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

IETF119 - ALLDISPATCH

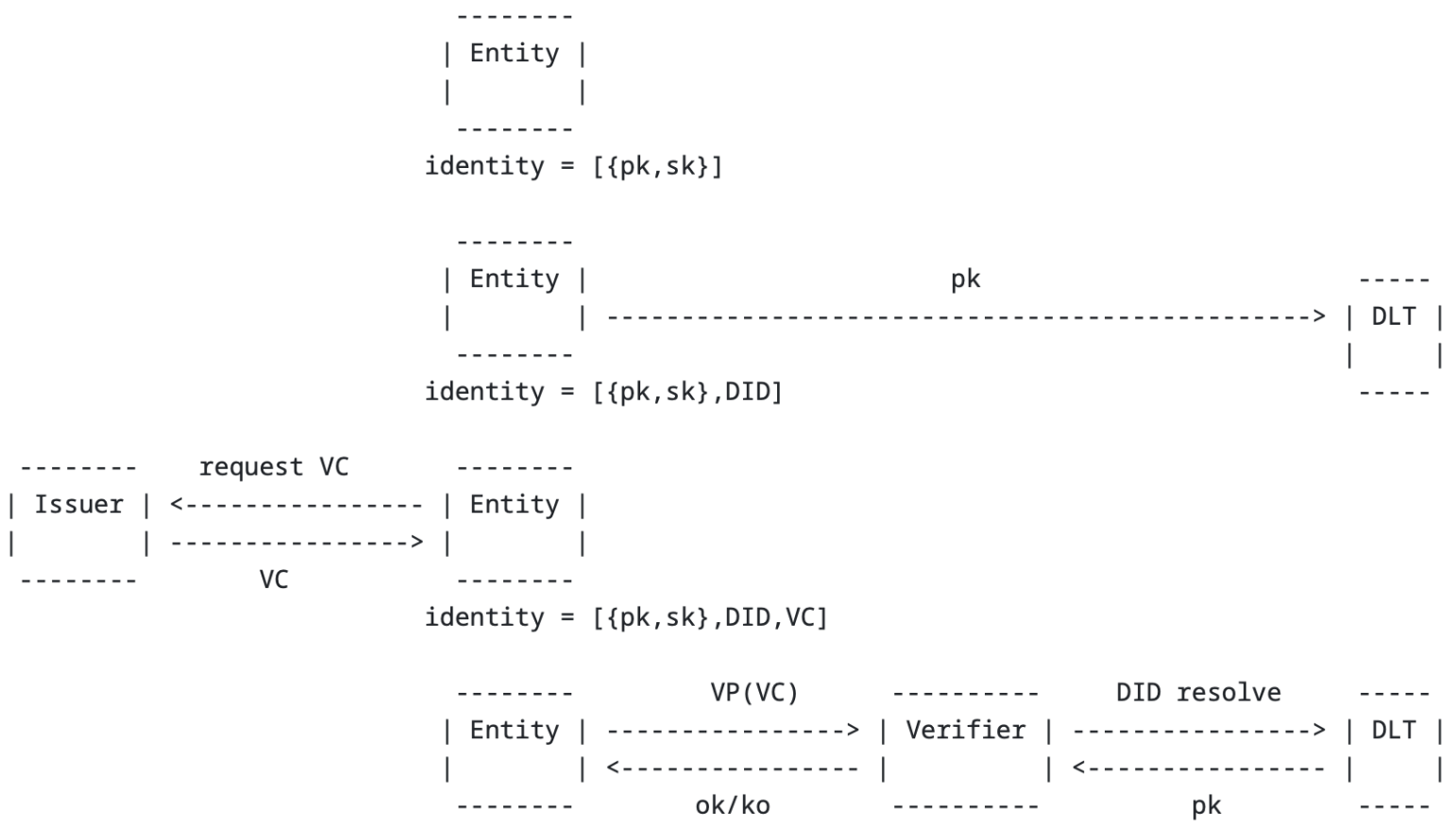
Self-Sovereign Identity (SSI)

- 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



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.

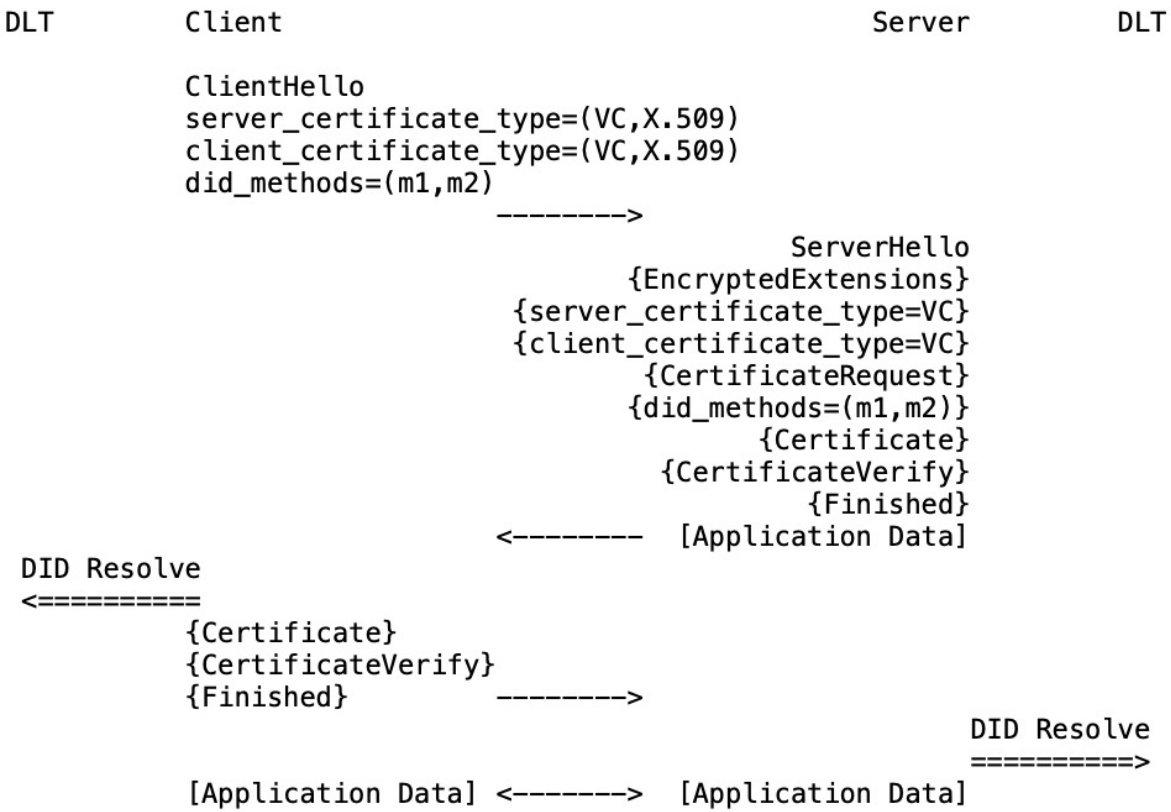
A new Certificate Type and Extension

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

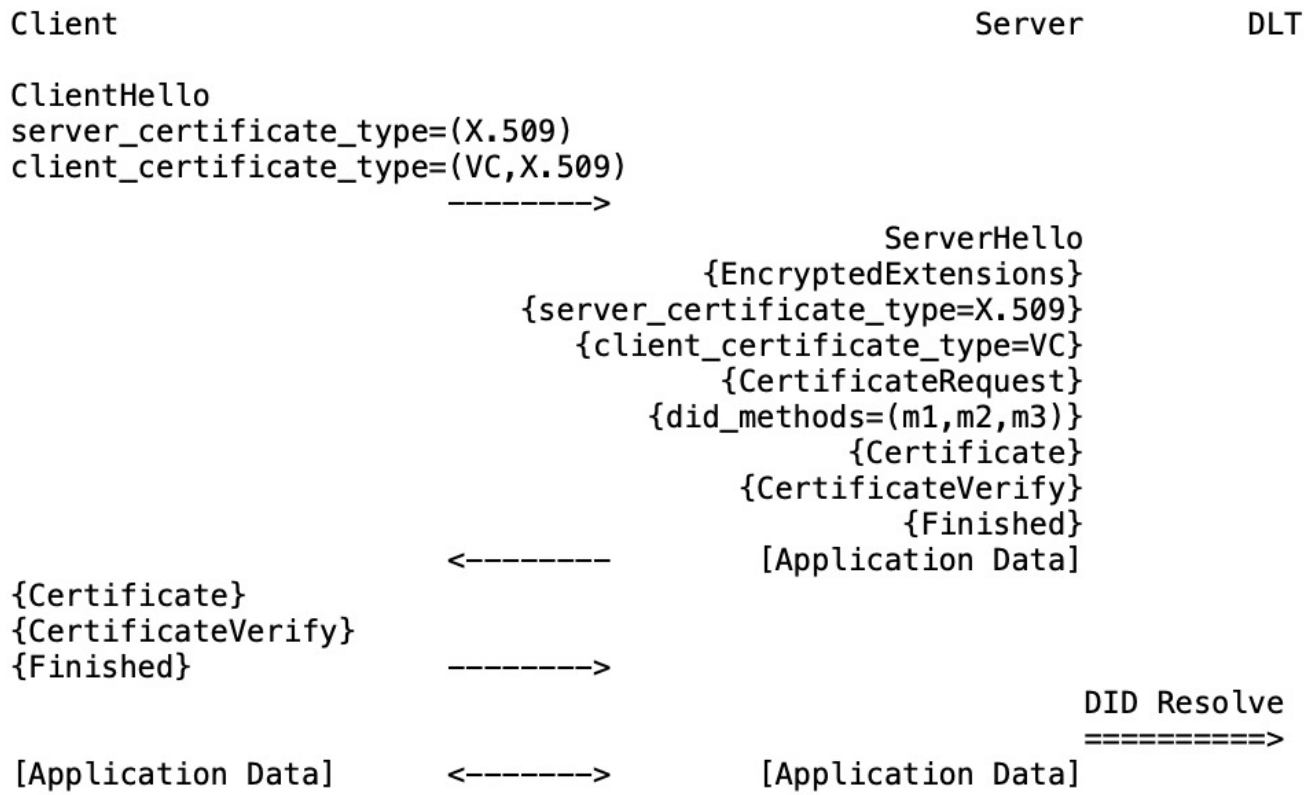
- **did_methods**: a new extension containing the list of DID Methods supported by the endpoint to resolve the DID of the peer.

- **Certificate** message will carry the VC content if the *VC* Certificate Type is selected.

Full TLS handshake with VC



Hybrid TLS handshake



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]

[1] https://datatracker.ietf.org/doc/html/draft-vesco-vcauthtls

[2] https://github.com/Cybersecurity-LINKS/openssl

[3] https://github.com/Cybersecurity-LINKS/openssl-ssi-provider