DANCE Protocols Status

IETF 114; Philadelphia
Thursday, July 28th 2022
Shumon Huque

Current protocol specification drafts

DANE TLS Client Authentication:

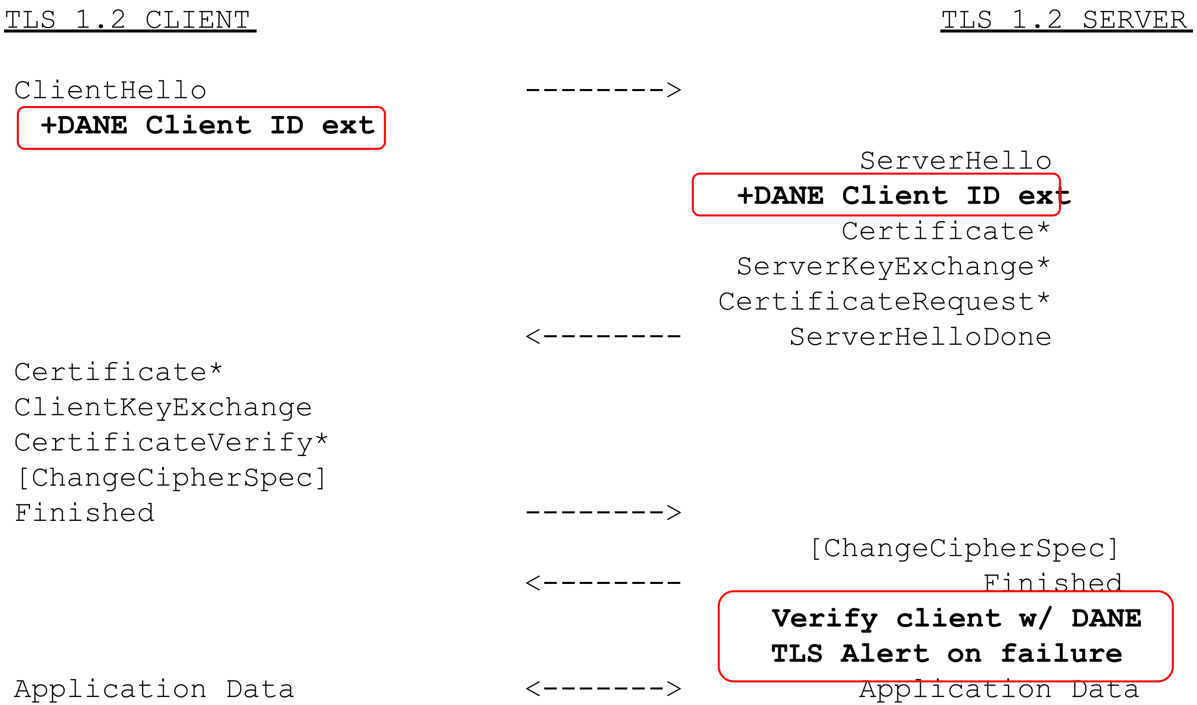
[draft-ietf-dance-client-auth-00]

TLS Extension for DANE Client Identity:

[draft-ietf-dance-tls-clientid-00]

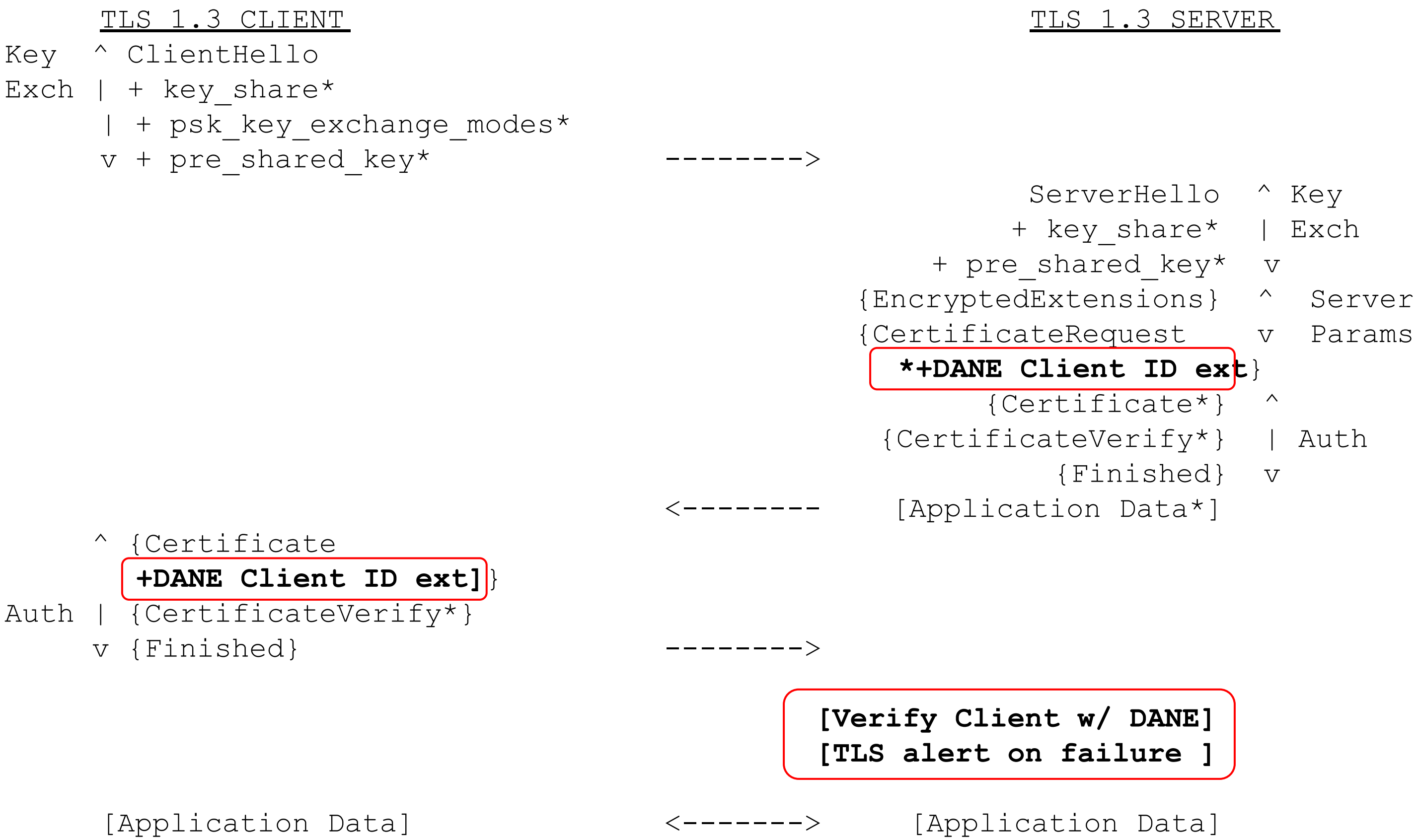
Note: TLS 1.2 vs 1.3 differences

- New TLS extension for conveying client's DANE identity to the server
    - For signaling support for DANE TLS client authentication (empty extension if signal only)
    - For conveying client DNS identity when used with TLS raw public key auth (RFC 7250)
    - **In TLS 1.3, this extension is carried in the (encrypted) Client Certificate message.**
    - **In TLS 1.2 it is carried in the first client Client Hello extension, and thus has no provision for privacy protection.**
    - The server can also send an empty extension to signal that it supports this capability.
        - **In TLS 1.2 this will be in the Server Hello extension**
        - **In TLS 1.3 this will be in the Certificate Request message, and is REQUIRED (see RFC 8446, Section 4.4.2).**



```
TLS 1.2 CLIENT                                                TLS 1.2 SERVER

ClientHello                        -------->
 +DANE Client ID ext
                                                     ServerHello
                                           +DANE Client ID ext
                                                    Certificate*
                                              ServerKeyExchange*
                                             CertificateRequest*
                                   <--------     ServerHelloDone
Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished                           -------->
                                              [ChangeCipherSpec]
                                   <--------            Finished
                                           Verify client w/ DANE
                                           TLS Alert on failure
Application Data                   <------->    Application Data
```



```
     TLS 1.3 CLIENT                                      TLS 1.3 SERVER
Key  ^ ClientHello
Exch | + key_share*
     | + psk_key_exchange_modes*
     v + pre_shared_key*           -------->
                                                     ServerHello  ^ Key
                                                    + key_share*  | Exch
                                               + pre_shared_key*  v
                                           {EncryptedExtensions}  ^  Server
                                           {CertificateRequest    v  Params
                                             *+DANE Client ID ext}
                                                  {Certificate*}  ^
                                            {CertificateVerify*}  | Auth
                                                      {Finished}  v
                                   <--------    [Application Data*]
     ^ {Certificate
        +DANE Client ID ext]}
Auth | {CertificateVerify*}
     v {Finished}                  -------->
                                        [Verify Client w/ DANE]
                                        [TLS alert on failure ]
      [Application Data]           <------->     [Application Data]
```

dance-client-auth

Comment on list from Michael Richardson:

“I think that the introduction is very weak; I think that more references and integration with the to-be-adopted architecture document will solve that problem.

I suggest we write "IoT" rather than "IOT"

Discussion & next steps

- Protocol specification is largely done in our opinion. What’s missing or remains to be done?

- Working on the architecture doc and more detailed description of application use cases may inform other enhancements.
- As will implementation experience.