MQTT-TLS Profile of ACE

draft-ietf-ace-mqtt-tls-profile-06

Cigdem Sengul

cigdem.sengul@brunel.ac.uk

IETF 108

July 29, 2020

Updates since the last interim

- Submitted draft-ietf-ace-mqtt-tls-profile-06
    - Replace the originally proposed scope format with AIF model.
    - Clarified client connection after submitting token via "authz- info" topic as TLS:Known(RPK/PSK)-MQTT:none.
    - Expanded acronyms on their first use including the ones in the title.
    - Added a definition for "Session".
    - Corrected "CONNACK" definition, which earlier said it's the first packet sent by the broker.
    - Added a statement that the broker will disconnect on almost any error and may not keep session state.
    - Clarified that the broker does not cache invalid tokens.

AIF-MQTT

- AIF-MQTT = AIF_Generic<filter, permissions>
  filter = tstr
  permissions = [+permission]
  permission = "pub" / "sub“

Example scope:

[["topic1“, ["pub", "sub"]], ["topic2/#",["pub"]], ["+/topic3",["sub"]]]

Open issue: Session Continuation

- *If necessary, the Broker MAY support session continuation, and hence, maintain and use client state from the existing session.* ***The client state MAY include token and its introspection result (for reference tokens) in addition to the MQTT session state.*** *When reconnecting to the Broker, the Client MUST still provide a token, as well as setting the Clean Start to 0 and supplying a Session Expiry interval in the CONNECT message. The Broker MUST perform proof-of-possession validation on the provided token. If the token matches the stored state, the Broker MAY skip introspecting a token by reference, and use the stored introspection result.*
- The Broker cannot validate if the reconnecting client is the same client
  - Example: Client A client_id 1 disconnects and client B connects with client_id 1. But client B cannot publish/subscribe more than what its token allows it to do.
- **Change MAY to MUST?**
  - Client then MUST use the previous session token to connect but client may have gotten a new token because its former token expired or some other reason.

Open issue: Reauthentication

- The Client MUST have used challenge-response PoP as defined in Section 4 and MUST use the same method for re-authentication.

- The Broker accepts re-authentication requests if the Client has already submitted a token (may be expired) and validated via challenge-response. Otherwise, the Broker MUST deny the request.

- The Broker MUST NOT process any data sent by the Client after the CONNECT packet including AUTH packets (Note that this is different in MQTT v5, the Broker is allowed to process AUTH packets even if the Broker rejects the CONNECT).

Questions

- Should this profile register thumbprints in a confirmation claim for CWT?
    - The AS MAY include the thumbprint of the RS's X.509 certificate in the 'rs_cnf’.

- ACE Profile Registry entry for mqtt_tls profile
    - CBOR Value CBOR abbreviation for this profile name?

Next steps

- Resolve remaining open issues
- Implementation updates
  - https://github.com/michaelg9/HiveACEclient
    - using the HiveMQ CE is a Java-based open source MQTT broker that fully supports MQTT 3.x and MQTT 5.
  - The Mosquitto prototype was only v3.1.1: https://github.com/ciseng/ace-mqtt-mosquitto