TLS out-of-band public key validation

draft-ietf-tls-oob-pubkey-04

Paul Wouters <pwouters@redhat.com>
Hannes Tschofenig <Hannes.Tschofenig@gmx.net>

Jul 31, 2012

Changes between draft-ietf-tls-oob-pubkey-02 / -03

- Clarification on requirements with (CoAP) [I-D.ietf-core-coap]
- Hash support moved to [I-D.ietf-tls-cached-info]
- Proposed a new Certificate Type
- Very limited client authentication support
  (by pubkey blob lookup only)
- Required cert_type registry of RFC 6091
- Which required uplifting of RFC 6091 to standards-track
- A bis draft of RFC 6091 only produced yawns
- ...

Changes between draft-ietf-tls-oob-pubkey-03 / -04

- Instead of new Certificate Type, proposes a new TLS Extension containing the CertificateType
- Add a cert-send / cert-receive extension to exchange which certificate types are supported
- Require new IANA registry for CertificateType
- No dependancy on RFC 6091
- Allow more elaborate client authentication (eg Hybrid X.509/Raw)

draft-ietf-tls-oob-pubkey-04

```
client_hello,
cert-receive=(RawPublicKey) ->
                              <- server_hello,
                                 cert-send=RawPublicKey,
                                 certificate,
                                 certificate_request,
                                 cert-receive=(RawPublicKey, X.509)
                                 server_key_exchange,
                                 server_hello_done

 cert-send=RawPublicKey,
 certificate,
 client_key_exchange,
 change_cipher_spec,
 finished ->

                              <- change_cipher_spec,
                                 finished

      Application Data <-------> Application Data
```

Open issues

- Example 2 (Fig. 3) conflicts with RFC 5246:
  - RFC 5246 states TLS extensions can only be included into the ClientHello or the ServerHello handshake message.
  - The draft states, that the client must send a 'cert-send' before its Certificate message, but after having received the server's 'cert-receive'.
- If introducing a new TLS extension, why not add a client id identifier? (i.e. key from dns like draft-dane-fanf-smtp or draft-hoffman-dane-smime)
- Clarification on wire format of SubjectPublicKeyInfo (ASN.1 variable-length vector, i.e., preceded by its length)