Self-Signed Certificate Trial

Malaysia

ICAO APAC Regional Office, Bangkok

26-30 May 2025

OBJECTIVE

Objective

- To study the feasibility of using self-signed certificate for enabling secured & encrypted Transport Layer Security (TLS) communication between SWIM EMS

- By using self-signed certificate for TLS transport/network encryption between SWIM nodes, as an **alternative** to Public Key Infrastructure (PKI) with centralized Certificate Authority (CA)

For comparison:

- Europe, with its centralised regulatory bodies, has established a centralized PKI for SWIM
- In contrast, the absence of such central governance in APAC necessitates a de-centralised approach with no single CA

TEST SUMMARY

Test Setup

- Done over the internet.
- Bandwidth restriction using tools like **tc** and **wondershaper** to emulate the CRV bandwidth restriction (2 Mbps).
- Certificate Signing Request (CSR) is done via email exchange.
- Automated testing for measuring the message throughput for the test scenarios.
  - Message testing tools used:
    - **Quiver**: https://github.com/ssorj/quiver
    - **Kame**: New tools derived from Quiver that can cover all 4 test scenarios: https://github.com/siagalabs/amqp-kamehameha

Test Status

- Currently done between 2 states: Malaysia and Singapore.

- The test is still ongoing.

- Activities done:
  - Certificate exchange.
  - Secure connection test (TLS).
  - Message exchange using the following scenarios:
    - PLAIN message exchange.
    - PLAIN message exchange with digital signature.
    - ENCRYPTED message exchange with digital signature.

Test Scenarios / Area Explored

- Secure connection using TLS (password and password-less).

- Message exchange with various message payload sizes.

- Message signing for non-repudiation.
  - Additional header.
  - **x-digital-signature**: contains the message digital signature.

- Message encryption for message confidentiality.
  - Additional header.
  - **x-encrypted-key**: contains the AES encryption key.
  - **x-iv**: AES encryption initialisation vector.

Current Findings

- No significant difference using TLS or PLAIN connection.
- Adding digital signature / encryption may increase the message size significantly especially on small payloads.
- Unrelated – choice of programming language for the client may impact the performance of message exchange.

What’s Next?

- To test other test scenarios based on any other suggested use cases.
- To test on Certificate revocation using CRL / OSCP.

What’s Next?

- Hope other states to be able to participate in this test to be able to further study the self-signed certificate method:
  - More issues will be discovered the more states are involved.
  - Trust establishment complexity:
    - No central authority – each state needs to manually decide which certificate to trust.
    - Trust store management – all states need to maintain and distribute trusted certificates.
  - Scalability issues – become unmanageable as the number of states increases.
  - Certificate renewal and rotation
    - Manual rotation – certificate expiry and compromise, all other states must update trust stores.
    - Risk of downtime – if trust is not updated in time, the connection will fail.

THANK YOU