

TLS 1.3 Extension for Certificate-based Authentication with an External Pre-Shared Key

draft-housley-tls-tls13-cert-with-extern-psk

Russ Housley

TLS WG at IETF 103

November 2018

A Bit of History

- In Montreal no one objected to the handling of external PSKs with certificates, but ...
- Some expressed desire for support of resumption PSKs too
 - Case 1: proof that the server still has access to the private key
 - Case 2: provide a different certificate on resumption
 - Of course this cannot be used with `early_data`
- Added both in draft-housley-tls-tls13-cert-with-extern-psk-02
- Some think too much complexity was added
- **Goal for today: determine way forward**

External PSK in Initial Handshake

Client

```
ClientHello
+ tls_cert_with_psk
+ supported_groups*
+ key_share
+ signature_algorithms*
+ psk_key_exchange_modes(psk_dhe_ke)
+ pre_shared_key
```

----->

```
{Certificate*}
{CertificateVerify*}
{Finished}
[Application Data]
```

<-----

----->

<----->

Server

```
ServerHello
+ tls_cert_with_psk
+ key_share
+ pre_shared_key
+ {EncryptedExtensions}
  {CertificateRequest*}
    {Certificate}
  {CertificateVerify}
  {Finished}
```

[Application Data]

Resumption PSK for Case 1

Client

```
ClientHello
+ early_data
+ tls_cert_with_psk
+ key_share
+ signature_algorithms*
+ psk_key_exchange_modes(psk_dhe_ke)
+ pre_shared_key
(Application Data*) ----->
```

```
(EndOfEarlyData)
{Finished}
[Application Data]
```

Server

```
ServerHello
+ tls_cert_with_psk
+ key_share
+ pre_shared_key
+ {EncryptedExtensions}
+ early_data*
{CertificateRequest*}
{Certificate}
{CertificateVerify}
{Finished}
[Application Data*]
```

<-----

----->

<----->

[Application Data]

Resumption PSK for Case 2

Client

```
ClientHello  
+ early_data  
+ tls_cert_with_psk  
+ key_share  
+ signature_algorithms*  
+ psk_key_exchange_modes(psk_dhe_ke)  
+ pre_shared_key  
(Application Data*) ----->
```

```
(EndOfEarlyData)  
{Finished}  
[Application Data]
```

Server

```
ServerHello  
+ tls_cert_with_psk  
+ key_share  
+ pre_shared_key  
+ {EncryptedExtensions}  
+ early_data*  
{CertificateRequest*}  
  {Certificate}  
  {CertificateVerify}  
  {Finished}  
[Application Data*]
```

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

Way Forward

I ask the WG Chairs to take some hums to guide the way forward. I will update the document based on their call of the consensus in the room.

The document should include support for ...

HUM 1) ... external PSKs with certificates for the initial handshake? Y/N

HUM 2) ... resumption PSKs with the same certificate for the subsequent handshake? Y/N

HUM 3) ... resumption PSKs with a different certificate for the subsequent handshake? Y/N