

# **draft-fieau-cdni-interfaces-https- delegation-05**

## **CDNI WG**

Frédéric Fieau, Emile Stephan  
Sanjay Mishra

Orange  
Verizon

IETF 103 – Bangkok

# Agenda

- Update since last proposal
- Next steps

# Updates to *draft-fieau-cdni-interfaces-https-delegation*

- *draft-fieau-cdni-interfaces-https-delegation* proposes extensions to the CDNI interfaces to exchange delegation metadata.
- This -05 version reflects the last comments in Montreal
  - supports the delegation methods objects:
    - Short Term Automatically Renewed certificates (STAR) - *draft-ietf-acme-star*
    - Delegated Credentials for TLS / SubCerts - *draft-ietf-tls-subcerts*
  - Removed Lurk from this version
  - PathMetaData includes the delegation methods to be used

## Next steps

- Now calling for adoption

Thank you

backup

## 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

# SecureDelegation object over 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

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-type": {
        "methods": ["MI.AcmeStarDelegationMethod",
                    "MI.LurkDelegationMethod"]
      }
    }
  ]
}
```

# 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

