Please suggest a better name!

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

Michael Richardson <<u>mcr+ietf@sandelman.ca</u>> Dan Harkins (Industrial Lounge) D. von Orhimb (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/l amps
  - 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.

## 2022-03-25

IETF113 LAMPS Vienna

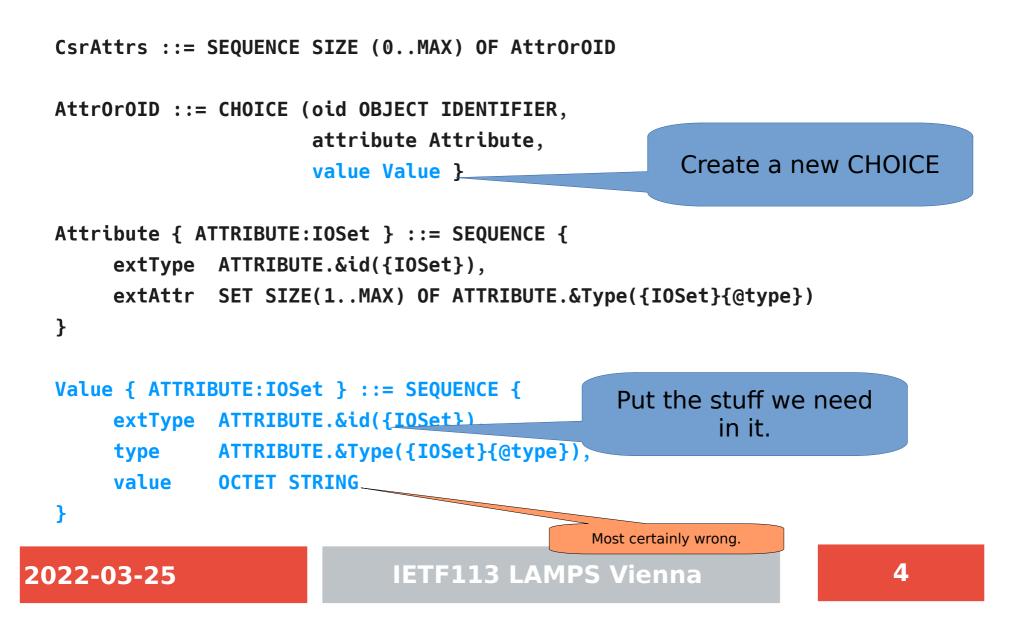
VIEWER WARNING: ASN.1 examples were created by ASN.1 amateur. Some examples may be harmful to your cognitive functioning.

Divergent views on how to proceed follow.



2022-03-25

# **Choice Alpha --- Make ACP usage work**



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

1:1 array What we had before

## CsrAttrs ::= SEQUENCE {

- oids SEQUENCE OF OBJECT IDENTIFIER,
- attrs **SEQUENCE OF Attribute**,
- subject [0] GenericName OPTIONAL,
- keySpec [1] KeySpec OPTIONAL,
- hashAlg [2] AlgorithmIdentifier OPTIONAL

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

## 2022-03-25

IETF113 LAMPS Vienna

# **Discussion/Questions**

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

> Every Canadian Squirrel has a constitutional right to Tim Hortons

#### 2022-03-25

**IETF113 LAMPS Vienna**