Transport Layer Security (TLS) Authentication with Verifiable Credential (VC)

https://datatracker.ietf.org/doc/draft-vesco-vcauthtls/

Andrea Vesco
Leonardo Perugini
{andrea.vesco, leonardo.perugini}@linksfoundation.com
Self-Sovereign Identity (SSI)

- A decentralized model of digital identity, in which entities have control over the information that they use to prove who they are.

- Identity consists of three components:
  - key pair;
  - Decentralized IDentifier (DID);
  - at least a Verifiable Credential (VC).

- VC and DID are currently in the process of specification by the W3C.
Generation of the Identity

\[
\text{identity} = \{\text{pk, sk}\}
\]

\[
\text{identity} = \{\text{pk, sk, DID}\}
\]

\[
\text{identity} = \{\text{pk, sk, DID, VC}\}
\]
How SSI authentication works

• Currently, SSI authentication occurs at the application layer; two endpoints first establish a TLS channel with server-only authentication using an X.509 certificate.

• Then, the client then sends its VP(VC) to the server for authentication.

• This process works very well for the web.

• However, there may be some cases where SSI authentication could be moved to the TLS layer ....
The IoT domain

• Managing X.509 certificates from enrolment to update and revocation is not straightforward in large-scale IoT systems.

• It may be that the adoption of SSI is a good idea.

• just few examples of pros:
  • an endpoint can update/rotate its key pair without the need of refreshing the VC,
  • an endpoint can revoke immediately its DID,
  • ...

• So, if entities have their own SSI, the VC can be a new Certificate Type for authentication at TLS layer.
A new Certificate Type and Extension

• Adding a new **Certificate Type** called VC in addition to X509 and RawPublicKey in the existing client_certificate_type and server_certificate_type extensions.

• **did_methods**: a new extension containing the list of DID Methods supported by the endpoint to resolve the DID of the peer.

• **Certificate** message will carry the VC content if the VC Certificate Type is selected.
Full TLS handshake with VC

<table>
<thead>
<tr>
<th>DLT</th>
<th>Client</th>
<th>Server</th>
<th>DLT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ClientHello</td>
<td>ServerHello</td>
<td></td>
</tr>
<tr>
<td></td>
<td>server_certificate_type=(VC, X.509)</td>
<td>{EncryptedExtensions}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>client_certificate_type=(VC, X.509)</td>
<td>{server_certificate_type=VC}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>did_methods=(m1, m2)</td>
<td>{client_certificate_type=VC}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{CertificateRequest}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{did_methods=(m1, m2)}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{Certificate}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{CertificateVerify}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{Finished}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>[Application Data]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DID Resolve</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>{Certificate}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>{CertificateVerify}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>{Finished}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[Application Data]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[Application Data]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DID Resolve
Hybrid TLS handshake

Client

ClientHello
server_certificate_type=(X.509)
client_certificate_type=(VC,X.509)

----->

ServerHello
{EncryptedExtensions}
{server_certificate_type=X.509}
{client_certificate_type=VC}
{CertificateRequest}
{did_methods=(m1,m2,m3)}
{Certificate}
{CertificateVerify}
{Finished}

<------- [Application Data]

{Certificate}
{CertificateVerify}
{Finished}

----->

[Application Data]

<------- [Application Data]

DID Resolve

<-------->
What we have already learned

- TLS WG
  - application or domain-specific extensions to TLS are out of scope; the WG usually only considers extensions to the protocol that are widely applicable.

- UTA WG
  - Possible interest in the topic, but extensions are out of scope.

- ?
Resources

I-D [1], OpenSSL [2] and SSI Provider [3]