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
Changes since last meeting

SecDir early review of previous version of draft
  • Pointed out that private key cannot be passed in clear text in an MI object

New version of draft: if used, the private key property of MI.DelegatedCredentials MUST be encrypted using JOSE/JWE envelope
  • Public key used for encryption is announced in the FCI.DelegatedCredentials property “PrivateKeyEncryptionKey”
Defined objects – Recap and 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
- Properties
  - number-delegated-certs-supported (mandatory)
  - PrivateKeyEncryptionKey (optional)

```json
{
  "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
- Properties:
  - delegated-credentials [array] (mandatory)
    - delegated-credential (mandatory)
    - private-key (optional)

```json
{
  "generic-metadata-type": "MI.DelegatedCredentials",
  "generic-metadata-value": {
    "delegated-credentials": [
      {
        "delegated-credential":
        "cBBfm8KK6pPz/tdgKyedwA...iXCCIAmzMM0R8FLi3Ba0UQ=="},
      {
        "delegated-credential":
        "4pyIGtjFdys1+9y/4sS/Fg...J+h9lnRY/xgmi65RLGKoRw=="},
      {
        "delegated-credential":
        "6PWFO0g2AXvUaULXLObcVA...HXoldT/qaYCCNEyeCc8JM2A=="}
    ]
  }
}
```
What’s next?

• Ask for WGLC
Thank you.