MQTT-TLS Profile of ACE

draft-ietf-ace-mqtt-tls-profile-02
Cigdem Sengul
Cigdem.Sengul@nominet.uk

IETF 106 ACE WG meeting
November 19, 2019
MQTT-ACE Version History

- **draft-ietf-ace-mqtt-tls-profile-00**
  - Published with minor changes from draft-sengul-ace-mqtt-tls-profile-04

- **draft-ietf-ace-mqtt-tls-profile-01**
  - MQTTv5 recommended version
  - Clarification MQTTS and HTTPS endpoints
  - JSON/CBOR encoding

- **draft-ietf-ace-mqtt-tls-profile-02**:
  - Client connection authentication/authorisation over TLS and MQTT
  - authz-info for token transport
  - PoP and TLS token binding
Protocols and Encodings

HTTPS: C-AS and Broker-AS
MQTTS: C-Broker

Supported encoding: JSON
May support: CBOR

JWT/CWT and PoP

Q: Any blockers with JWT if using rfc7800 and draft-ietf-ace-oauth-params?
# Client Authentication/Authorisation

**RECOMMENDED**: TLS:Anon-MQTT:ace.

<table>
<thead>
<tr>
<th>TLS</th>
<th>MQTT</th>
<th>ACE</th>
</tr>
</thead>
<tbody>
<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.ietf-ace-dtls-authorize]</td>
<td>SHOULD NOT be chosen Token in CONNECT overwrites any permission during TLS handshake</td>
</tr>
</tbody>
</table>
authz-info: The Authorization Information Topic

PUBLISH-only topic that is not protected

Broker MAY return response code 'Not Authorized'
if PUBLISH message QoS > 1

Broker stores and indexes all tokens
Similar to DTLS profile for ACE [I-D.ietf-ace-dtls-authorize]
TLS: none – MQTT: ACE

MQTT v5: Authentication Using AUTH Property

**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 to be decided:**
The length and format of the input challenge configurable? RECOMMEND length?
Register which tls-exporter label?

**Proof-of-Possession using a challenge/response**

Open issues to be decided:
The length and format of the input challenge configurable? RECOMMEND length?
TLS: none – MQTT: ACE

MQTT v5: AS Discovery

Client

TLS set-up

CONNECT-
AUTH method: ace
AUTH data: none

Broker

AS Discovery
User Property: utf-8 string pair

CONNACK ‘Not authorized’
User Property – AS creation hints

Not possible for MQTT v3.1.1
Ongoing/Next steps

• Implementation in Edinburgh University

• Tidy up Client Authentication and PoP with secret from TLS-exporter

• Add payload encryption for the PUBLISH message?
  • I-D.ietf-ace-key-groupcomm