draft-ietf-cdni-https-delegation-subcerts-00

History
• Update of draft-fieau-interfaces-https-delegation-subcerts-01
• Now a WG Internet-Draft

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
Changes compared to draft-fieau-interfaces-https-delegation-subcerts-01

• Removed delegated credential fetching mechanism via HTTP GET
  • Such interface is probably out of scope of CDNI. We may want to define such mechanism in some other group/body.
  • Removed MI.ConfDelegatedCredentials (contained URL to fetch delegated credentials).

• Introduced FCI.DelegatedCredentials
  • Allows the dCDN to announce number of delegated credentials needed
  • 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
Defined objects examples

FCI.DelegatedCredentials

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

MI.DelegatedCredentials

{  
  "generic-metadata-type": "MI.DelegatedCredentials",  
  "generic-metadata-value": {  
    "delegated-credentials": [  
      {"delegated-credential":  
        "70105f9bc28aea93f3fed7602b279dc0...8970822009b330cd11f052c8dc16b451"},  
      {"delegated-credential":  
        "e29c881ad8c5772b35fbdcbfe2c4bf16...27e87d967458ff18268bae512c62a847"},  
      {"delegated-credential":  
        "e8f5853b4836017bd46942d72ce6dc54...1d7a25753fea698082344c8273c24cd8"}  
    ]  
  }  
}
Objects definition

**FCI.DelegatedCredentials**

Property: number-delegated-certs-needed
Description: Number of delegated credentials needed by the dCDN.
Type: integer
Mandatory-to-Specify: Yes

**MI.DelegatedCredentials**

Property: delegated-credentials
Description: Array of delegated credentials.
Type: array
Mandatory-to-Specify: Yes

Each item of the array is composed of the properties:

- Property: delegated-credential
  Description: hex-encoded delegated credential structure DelegatedCredential as defined in [I-D.ietf-tls-subcerts].
  Mandatory-to-Specify: Yes

- Property: private-key
  Description: private key corresponding to the public key contained in the DelegatedCredential.
  Mandatory-to-Specify: No
Other changes compared to draft-fieau-interfaces-https-delegation-subcerts-01

• Added security considerations and privacy considerations sections
• Private keys optional in DelegatedCredential object.
  • Allows the dCDN to handle delegated credentials key generation (or to provide these keys via other means)
  • How public keys of the dCDN are communicated to uCDN is currently out of scope of draft