Please suggest a better name!

Clarification of RFC7030 CSR Attributes definition draft-richardson-lamps-rfc7030-csrattrs

Michael Richardson <mcr+ietf@sandelman.ca>
Dan Harkins (Industrial Lounge)
D. von Orheimb (Siemens)
Owen Friel (Cisco)

The Story so far

- RFC7030 was unclear about CSR attributes
- RFC8994 (ACP) and RFC8995 (BRSKI) made an assumption that values could be provided
  - (RFC7030 and RFC8995 have one author in common)
- We had a virtual interim meeting at the end of August
  - https://datatracker.ietf.org/meeting/interim-2021-lamps-02/session/lamps
  - https://www.youtube.com/watch?v=yAg9hKE844g
- We seemed to come to conclude that we need to issue an Updates RFC7030 to fix the CSR Attributes
  - That the document was correct, and the ACP usage was wrong.
- Formed design team, had a few private threads, but no meetings, and little progress on draft and questions.

VIEWER WARNING: ASN.1 examples were created by ASN.1 amateur.
Some examples may be harmful to your cognitive functioning.

Divergent views on how to proceed follow.

Choice Alpha --- Make ACP usage work

```
CsrAttrs ::= SEQUENCE SIZE (0..MAX) OF AttrOrOID

AttrOrOID ::= CHOICE (oid OBJECT IDENTIFIER,
                      attribute Attribute,
                      value Value }

Attribute { ATTRIBUTE:IOSet } ::= SEQUENCE {
     extType  ATTRIBUTE.&id({IOSet}),
     extAttr  SET SIZE(1..MAX) OF ATTRIBUTE.&Type({IOSet}{@type})
}

Value { ATTRIBUTE:IOSet } ::= SEQUENCE {
     extType  ATTRIBUTE.&id({IOSet}),
     type     ATTRIBUTE.&Type({IOSet}{@type}),
     value    OCTET STRING
}
```

Create a new CHOICE

Put the stuff we need in it.

Most certainly wrong.

Choice Beta --- create new encoding to address name/keyspec needs only

```
CsrAttrs ::= SEQUENCE {
        oids      SEQUENCE OF OBJECT IDENTIFIER,
        attrs     SEQUENCE OF Attribute,
        subject     [0] GenericName OPTIONAL,
        keySpec   [1] KeySpec OPTIONAL,
        hashAlg   [2] AlgorithmIdentifier OPTIONAL
}
```

1:1 array
What we had before

Specific entries
To deal with todays
Current needs.
Extensible by new
revision to ASN.1

Discussion/Questions

Building at Carleton University, where CERN's ATLAS detector was built.

Every Canadian Squirrel has a constitutional right to Tim Hortons