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
Motivation for HTTPS Delegation for CDNI

- Metadata for HTTPS Delegation?
  - dCDNs are currently not aware of supported delegation methods by uCDN
  - Adding delegation metadata enables CDNs to become aware of one or more delegation methods (without the need for shared private keys)

- Develop a common framework for HTTPS delegation
  - Integrate standards based delegation scheme to CDNI metadata
  - Would want to add Metadata that describes how to bootstrap delegation methods between the uCDN and dCDN.

- HTTPS traffic delegation
  - Does not changes Security
    - Not in scope to instruct how to manage certificates
    - Provides a means to communicate supported HTTPS delegation methods

- Several delegation methods are currently being proposed in the IETF:
  - STAR
  - SubCerts
  - LURK
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)
  - Delegated Credentials for TLS / SubCerts
  - **New: LURK**
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:

```json
{
    "metadata": [
        {
            "generic-metadata-type": "MI.SecureDelegation"
        }
    ]
}
```
Example updated from draft –05: without MI.SecureDelegation

Explicitly indicate support method such as AcmeStarDelegationMethod and/or SubcertsDelegationMethod, and/or LurkDelegationMethod:

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"
            }
        }
    ]
}
Questions?
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).

```json
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).

```json
SubCertDelegationMethod: {
  "generic-metadata-type": "MI.SubcertsDelegationMethod",
  "generic-metadata-value": {
    "credentialsdelegatingentity": Endpoint,
    "credentialrecipiententity": Endpoint,
    "credentialslocationuri": Link,
    "periodicity": Periodicity
  }
}
```
STAR call-flow in CDNI

```
<table>
<thead>
<tr>
<th>uCDN</th>
<th>dCDN</th>
<th>CA</th>
</tr>
</thead>
<tbody>
<tr>
<td>STAR Proxy/</td>
<td>STAR Client</td>
<td>ACME/STAR Server</td>
</tr>
<tr>
<td>ACME client</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SecureDelegationMetadata</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;----------------------&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application/Challenge for STAR dCDN cert</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;----------------------&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Retrieve STAR cert</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;----------------------&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>+--------.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Automatic renewal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;------'</td>
</tr>
<tr>
<td></td>
<td>Retrieve STAR cert</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;----------------------&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Terminate Order ID (STAR API)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;----------------------&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Done</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;----------------------&gt;</td>
<td></td>
</tr>
</tbody>
</table>
```
Limited Usage of Remote Keys