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

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

Please suggest a better name!
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
Current Suggested ASN.1

CsrAttrs ::= SEQUENCE {
  oids      SEQUENCE OF OBJECT IDENTIFIER, --
  used mostly for challengePassword
  attrs     SEQUENCE SIZE (0..MAX) OF
  Attribute, -- mostly for X.509 extensions
  subject   [0] Name OPTIONAL,
  keySpec   [1] KeySpec OPTIONAL,
  hashAlg   [2] AlgorithmIdentifier OPTIONAL
}

Or GenericName?
Discussion/Questions
Backup slides follow
Example from running code

X509v3 extensions:

X509v3 Subject Alternative Name:

otherName:rfc8994+fd739fc23c3440112233445500000100+@acp.example.com

X509v3 Basic Constraints:

CA:FALSE
6.2.2. ACP Certificate AcpNodeName

```plaintext
cpc-node-name = local-part "@" acp-domain-name
local-part = [ acp-address ] [ "+" rsub extensions ]
acp-address = 32HEXDIG / "0" ; HEXDIG as of [RFC5234], Appendix B.1
rsub = [ <subdomain> ] ; <subdomain> as of [RFC1034], Section 3.5
acp-domain-name = <domain> ; as of [RFC1034], Section 3.5
extensions = *( "+" extension )
extension = 1*etext ; future standard definition.
etext = ALPHA / DIGIT / ; Printable US-ASCII
   "!" / "#" / "$" / "&" / "'" / "*" / "-" / "/" / "=" / "?" / "^" / "_" / "\" / "{" / "|" / "}" / "~"

routing-subdomain = [ rsub "." ] acp-domain-name
```

Figure 2: ACP Node Name ABNF

Example:
Given an ACP address of fd89:b714:f3db:0:200:0:6400:0000, an ACP domain name of acp.example.com, and an rsub extension of area51.research, then this results in the following:

```plaintext
acp-node-name = fd89b714f3db00000200000064000000 +area51.research@acp.example.com
acp-domain-name = acp.example.com
routing-subdomain = area51.research.acp.example.com
```