SCSV & Credential Protection
Ciphersuites for (TLS)
draft-badra-tls-identity-protection
draft-badra-tls-ciphersuite-identity-protection

Mohamad Badra
ETF 83, Paris, France
Identity Protection

- Send the Certificate and CertificateVerify messages encrypted during the Handshake
  - send the ChangeCipherSpec before Certificate and CertificateVerify and after ClientKeyExchange
  - Initially proposed in 2000
Messages order changes

- Could be done using
  - Extensions
    - RFC5246: both the SSLv3 and TLS 1.0/TLS 1.1 specifications require implementations to ignore data following the ClientHello (i.e., extensions) if they do not understand it. However, some SSLv3 and TLS 1.0 implementations incorrectly fail the handshake in such a case. This means that clients that offer extensions may encounter handshake failures
Messages order changes

- **Cipher Suites**
  - Example: TLS_CP_RSA_WITH_RC4_128_MD5
  - `draft-badra-tls-ciphersuite-identity-protection`

- **SCSV in ClientHello.cipher_suites**
  - No extension is needed
  - `draft-badra-tls-identity-protection`
Messages order

Client                                      Server

ClientHello  -------->  ServerHello

Certificate
CertificateRequest

<--------  ServerHelloDone

ClientKeyExchange
ChangeCipherSpec
Certificate
CertificateVerify
Finished  -------->

<--------  Finished

ChangeCipherSpec

No authenticated indication is received from the server before sending the Client Certificate
Authenticated indication is implicitly provided in the received Finished from the server
Messages order case: SCSV

When the SCSV is selected, in verify_data, replace
Hash(handshake_messages) with
Hash(handshake_messages + \{ 0xXX,0xXX\})

Where: + means concatenation
\{ 0xXX,0xXX \} is the SCSV code.

The client never sends its Certificate before receiving an authenticated indication from the server.
Current and Next Steps

- Implementations
- WG item?