MQTT-TLS Profile of ACE

draft-ietf-ace-mqtt-tls-profile-03
Cigdem Sengul
Cigdem.Sengul@nominet.uk

Interim, ACE WG
January 31, 2020
Updates since IETF 106:

- **draft-ietf-ace-mqtt-tls-profile-03:**
  - Added the option of Broker certificate thumbprint in the 'rs_cnf’ sent to the Client.
  - Clarified the use of a random nonce from the TLS Exporter for PoP, added to the IANA requirements that the label should be registered.
  - Added a client nonce, when Challenge/Response Authentication is used between Client and Broker.
  - Clarified the use of the "authz-info" topic and the error response if token validation fails.
  - Added clarification on wildcard use in scopes for publish/subscribe permissions
  - Reorganised sections so that token authorisation for publish/subscribe messages are better placed
### Client Authentication/Authorisation

Daniel’s comments on presentation, and multiple tokens

<table>
<thead>
<tr>
<th>TLS</th>
<th>MQTT</th>
<th>ACE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Anon</td>
<td>Public topics Authz-info</td>
<td>Token in CONNECT AS-Discovery</td>
</tr>
<tr>
<td>Known (RPK/PSK)</td>
<td>RPK – token via authz-info PSK– token “psk_identity” [I-D.iotf-ace-dtls-authorize]</td>
<td>SHOULD NOT be chosen Token in CONNECT overwrites any permission during TLS handshake</td>
</tr>
</tbody>
</table>
TLS: none – MQTT: ACE

MQTT v5: Authentication Using AUTH Property

**Client**
- TLS set-up
- CONNECT AUTH data: Token + pop=MAC/Sign(tls-exporter(s))
- CONNACK
- Introspect token (OPT)
- Verify pop using tls_exporter(s)

**Broker**

Proof-of-Possession using a secret from the TLS session

**Only option for MQTT v3.1.1:** Username=Token; Password= pop

MQTT Binary Data encoding for token + pop

**Open issues:**
- The length and format of the input challenge configurable?
- RECOMMEND length? **STILL TO BE DECIDED.**
- Register which tls-exporter label? **DONE – EXPORTER-ACE-Sign-Challenge.**

**Client**
- TLS set-up
- CONNECT AUTH data: Token
- AUTH – Continue Authentication:
  - Rs nonce
  - Response=Sign/MAC(Rs nonce, Client nonce)
- CONNACK
- Introspect token (OPT)
- Verify Response

**Broker**

Proof-of-Possession using a challenge/response

**Open issues:**
- The length and format of the input challenge configurable? RECOMMEND length? **STILL TO BE DECIDED.**
- Does not use channel binding.
Open issues / Other Discussion Points:

IETF 106 Singapore

• Add payload encryption for the PUBLISH message – Discussion started for the pub-sub document

Reviews Jim/Daniel

3. Format of the AUTH data: https://github.com/ace-wg/mqtt-tls-profile/issues/40
5. Matching Wildcard topics in subscriptions to wildcards in permissions.
6. Question about WPKI etc. support in the document…
7. Specify further what token as reference looks like?