draft-fieau-cdni-interfaces-https-delegation-01

CDNI WG

Frédéric Fieau, Emile Stephan   Orange

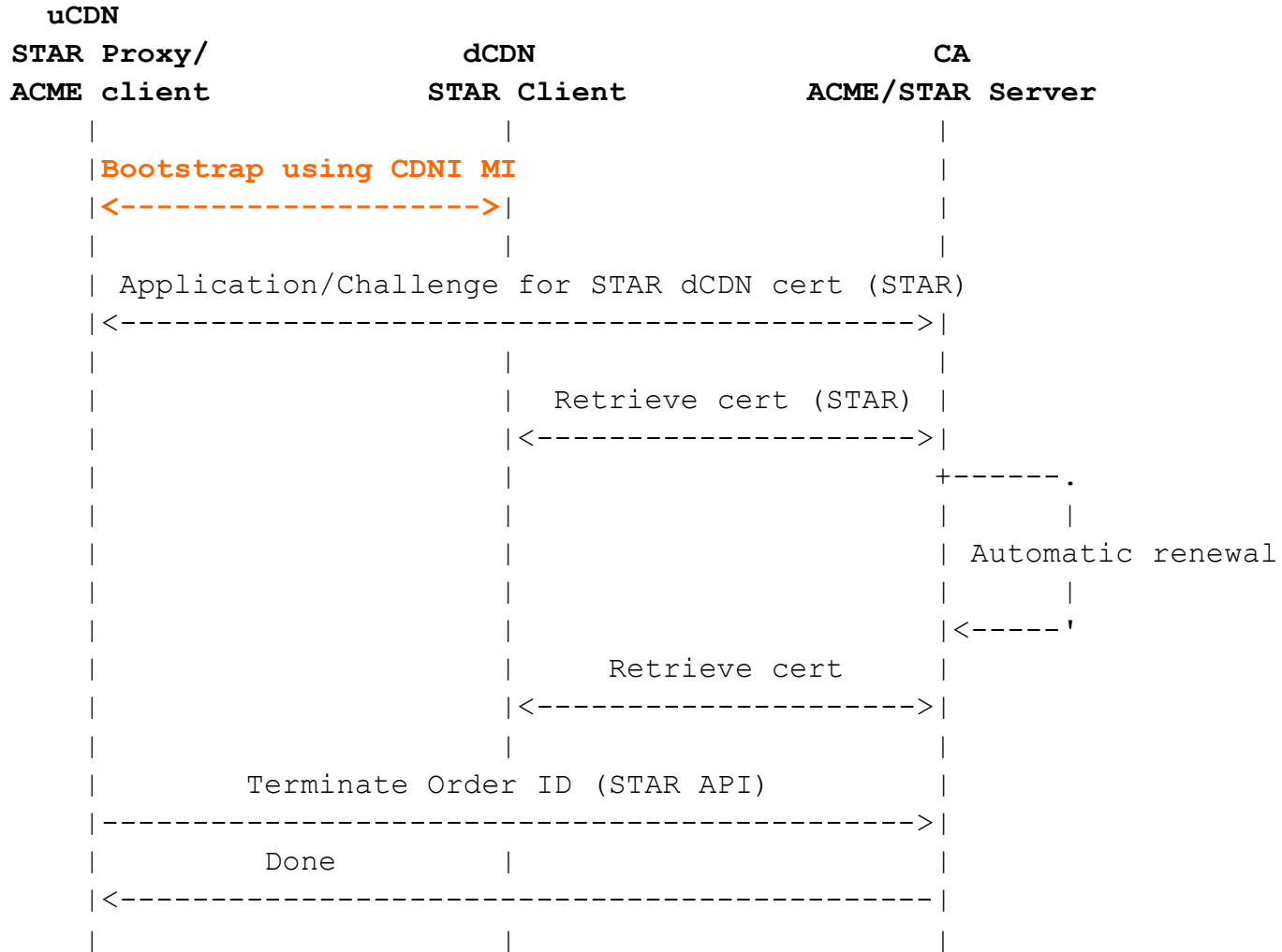Sanjay Mishra   Verizon

IETF 99 – Prague

Adding HTTPS delegation support to metadata interface

- draft-fieau-cdni-interfaces-https-delegation proposes an update to the CDNi interfaces to take into account HTTPS delegation mechanisms the IETF is working on.

- The current version adds objects to the metadata interface (RFC8006) to support draft-ietf-acme-star-00 Short Term Automatically Renewed certificates:

  – provides the dCDN (START NDC entity) with information about credentials renewal the CA is producing on behalf of uCDN (DNO STAR entity)

STAR call-flow in CDNI

```
       uCDN
    STAR Proxy/                  dCDN                        CA
    ACME client              STAR Client           ACME/STAR Server
         |                        |                        |
         |Bootstrap using CDNI MI |                        |
         |<---------------------->|                        |
         |                        |                        |
         | Application/Challenge for STAR dCDN cert (STAR)  |
         |<----------------------------------------------->|
         |                        |                        |
         |                        | Retrieve cert (STAR) |
         |                        |<-------------------->|
         |                        |                   +------.
         |                        |                   |      |
         |                        |                   | Automatic renewal
         |                        |                   |      |
         |                        |                   |<-----'
         |                        | Retrieve cert   |
         |                        |<-------------------->|
         |                        |                        |
         | Terminate Order ID (STAR API)                   |
         |----------------------------------------------->|
         |        Done            |                        |
         |<-----------------------------------------------|
         |                        |                        |
```

Proposed MI objects to handle delegation

SecuredDelegation :
```
{
      "generic-metadata-type": "MI.SecuredDelegation",
      "generic-metadata-value":
      {
         "timewindow": TimeWindowACL,
         "delegationMethod": AcmeStarDelegationMethod,
         "pathpattern": PathPattern,
         "delegatedDomain": HostMatch,
      }
}

            AcmeStarDelegationMethod:
            {
                  "generic-metadata-type": "MI.AcmeStarDelegationMethod",
                  "generic-metadata-value": {
                     "starproxy": Endpoint,
                     "acmeserver": Endpoint,
                     "credentialslocationuri": Link,
                     "periodicity": Periodicity
                  }
            }
```

Next steps discussions

- Add support for Ekr subcerts (draft-rescorla-tls-subcerts)

- Discuss other delegation solutions for CDNI

- Identify changes on the other CDNI interfaces for supporting HTTPS delegation.

- Discuss bootstrap using CDNI MI