contained within the RSC), and each IP address prefix(es) and/or AS Identifier(s) in the RSC is contained within the set of IP addresses specified by the EE certificate's IP address delegation extension.
	o A validator implementation [FORT] based on the FORT validator was developed by Alberto Leiva.
The authors would like to thank Nimrod Levy, and Tim Bruijnzeels for document review and suggestions.	The authors would like to thank Nimrod Levy, Tim Bruijnzeels, and Alberto Leiva for document review and suggestions.
Appendix B. Document changelog - RFC EDITOR: REMOVE BEFORE PUBLICATION	Appendix B. Document changelog - RFC EDITOR: REMOVE BEFORE PUBLICATION
B.1. changes from -02 -> -03	B.1. changes from -03 -> -04 o Alberto pointed out the asID validation also needs to be documented. B.2. changes from -02 -> -03

Example .sig file

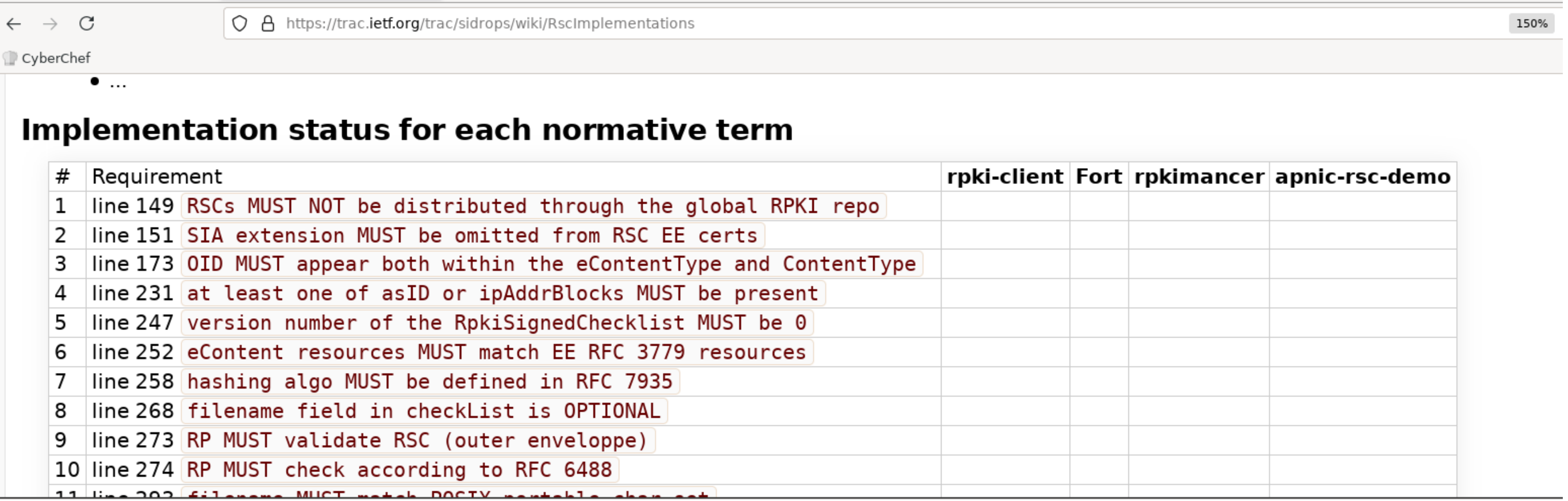
https://github.com/job/draft-rpki-checklists/tree/main/example file “checklist.sig”



```
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



- …

Implementation status for each normative term

#	Requirement	rpki-client	Fort	rpkimancer	apnic-rsc-demo
1	line 149 `RSCs MUST NOT be distributed through the global RPKI repo`				
2	line 151 `SIA extension MUST be omitted from RSC EE certs`				
3	line 173 `OID MUST appear both within the eContentType and ContentType`				
4	line 231 `at least one of asID or ipAddrBlocks MUST be present`				
5	line 247 `version number of the RpkiSignedChecklist MUST be 0`				
6	line 252 `eContent resources MUST match EE RFC 3779 resources`				
7	line 258 `hashing algo MUST be defined in RFC 7935`				
8	line 268 `filename field in checkList is OPTIONAL`				
9	line 273 `RP MUST validate RSC (outer enveloppe)`				
10	line 274 `RP MUST check according to RFC 6488`				
11	line 293 `filename MUST match POSIX portable char set`				

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-----
```

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!

Don't forget a RSC REVOKE tool! :-)

Next steps?

- Wait for more feedback from *RSC issuers?* (for example RIRs)
- Wait for more Relying Party implementation reports?
- Or wrap it up … WG Last Call?