

# draft-ietf-cdni-https- delegation-subcerts-03

IETF 117 – CDNI WG

Christoph Neumann – July 26th, 2023

# Scope

Specifies MI and FCI objects enabling HTTPS delegation in CDNI based on “Delegated Credentials for (D)TLS” as defined in IETF TLS WG: draft-ietf-tls-subcerts

Two objects defined:

- FCI.DelegatedCredentials
- MI.DelegatedCredentials

# Defined objects examples

## FCI.DelegatedCredentials

- Allows the dCDN to announce the maximum number of delegated credentials supported ; typically, but not necessarily linked with the number of servers

```
{ "capabilities": [  
  {  
    "capability-type": "FCI.DelegatedCredentials",  
    "capability-value": {  
      "number-delegated-certs-supported": 3  
    }  
    "footprints": [  
      <Footprint objects>  
    ]  
  }  
]
```

## MI.DelegatedCredentials

- Contains an array of delegated credentials
- Allows the uCDN to push a set of delegated credentials to the dCDN

```
{ "generic-metadata-type": "MI.DelegatedCredentials",  
  "generic-metadata-value": {  
    "delegated-credentials": [  
      {"delegated-credential":  
        "cBBfm8KK6pPz/tdgKyedwA...  
        iXCCIAmzMM0R8FLI3Ba0UQ=="},  
      {"delegated-credential":  
        "4pylGtjFdys1+9y/4sS/Fg...  
        J+h9lnRY/xgmi65RLGKoRw=="},  
      {"delegated-credential":  
        "6PWFO0g2AXvUaULXLObcVA...  
        HXoldT/qaYCCNEyCc8JM2A=="}}]  
  }  
}
```

# Changes since last meeting

- Typos, reformulation and text polishing
- Added RFC2119 boilerplate + MUST/SHOULD clarifications
  - The uCDN SHOULD keep track of distributed certs and expiration times and the uCDN SHOULD refresh the certs after expiration
    - There might be valid reasons for a uCDN not to keep track of certificate validity periods and refresh the certs (e.g., single shot deployments, deprovisioning of dCDN)
- Delegated-credential property now base64 encoded
- Security consideration section expanded
  - passing key material through the MI is dangerous and should be avoided

# What's next?

- Ask for WGLC

Thank you.