Demonstration: Binding X.509 certificates to DIDs

markus@danubetech.com, 13th August 2022

The DHS SVIP cohort has been discussing how a DID's verification method can be bound to a traditional X.509 certificate chain. This can be useful when considering existing trusted CA infrastructure (e.g. FPKICA, ICAO ePassport, etc.).

Orie Steele (Transmute) has described some experiments using did:web and OpenSSL. The Trust-over-IP Foundation has also worked on the topic of X.509 interoperability. In Rebooting-the-Web-of-Trust #11, an advance paper also covers this topic.

We (Danube Tech) have built an extension of our Universal Resolver EE product that can verify such bindings. It supports the x509CertificateChain property from the W3C Security Vocabulary, as well as the x5c parameter from the JWK specification. In other words, using these constructs, an X.509 certificate can be embedded in one or more verification method(s) in a DID document.

A DID resolver can then verify the binding and return a warning or error in the DID resolution metadata if a verification method in a DID document cannot be traced back to a trusted CA.

Example DIDs that have been created:

DID (click to resolve)	Comment
did:web:danubetech.com:did:test4	Uses 'x509CertificateChain'
did:web:danubetech.com:did:test4-jwk	Uses 'x5c'
did:web:danubetech.com:did:test5	Uses 'x509CertificateChain'
did:web:danubetech.com:did:test5-jwk	Uses 'x5c'
did:web:danubetech.com:did:test6	Uses 'x509CertificateChain'
did:web:danubetech.com:did:test6-jwk	Uses 'x5c'

Demonstration

As part of the DHS SVIP program, Danube Tech has deployed an instance of our Universal Resolver EE product. This instance is protected by OAuth2. The following steps can be executed to demonstrate the X.509 binding functionality.

1. Obtain OAuth2 access token

The following command should return an OAuth2 access token that can be used in the subsequent steps.

```
curl -X POST \
      -H "Authorization: Basic
YjY4Y2I2ZDctNGI5Yi00ODdkLThkZjktM2RkNzg4ZmYyZGEzOm5jalFDYjFJZkhTLW1UTnYuVDBycXV
NdzBK" \
      -H "Content-Type: application/x-www-form-urlencoded" \
      --data grant_type=client_credentials \
      --data scope=resolve:dids \
      "https://auth.uscis.svip.danubetech.com/oauth2/token"
```

2. Resolve DIDs

The first 4 commands contain verification methods that are bound to a trusted certificate chain and should therefore not result in a warning/error. The last 2 commands should return a warning/error in the DID resolution metadata, since the verification methods are not trusted.

Note that a parameter "overrideCertificatePolicy" is passed to the DID resolver, to control the X.509 verification functionality. Possible values of this parameter are "ignore", "warn", "error".

```
curl -X GET \
      -H "Authorization: Bearer ...token.here..." \
"https://resolver.svip.danubetech.com/1.0/identifiers/did%3Aweb%3Adanubetech.co
m%3Adid%3Atest4?overrideCertificatePolicy=warn"

curl -X GET \
      -H "Authorization: Bearer ...token.here..." \
"https://resolver.svip.danubetech.com/1.0/identifiers/did%3Aweb%3Adanubetech.co
m%3Adid%3Atest4-jwk?overrideCertificatePolicy=warn"

curl -X GET \
      -H "Authorization: Bearer ...token.here..." \
"https://resolver.svip.danubetech.com/1.0/identifiers/did%3Aweb%3Adanubetech.co
m%3Adid%3Atest5?overrideCertificatePolicy=warn"

curl -X GET \
      -H "Authorization: Bearer ...token.here..." \
```

```
"https://resolver.svip.danubetech.com/1.0/identifiers/did%3Aweb%3Adanubetech.com%3Adid%3Atest5-jwk?overrideCertificatePolicy=warn"

curl -X GET \
      -H "Authorization: Bearer ...token.here..." \
"https://resolver.svip.danubetech.com/1.0/identifiers/did%3Aweb%3Adanubetech.com%3Adid%3Atest6?overrideCertificatePolicy=warn"

curl -X GET \
      -H "Authorization: Bearer ...token.here..." \
"https://resolver.svip.danubetech.com/1.0/identifiers/did%3Aweb%3Adanubetech.com%3Adid%3Atest6-jwk?overrideCertificatePolicy=warn"
```

Appendix

The following is a root certificate that is configured at the DID resolver to be "trusted".

```
-----BEGIN CERTIFICATE-----
MIIBcTCB+aADAgECAhRvwa6rU7L8ebr71cjKP3OXw/SVeDAKBggqhkjOPQQDAjAS
MRAwDgYDVQQDDAdSb290LWNhMB4XDTIyMDIxNTAxMDg0MloXDTMyMDIxMzAxMDg0
MlowEjEQMA4GA1UEAwwHUm9vdC1jYTB2MBAGByqGSM49AgEGBSuBBAAiA2IABA1V
EmpU3LnlDsK+9yFZXDTaSiQTcteiRZ7fRZ7tNGT5SX8mYGtS6SUTGld7RBVk1uPY
nYTuA3IWKaOGcMhgS8LmlIGs2y6Fs7NK0E1yEyqBDMC2Jbu9MzrLlHcyOWEP2qMQ
MA4wDAYDVR0TBAUwAwEB/zAKBggqhkjOPQQDAgNnADBkAjAZ8ul/Z1dQ2imtko0y
EdICdPCfgr569qgF7cPxft3jKk7IOYd44IVBbJtUHSQMDCACMARj4pCBLego9uBA
JJerM75TK8og6rNPn8XNdyWW2Fw8w9qT3aU7r2lty0owMb3H/g==
-----END CERTIFICATE-----
```