

Please suggest  
a better name!

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

Michael Richardson <[mcr+ietf@sandelman.ca](mailto:mcr+ietf@sandelman.ca)>

Dan Harkins (Industrial Lounge)

David von Oheimb (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**.
- That the only real problem was that we needed an extra layer of ExtensionRequest to hold the subjectAltName components.

# What WRONG looked like

```
0 72: SEQUENCE {
2 70:   SEQUENCE {
4   3:     OBJECT IDENTIFIER subjectAltName (2 5 29 17)
9 63:     SET {
11 61:       SEQUENCE {
13 59:         [1] {
15 57:           UTF8String
           :           'rfc8994+fd739fc23c3440112233445500000000+@acp.ex'
           :           'ample.com'
           :         }
           :       }
           :     }
           :   }
           : }
```

# What RIGHT now looks like

```
0 90: SEQUENCE {
2 88:   SEQUENCE {
4 9:    OBJECT IDENTIFIER extensionRequest (1 2 840 113549 1 9 14)
15 75:   SET {
17 73:    SEQUENCE {
19 3:     OBJECT IDENTIFIER subjectAltName (2 5 29 17)
24 3:     [0] {
26 1:      BOOLEAN TRUE
      :      }
29 61:    SEQUENCE {
31 59:     [0] {
33 57:      UTF8String
      :      'rfc8994+fd739fc23c3440112233445500000000+@acp.ex'
      :      'ample.com'
      :      }
      :    }
      :  }
      : }
      : }
      : }
```

critical

# Discussion/Questions

Time to adopt document?

