draft-fieau-cdni-interfaces-https-delegation-04

CDNI WG

Frédéric Fieau, Emile Stephan — Orange
Sanjay Mishra — Verizon

IETF 102 – Montreal
July 2018

Agenda

- Motivation for standardizing delegation for CDNI
- Update since last proposal
- Metadata examples
- Other areas for consideration

Motivations for HTTPS Delegation for CDNI

- HTTPS traffic delegation
  - Security: how to manage certificates/private keys between delegated and delegating entities
  - Several delegation methods are currently being proposed at the IETF: STAR, SubCerts and LURK ... for provisioning HTTPS delivery credentials.

- Delegation issues in CDNI
  - dCDNs are currently not aware of supported delegation methods by uCDN
  - Metadata should describe how to bootstrap delegation methods between both CDNs – uCDN and dCDN.

- Common framework for HTTPS delegation
  - Provide for a standard based delegation scheme utilizing CDNI metadata
  - Applicable to CDNs without a footprint in a specific serving area and/or between a CDN and the last mile delivery

Updates to `draft-fieau-cdni-interfaces-https-delegation` since -02

- ***`draft-fieau-cdni-interfaces-https-delegation`*** proposes extensions to the CDNi interfaces to exchange delegation metadata.

- This -04 version has textual and metadata model edits

- The current draft supports delegation methods objects:
  - Short Term Automatically Renewed certificates (STAR)
    - https://datatracker.ietf.org/doc/draft-ietf-acme-star/
  - Delegated Credentials for TLS / SubCerts
    - https://datatracker.ietf.org/doc/draft-ietf-tls-subcerts/
  - **New: LURK**
    - https://datatracker.ietf.org/doc/draft-mglt-lurk-lurk/
    - https://datatracker.ietf.org/doc/draft-mglt-lurk-tls12/
    - https://tools.ietf.org/html/draft-mglt-lurk-tls13-00

Added: Support for LURK draft-mglt-lurk-tls

- Use case:
  - uCDN delegates HTTPS delivery to dCDN using its own credentials derived from a KeyServer

- Proposal:
  - Add a new metadata object in RFC8006 to support the LURK draft (draft-mglt-lurk-tls).

```
LurkDelegationMethod: {
        "generic-metadata-type": "MI.LurkDelegationMethod",
        "generic-metadata-value": {
            "keyserver": Endpoint,
         }
}
```

Example

```
PathMatch:
{
   "path-pattern": {
      "pattern": "/movies/*",
      "case-sensitive": true},
   "path-Metadata": {
      "type": "MI.PathMetadata",
      "href": "https://metadata.ucdn/video.example.com/movies"}
}

PathMetadata:
{
   "metadata": [
      {
      "generic-metadata-type": "MI.SecureDelegation"
      "generic-metadata-value": {
         "methods ": [“MI.AcmeStarDelegationMethod”,
                 “MI.LurkDelegationMethod”]
      }
   }]
}
```

Delegation Extension to PathMetaData

- uCDN is delegating HTTPS delivery to dCDN, and it needs to convey information about how delegation is enforced.
- We propose an extension to PathMetadata (RFC8006) through the « MI.SecureDelegation » object that allows the uCDN to describe delegation information to a dCDN.
- This method involves the definition of the delegation metadata for each path URL of the delegated entity (dCDN)

```
PathMetadata:
{
    "metadata": [
        {
        "generic-metadata-type": "MI.SecureDelegation"
        "generic-metadata-type": {
            "methods ": Array of DelegationMethods
        }
    }]
}
```

Example updated from draft –05: without MI.SecureDelegation

The presence (or lack thereof) of an AcmeStarDelegationMethod, SubcertsDelegationMethod, and/or LurkDelegationMethod imply support (or lack thereof) for the given method.

PathMetadata:

```
{
    "metadata": [
        {
        "generic-metadata-type": "MI.AcmeStarDelegationMethod"
        "generic-metadata-value": {
          "starproxy": "10.2.2.2",
          "acmeserver" : "10.2.3.3",
          "credentialslocationuri": “www.ucdn.com/credentials",
          "periodicity": 36000
        },
        {
        "generic-metadata-type": "MI.LurkDelegationMethod"
        "generic-metadata-value": {
           "keyserver": “10.2.2.2”,
        }
    }]
}
```

Other areas for consideration

- Identify other needs on CDNI interfaces for supporting HTTPS delegation, e.g.:
  - Capabilities interface: advertise supported delegation methods,
  - Control interface: force credential renew, or revoke delegation

Thank you

Backup

Support for ACME/STAR draft-ietf-acme-star

- Use case:
  - uCDN delegates HTTPS delivery to dCDN requesting the CA to issue a short-term automatically renewed certificate.

- Proposal:
  - Add metadata object in RFC8006 to support the draft ACME/STAR delegation model (draft-ietf-acme-star).

```
AcmeStarDelegationMethod: {
    "generic-metadata-type": "MI.AcmeStarDelegationMethod",
    "generic-metadata-value": {
        "starproxy": "10.2.2.2",
        "acmeserver" : "10.2.3.3",
        "credentialslocationuri": “www.ucdn.com/credentials",
        "periodicity": 36000
    }
}
```

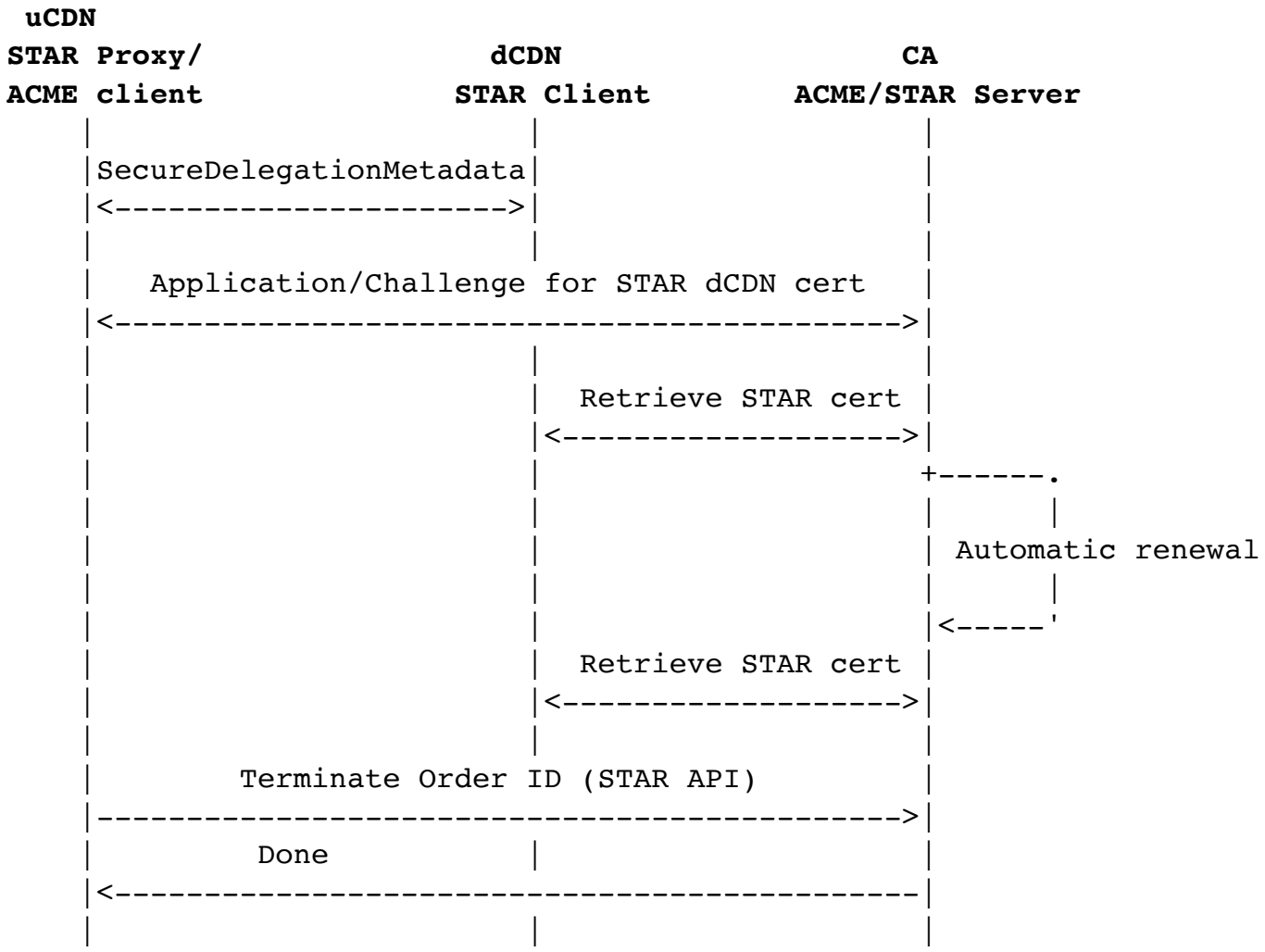
Support for TLS/SubCerts draft-ietf-tls-subcerts

- Use case:
  - uCDN delegates HTTPS delivery to dCDN using its own credentials without the need to request a certificate from the CA

- Proposal:
  - Add a new metadata object in RFC8006 to support the draft TLS/SubCerts delegation model (draft-ietf-tls-subcerts).

```
SubCertDelegationMethod: {
        "generic-metadata-type": "MI.SubcertsDelegationMethod",
        "generic-metadata-value": {
            "credentialsdelegatingentity": Endpoint,
            "credentialrecipiententity": Endpoint,
            "credentialslocationuri": Link,
            "periodicity": Periodicity
        }
}
```

STAR call-flow in CDNI



Limited Usage of Remote Keys