draft-ietf-cdni-interfaces-https-delegation

IETF 111 - CDNI WG

Frederic Fieau, Emile Stephan - July 27th, 2021

About Certificate sharing based Delegation methods

- RFC 8739 (STAR)
- STAR Delegation
- Delegated Credentials (Internet Draft)

HTTPS Delegation

- Internet Draft https://datatracker.ietf.org/doc/draft-ietf-cdni-interfaces-https-delegation/ - v05
  - Defines constructs using CDNI Metadata interfaces to enable content delegation for the “certificate” based content delegation
  - I-D is adopted as a WG in CDNI WG

CDNI extensions to support Delegation

- Internet Draft, CDNI HTTPS Delegation CDNI extension to the current Metadata interface model that allows bootstrapping delegation methods between a uCDN and a delegate dCDN

- Proposed extension reuses PathMetadata object, as defined in [RFC8006], and adds new "Delegation methods" objects:
  - AcmeStarDelegationMethod
  - SubcertsDelegationMethod

HTTPS Delegation Usage:

PathMetadata can be modeled for ACMEStarDelegationMethod as follows:

PathMetadata:

```
{
"metadata": [
    {
        "generic-metadata-type": "MI.AcmeStarDelegationMethod",
        "generic-metadata-value": {
        "star-proxy": "10.2.2.2",
        "acme-server" : "10.2.3.3",
        "credentials-location-uri": "www.ucdn.com/credentials",
        "periodicity": 36000,
        "CSR-template": Json/Text representing the CSR template (see section 4.2)
    }}]
}
```

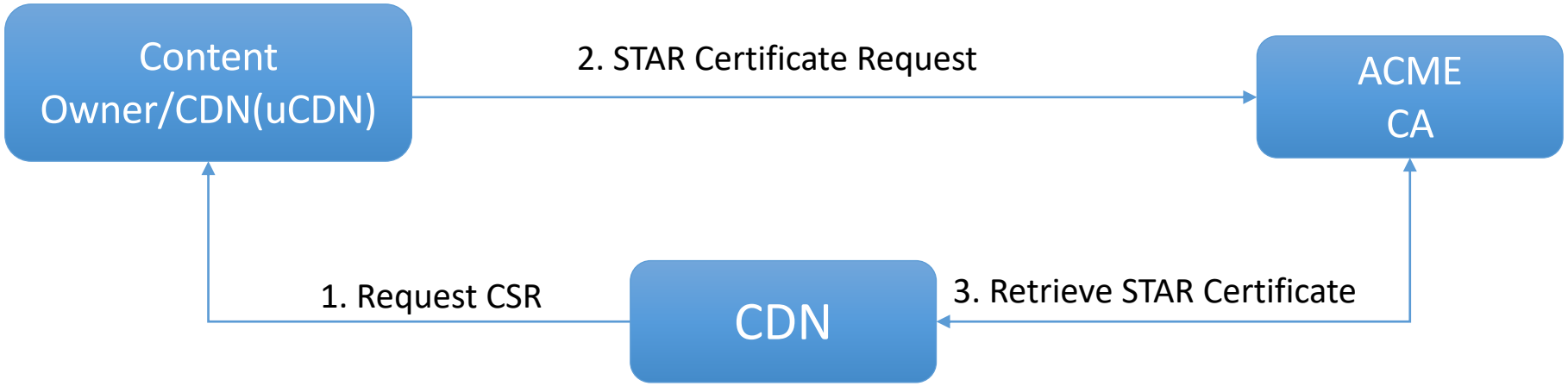
What’s next?

- Confirm Delegated Credentials call-flow
- Find new contributors to the draft

Thank you

Annex

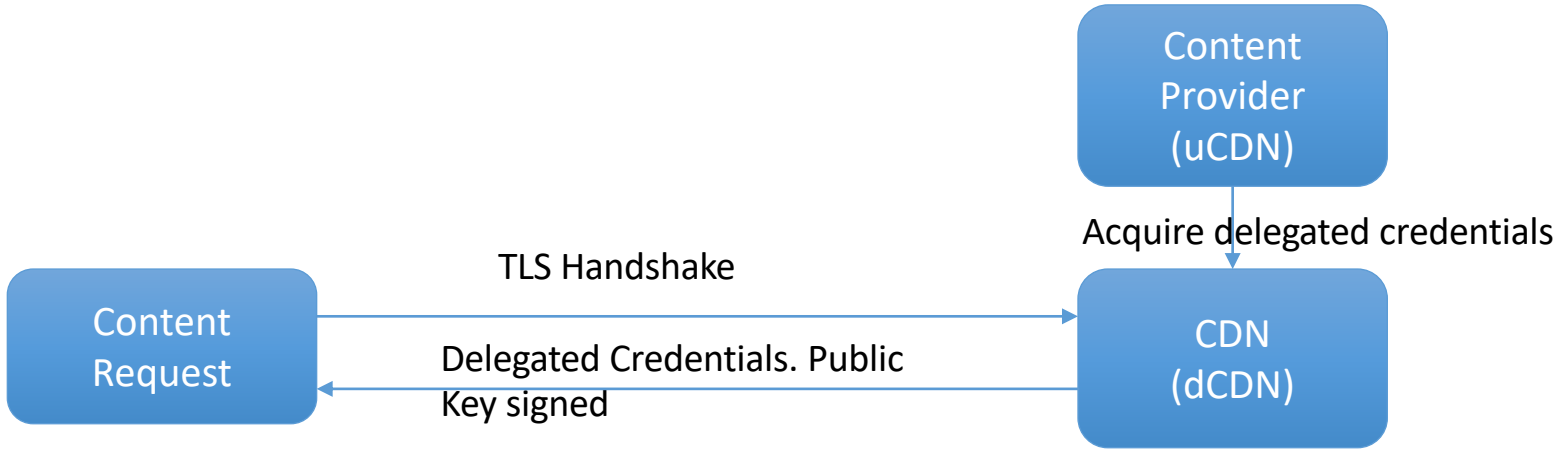
Short-term Automatically Renewed Certificate (STAR)



- CP/uCDN (Domain owner) registers with the CA over the ACME protocol (RFC 8739)
- dCDN establishes an ACME account with uCDN
  - uCDN controls policies such as what domain names and cert. validity period
- dCDN issues to uCDN a Certificate Singing Request (CSR) based upon agreed template (STAR Delegation)
- dCDN retrieves certificate from the ACME CA (STAR Delegation)

https://www.rfc-editor.org/rfc/rfc8739.pdf

Delegated Credentials



- Optional extension advertised by the client in ClientHello during TLS handshake
- Server replies with an extension containing a “Delegated Credential”
  - Public key
  - Validity Period
  - Additional constraints (maybe)
  - Signed by delegator’s private key
- CertificateVerify uses key from Delegated Credential instead of Certificate

https://tools.ietf.org/pdf/draft-ietf-tls-subcerts-00.pdf