International Civil Aviation Organization

The Tenth Meeting of System Wide Information Management Task Force (SWIM TF/10)

Bangkok, Thailand, 20 – 23 May 2025

Agenda Item 5: b) SWIM Infrastructure

USING A SELF-SIGNED CERTIFICATE FOR SECURED SWIM COMMUNICATION EXCHANGE

(Presented by MALAYSIA)

SUMMARY

This paper examines the potential for experimenting a Transport Layer Security (TLS) between SWIM EMS nodes communications under a situation where a centralised Certificate Authority (CA) for TLS certificate is not feasible. The paper reports on the exploration activities on the use of self-signed certificates which was required in order to established encrypted TLS transport between SWIM EMS and to conduct trials using such certificates to ensure secure information exchange within the APAC SWIM environment.

1. INTRODUCTION

1.1 The purpose of this taskforce is to study the feasibility of using self-signed certificate for enabling Transport Layer Security (TLS) communication between SWIM EMS, with a main purpose of enabling encryption at the IP transport layer (TCP).

1.2 In TLS communication standards, certificates serve as digital identity cards, verifying the authenticity of the communicating parties, typically the server and optionally the client. These certificates, issued usually by trusted Certificate Authorities (CAs), contain the public key of the entity and are cryptographically signed by the CA, assuring clients that the server's public key genuinely belongs to the claimed domain. This verification process is crucial for establishing a secure and encrypted connection, as it prevents man-in-the-middle attacks where malicious actors might try to intercept or tamper with the communication by impersonating one of the parties.

1.3 As a comparison, Europe, with its centralised regulatory bodies, has established a single CA for SWIM. In contrast, the absence of such central governance in APAC necessitates a decentralised approach with no single CA.

1.4 Thus, the purpose of this taskforce is to study and experiment on using self-signed certificate for TLS communication.

2. DISCUSSION

2.1 To set the primary objective and the overall scope of testing.

2.2 To identify the participant states for this testing, which initially start with Malaysia, Singapore and Thailand, and other states who have expressed their interest.

2.3 To determine the appropriate testing environment, including server and network configurations.

2.4 To determine the testing scenarios and parameters, which should be based on the defined objectives and scope.

2.5 To decide on which method is most suitable for certificate generation and distribution.

PROPOSED TESTING AND EXPERIMENT

2.6 Testing environment that was agreed:

2.6.1 Network: Using public internet, due to the testing exercise may cause higher bandwidth utilization thus the need to avoid using CRV network which currently serving the production system. Also, access network must be ‘shaped’ to emulated typical CRV access bandwidth e.g. 2 Mbps.

2.6.2 Computing/servers: Because the proposed network is a public internet, the testing SWIM EMS node server can be either any public cloud servers, or existing servers in data center belong to the states, with public internet access.

2.7 Testing scenarios:

2.7.1 Test 1 - No TLS/SSL:
To evaluate the throughput and latency of message exchange using a plain connection as a benchmark.

2.7.2 Test 2 - With self-signed TLS certificate authentication & encryption:
To establish TLS connectivity and client authentication using a self-signed certificate

2.7.3 Test 3 - With TLS + message signing:
To incorporate message signing for non-repudiation.

2.7.4 Test 4 - With TLS + message signing + message body encryption:
To incorporate both digital signature and message body encryption to achieve message confidentiality and non-repudiation.

2.8 For each scenario during the testing, the performance metrics will be captured and be presented. Some of the metrics that are proposed for performance measurements are memory utilisation, CPU utilization, message throughput (number of messages per seconds), message latency and delay.

CURRENT PROGRESS OF TESTING

2.9 Currently Hong Kong, New Zealand, Vietnam and Pakistan have expressed their interest in joining the testing. After sharing the pre-requisite for joining the test to these 4 states, New Zealand has agreed to participate.

2.10 The proposed method for certificate generation for neighbor states is via Certificate Signing Request (CSR) method, where the private key of each states remains secret and never leave the country.

2.11 During the preliminary testing, Malaysia and Singapore managed to established TLS connection between their SWIM EMS using self-signed certificates.

2.12 The states member still in the discussion stage and experimenting on how the performance metrics should be compared, and what tools is suitable for message simulation testing. Once these matters have been finalized, the full testing can be started.

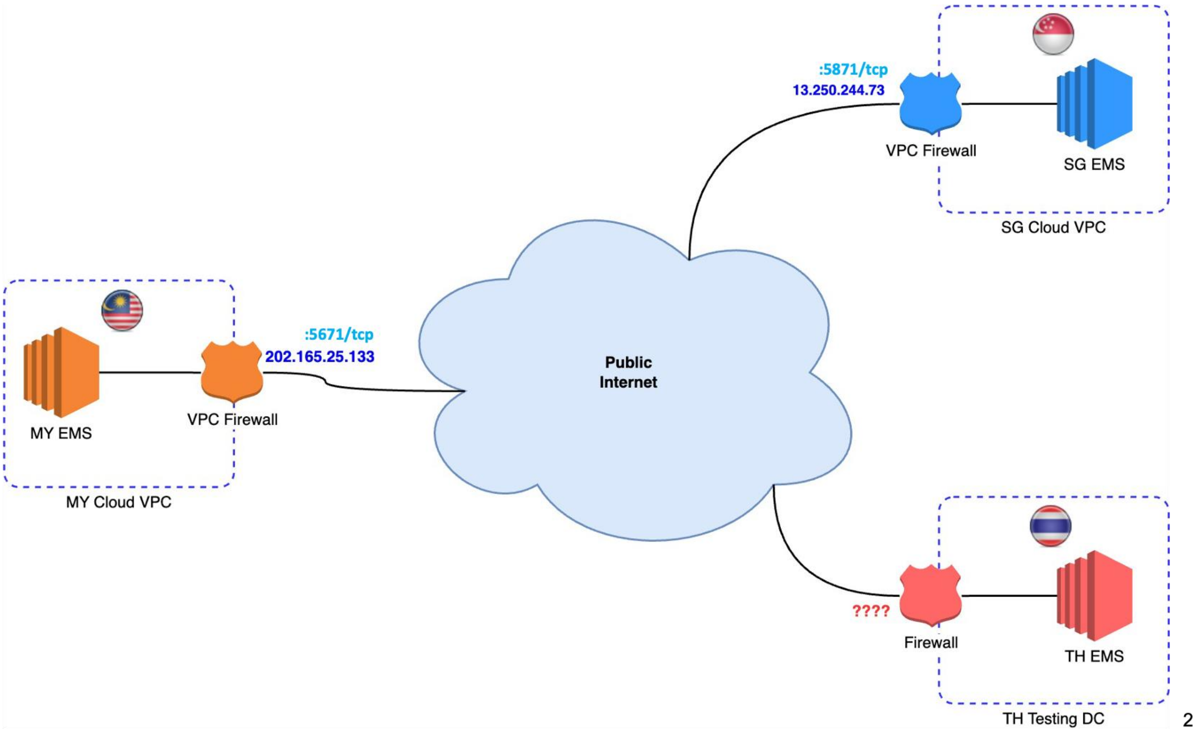

Figure 1: Current setup of self-signed certificate SWIM TLS communication

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper;
b) discuss the present proposal; and
c) discuss any relevant matter as appropriate

– – – – – – – – – – – – – –