CDNI Protected Secrets Metadata

draft-rosenblum-cdni-protected-secrets-metadata-00

Ben Rosenblum
CDNI WG, IETF 116
March 27, 2023

Objectives

- Provide a secure bi-directional mechanism for exchange of sensitive values (e.g., auth tokens) in the context of Capability Advertisements and Configuration Metadata

- Allow this mechanism to function without any required out-of-band communication via embedded cryptographic messages

- But also support reference to external services like HashiCorp Vault in place of the in-band mechanism

MI.SecretStore

- Define the configuration for associated `MI.SecretValue`
  - An embedded message in CMS (RFC5652) format OR
  - A cleartext value for development and test environments OR
  - Either a reference to an external service

```
{
  "secret-store-id": "store-1",
  "secret-store-type": "MI.SecretStoreTypeEmbedded",
  "secret-store-certificate-id": "cert-1",
  "secret-store-config": {
      "format": "cms"
  }
}
```

```
{
  "secret-store-id": "store-1",
  "secret-store-type": "MI.SecretStoreTypeEmbedded",
  "secret-store-config": {
      "format": "cleartext"
  }
}
```

```
{
  "secret-store-id": "store-2-vaultv2",
  "secret-store-type": "MI.SecretStoreTypeVault",
  "secret-store-config": {
      "endpoint": "https://vault.example.com/v1/secret",
      "version": 2,
      "namespace": "customer-1"
  }
}
```

MI.SecretValue

- The object container for embedded CMS values or for references to secrets stored on an external service

- Consists of a reference to the MI.SecretStore configuration and either a "secret-value" or "secret-path" property

- Used as a property value inside other MI or FCI objects which contain secret data

```
{
  "secret-store-id": "store-2-vaultv1",
  "secret-path": "bar/baz/importantsecret"
}
```

```
{
  "secret-store-id": "store-1-cms",
  "secret-value": "MIIBiQYJKoZIhvcNAQcDoIIBejCCAXYCAQAxggEhMIIBHQI
    BADAFMAACAQEwDQYJKoZIhvcNAQEBBQAEggEApJeXzsUS1jbAyNtQiJ9um9IMI
    HW5B2g+gHnXdNSTyd33OEfTR6yLSZihBlFbHpY3qSzK1CX7RF5Oz3SqLDW+r3i
    1D/aHbVXwQbviWHEvHterql8l9VDm2FCNaDx5vihdbtvng3+/vdJNNMMhmovwZ
    L5uhPsK81DkKwZCvznMMWt8YdNSFGT62f73ash7Eg/mS54IUyYOJHYrXEkRLSj
    vl0j+JqcIR8hCOCA78+5bS4MgfdsS9xxSwQTrPru6EdTivMDKE/jlKg7li8lWd
    irWqtv0za5gLmH5T+zslXIoklwERAE50Jj8FxZD98EikKH8DAa+JeFsBm6Z1+y
    VFsWucTBMBgkqhkiG9w0BBwEwHQYJYIZIAWUDBAEqBBBws1riXA6m336zRbsiK
    trVgCA267133v2zD/wjFQHXrKSJfd/2YJaxPskgdmQaVlgWCw=="
}
```

MI.SecretCertificate

- Communicates a PEM format X.509 cert to the other party for use in a `MI.SecretStore` of type `MI.SecretStoreTypeEmbedded`


```
{
  "certificate-id": "cert-1",
  "certificate-value": "MIIDZTCCAk2gAwIBAgIUFJokJzAxDgUGsBd8uhSblpMwSLAwDQYJKoZIhvcNAQELBQAwQjELM
    AkGA1UEBhMCVVMxEDAOBgNVBAgMB0dlb3JnaWExITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDAeFw0yMz
    AxMjMyMDM2MDNaFw0yMzAyMjIyMDM2MDNaMEIxCzAJBgNVBAYTAlVTMRAwDgYDVQQIDAdHZW9yZ2lhMSEwHwYDVQQKDBh
    JbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCT11o9yebJmjiq7mXb
    Ltnr5THpTnyahNpKECI+N8YZSl5+cS9hGa06zKQV3MNxbjJ15smmeWbgynYGwqhs5ZXGUjzd8S1/M1A08z1VFhEJiODQ0
    0f3BOocpIn25RQzFz/BOLREW7sLkrhuz/WVBR3bzp6T1gu3nKcRSNuNxO1p9490gS1LhsZYQKfNvncuxBCP0GTNbUOXd6
    xkQ+EX5cEKoODUYWzOMdMAMlEEFb4jUjxYbbJoygwTMHpG2yGAQ2IXpB2/wrrawivxDHlMHGpML+Ie8o6YBR4PDiOJmlC
    g9uIsirf65R1zhfcCxmNQ7z/IggC0WNQjZwymeZT9cFDdAgMBAAGjUzBRMB0GA1UdDgQWBBQb5eJeYLEpErJetb1eid5B
    gsS3uTAfBgNVHSMEGDAWgBQb5eJeYLEpErJetb1eid5BgsS3uTAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA
    4IBAQBURnrjVbHVwfV/u/xjzK8p4dTke0xb0oKt0J5YeH95sRa66m3tQJYf0jbMNQ8InfXK0IzGM/uUOJX3daeOMQxMbJ
    vaUDZV64kuU6IgkEQuLwkOP5k0Rc9+SuRMlvWOB2exiyQkd2iHJtURuEtvB39LIr4pPDsicBAYxsm5ybIWCmqNMPkVl8Q
    ks3lAXeF+xvH11tmciTJSYP0Ud2psbV3lduD76UT2bzDGkr690KqroNS57WbQrHxEhtMbdq0cPfzqFlxyhckqNYrcw2v1
    igQDhplQ2eUc4ye0Mvimj1Me2mWjPvilhvS3vDGhrmcx9mlishlI/RFy6yDI1gtkF7eS"
}
```



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            14:9a:24:27:30:31:0e:05:06:b0:17:7c:ba:14:9b:96:93:30:48:b0
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = Georgia, O = Internet Widgits Pty Ltd
        Validity
            Not Before: Jan 23 20:36:03 2023 GMT
            Not After : Feb 22 20:36:03 2023 GMT
        Subject: C = US, ST = Georgia, O = Internet Widgits Pty Ltd
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:93:d7:5a:3d:c9:e6:c9:9a:38:aa:ee:65:db:2e:
                    d9:eb:e5:31:e9:4e:7c:9a:84:da:4a:10:22:3e:37:
                    c6:19:4a:5e:7e:71:2f:61:19:ad:3a:cc:a4:15:dc:
                    c3:71:6e:32:75:e6:c9:a6:79:66:e0:ca:76:06:c2:
                    a8:6c:e5:95:c6:52:3c:dd:f1:2d:7f:33:50:34:f3:
                    3d:55:16:11:09:88:e0:d0:d3:47:f7:04:ea:1c:a4:
                    89:f6:e5:14:33:17:3f:c1:38:b4:44:5b:bb:0b:92:
                    b8:6e:cf:f5:95:05:1d:db:ce:9e:93:d6:0b:b7:9c:
                    a7:11:48:db:8d:c4:ed:69:f7:8f:74:81:2d:4b:86:
                    c6:58:40:a7:cd:be:77:2e:c4:10:8f:d0:64:cd:6d:
                    43:97:77:ac:64:43:e1:17:e5:c1:0a:a0:e0:d4:61:
                    6c:ce:31:d3:00:32:51:04:15:be:23:52:3c:58:6d:
                    b2:68:ca:0c:13:30:7a:46:db:21:80:43:62:17:a4:
                    1d:bf:c2:ba:da:c2:2b:f1:0c:79:4c:1c:6a:4c:2f:
                    e2:1e:f2:8e:98:05:1e:0f:0e:23:89:9a:50:a0:f6:
                    e2:2c:8a:b7:fa:e5:1d:73:85:f7:02:c6:63:50:ef:
                    3f:c8:82:00:b4:58:d4:23:67:0c:a6:79:94:fd:70:
                    50:dd
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                1B:E5:E2:5E:60:B1:29:12:B2:5E:B5:BD:5E:89:DE:41:82:C4:B7:B9
            X509v3 Authority Key Identifier:
                keyid:1B:E5:E2:5E:60:B1:29:12:B2:5E:B5:BD:5E:89:DE:41:82:C4:B7:B9
```

FCI Wrappers

Allow use of `MI.SecretStore` and `MI.SecretStoreCertificate` from the Advertisement side for bi-directional exchange of secrets

```
{
  "capabilities": [
    {
      "capability-type": "FCI.SecretStore",
      "capability-value": {
        "secret-store-id": "store-1",
        "secret-store-type": "MI.SecretStoreTypeEmbedded",
        "secret-store-config": {
          "format": "cms"
        }
      }
    }
  ]
}
```

```
{
  "capabilities": [
    {
      "capability-type": "FCI.SecretCertificate",
      "capability-value": {
        "certificate-id": "cert-1",
        "certificate-value": "MIIDZTCCAk2gAwIBAgIUFJokJzAxDgUGsBd8uhSblpMwSLAwDQYJKoZIhvcNAQELB
          QAwQjELMAkGA1UEBhMCVVMxEDAOBgNVBAgMB0dlb3JnaWExITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUH
          R5IEx0ZDAeFw0yMzAxMjMyMDM2MDNaFw0yMzAyMjIyMDM2MDNaMEIxCzAJBgNVBAYTAlVTMRAwDgYDVQQIDAd
          HZW9yZ2lhMSEwHwYDVQQKDBhJbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQwggEiMA0GCSqGSIb3DQEBAQUAA4IB
          DwAwggEKAoIBAQCT11o9yebJmjiq7mXbLtnr5THpTnyahNpKECI+N8YZSl5+cS9hGa06zKQV3MNxbjJ15smme
          WbgynYGwqhs5ZXGUjzd8S1/M1A08z1VFhEJiODQ00f3BOocpIn25RQzFz/BOLREW7sLkrhuz/WVBR3bzp6T1g
          u3nKcRSNuNxO1p9490gS1LhsZYQKfNvncuxBCP0GTNbUOXd6xkQ+EX5cEKoODUYWzOMdMAMlEEFb4jUjxYbbJ
          oygwTMHpG2yGAQ2IXpB2/wrrawivxDHlMHGpML+Ie8o6YBR4PDiOJmlCg9uIsirf65R1zhfcCxmNQ7z/IggC0
          WNQjZwymeZT9cFDdAgMBAAGjUzBRMB0GA1UdDgQWBBQb5eJeYLEpErJetb1eid5BgsS3uTAfBgNVHSMEGDAWg
          BQb5eJeYLEpErJetb1eid5BgsS3uTAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBURnrjVb
          HVwfV/u/xjzK8p4dTke0xb0oKt0J5YeH95sRa66m3tQJYf0jbMNQ8InfXK0IzGM/uUOJX3daeOMQxMbJvaUDZ
          V64kuU6IgkEQuLwkOP5k0Rc9+SuRMlvWOB2exiyQkd2iHJtURuEtvB39LIr4pPDsicBAYxsm5ybIWCmqNMPkV
          l8Qks3lAXeF+xvH11tmciTJSYP0Ud2psbV3lduD76UT2bzDGkr690KqroNS57WbQrHxEhtMbdq0cPfzqFlxyh
          ckqNYrcw2v1igQDhplQ2eUc4ye0Mvimj1Me2mWjPvilhvS3vDGhrmcx9mlishlI/RFy6yDI1gtkF7eS"
      }
    }
  ]
}
```