Discussion on using CDDL in BRISKI-PRM enroll-trigger message

draft-ietf-anima-brski-prm-12
Repo URL: https://github.com/anima-wg/anima-brski-prm

Steffen Fries, Thomas Werner, Elliot Lear, Michael Richardson
Shepherd: Matthias Kovatsch

ANIMA Working Group Interim Meeting, April 19, 2024
CDDL usage in BRSKI-PRM

Background

- Took over the usage of CDDL for BRSKI-PRM status messages from RFC 8995
- Based on the Shepherd review CDDL is now been used in BRSKI-PRM version 12, were no YANG module is available (formerly described based on JSON examples)
- During IETF 119 ANIMA WG meeting comment was received regarding CDDL definition for the enroll-trigger (pledgeenrollrequesttrigger), which is defined as
  ```
  pledgeenrollrequesttrigger = {
    "enroll-type": "enroll-generic-cert"
  }
  ```
- Current definition is limited to one concrete value: “enroll-generic-cert”
- Intention to be flexible for different values for "enroll-type" for further use cases, BRSKI-PRM currently only defines: “enroll-generic-cert”
- Proposal to be discussed (next slide)
CDDL usage in BRSKI-PRM
Proposal

- Goal: Define option to carry a single value of "enroll-type" at a time. Wildcard character for the string are not needed.

- Proposed CDDL

```cddl
pledgeenrollrequesttrigger = {
    "enroll-type": { $$arbitrary-enrolltypestring }
}
```

with additional explanation:

In the context of BRSKI-PRM the value of: $$arbitrary-enrolltypestring
is defined as: "enroll-generic-cert"
to request the pledge to create a CSR for a generic LDevID certificate.
Other specifications using this mechanism may define further values, e.g., to bootstrap application related certificates, e.g. with value "enroll-app-cert"

- Correct proposal?

4/18/2024