MQTT-TLS Profile of ACE

draft-ietf-ace-mqtt-tls-profile-02

Cigdem Sengul

Cigdem.Sengul@nominet.uk

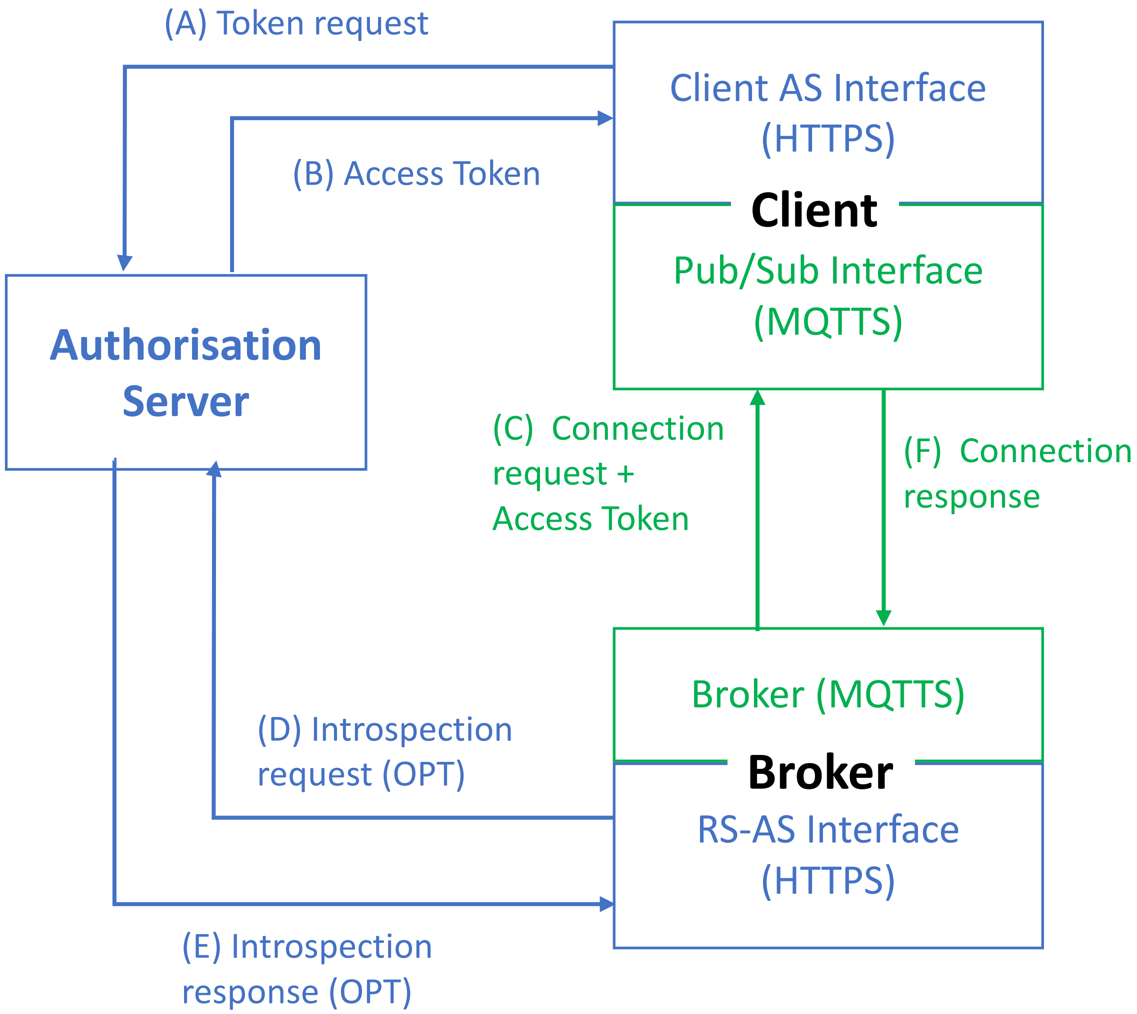
IETF 106 ACE WG meeting

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



(A) Token request
(B) Access Token
Client AS Interface (HTTPS)
Client
Pub/Sub Interface (MQTTS)
Authorisation Server
(C) Connection request + Access Token
(F) Connection response
Broker (MQTTS)
Broker
RS-AS Interface (HTTPS)
(D) Introspection request (OPT)
(E) Introspection response (OPT)

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.

MQTT TLS	None	ACE
Anon	Public topics Authz-info	Token in CONNECT AS-Discovery
Known (RPK/PSK)	RPK – token via authz-info PSK– token “psk_identity” [I-D.ietf-ace-dtls-authorize]	SHOULD NOT be chosen Token in CONNECT overwrites any permission during TLS handshake

TLS:Known(RPK/PSK) – MQTT:none

authz-info: The Authorization Information Topic

PUBLISH-only topic that is not protected

Broker MAY return response code ’Not Authorized’

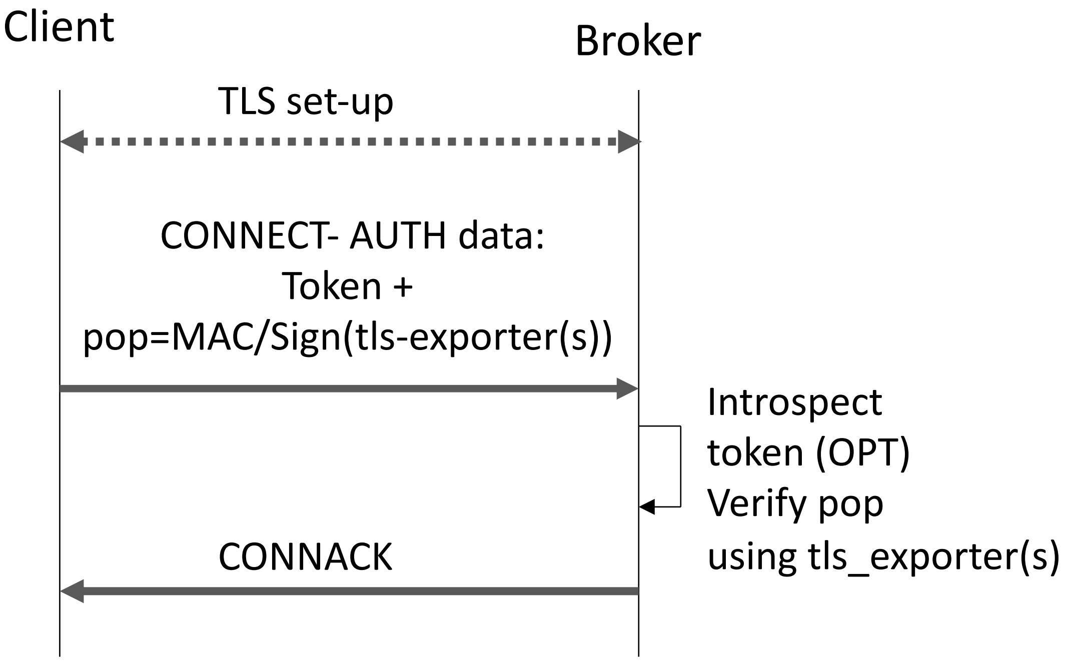
if PUBLISH message QoS > 1

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

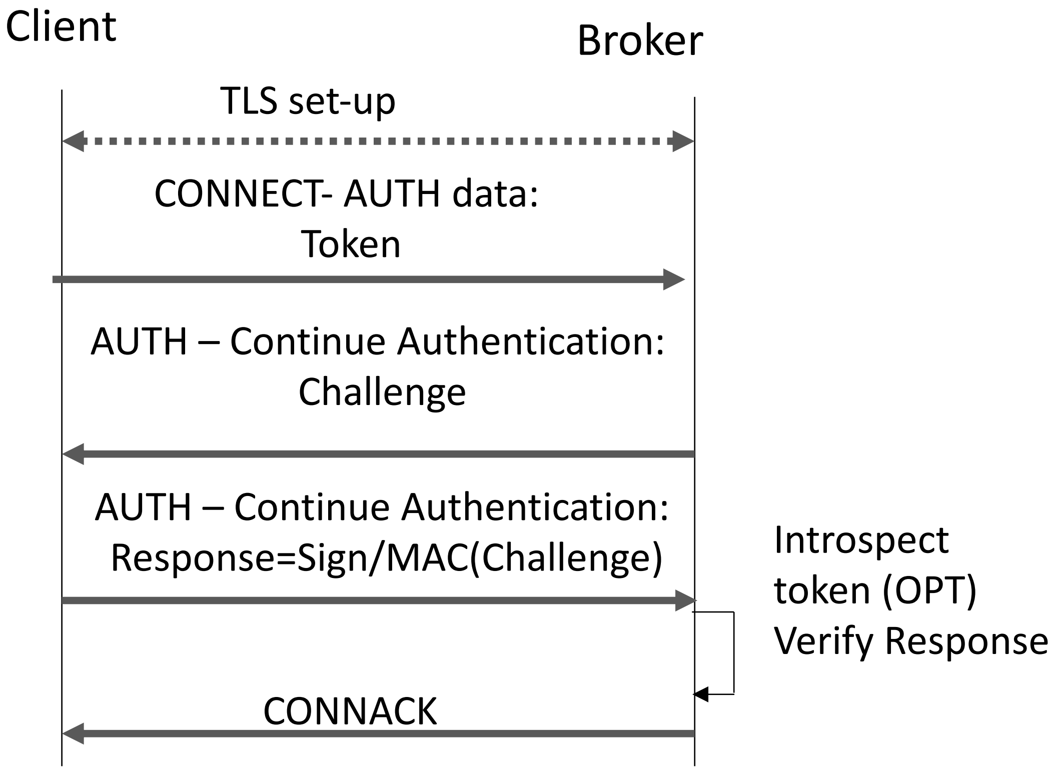
MQTT Binary Data encoding for token + pop

Open issues to be decided:

The length and format of the input challenge configurable?

RECOMMEND length?

Register which tls-exporter label?



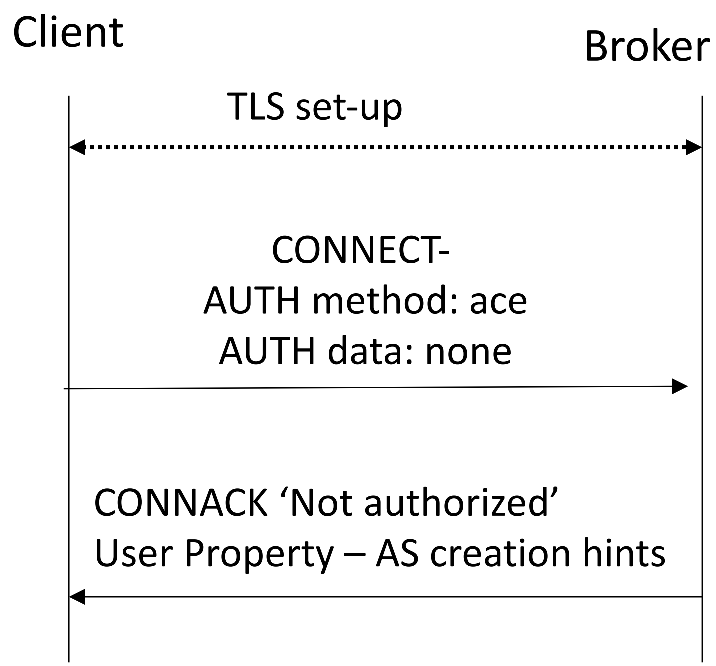
Proof-of-Possession using a challenge/response

Open issues to be decided:

The length and format of the input challenge configurable? RECOMMEND length?

TLS:none – MQTT:ACE

MQTT v5: AS Discovery



AS Discovery

User Property: utf-8 string pair

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