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
  • Allows the dCDN to announce number of delegated credentials supported
  • Typically updated before expiration of delegated credentials (e.g., one day before)
  • Dynamicity of mechanism limited, but could do the job to start with
• MI. DelegatedCredentials now contains an array of delegated credentials
  • Allows the uCDN to push a set of delegated credentials to the dCDN

No updates on the document since last IETF meeting
Defined objects examples

FCI.DelegatedCredentials

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

MI.DelegatedCredentials

{
  "generic-metadata-type": "MI.DelegatedCredentials",
  "generic-metadata-value": {
    "delegated-credentials": [
      {
        "delegated-credential": "70105f9bc28aea93f3fed7602b279dc0...8970822009b330cd11f052c8dc16b451"},
      {
        "delegated-credential": "e29c881ad8c5772b35fbdcbfe2c4bf16...27e87d967458ff18268bae512c62a847"},
      {
        "delegated-credential": "e8f5853b4836017bd46942d72ce6dc54...1d7a25753fea698082344c8273c24cd8"}
    ]
  }
}
}
Ongoing discussion on delegated credential renewal and fetching mechanism

The currently proposed FCI.DelegatedCredentials object offers limited dynamicity regarding credential renewal and fetching. FCI is used as a signaling mechanism, which goes far beyond the original capabilities' announcement.

Two alternatives:

1. Kevin proposed to remove FCI.DelegatedCredentials
   - Instead, rely on linked MI. DelegatedCredentials objects (instead of embedded objects)
     - Set a HTTP cache duration of zero for these objects
     - Would allow the dCDN to fetch as many and new MI objects as needed
   - New proposal is tweaking a bit the spirit/idea of the original CDNI Metadata interface
   - Not supported by SVTA

2. Broapeak proposal to slightly change the semantic attached to FCI.DelegatedCredentials object
   - FCI object allows the dCDN to announce the maximum number of delegated credentials supported; typically, but not necessarily linked with the number of servers
   - FCI object is not used to cope with expiry and renewal of delegated credential ➔ uCDN knowing the renewal period, uCDN must refresh/push new credentials through MI interface
   - uCDN must provision on time the dCDN with delegated credentials according to the dCDN capability

➤ Opinions, discussion?
Thank you.