Self Signed Certificate for SWIM EMS Connectivity

By Malaysia

WP/16:

SWIM Self Signed TLS Certificate

ICAO APAC Regional Office, Bangkok

20-23 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

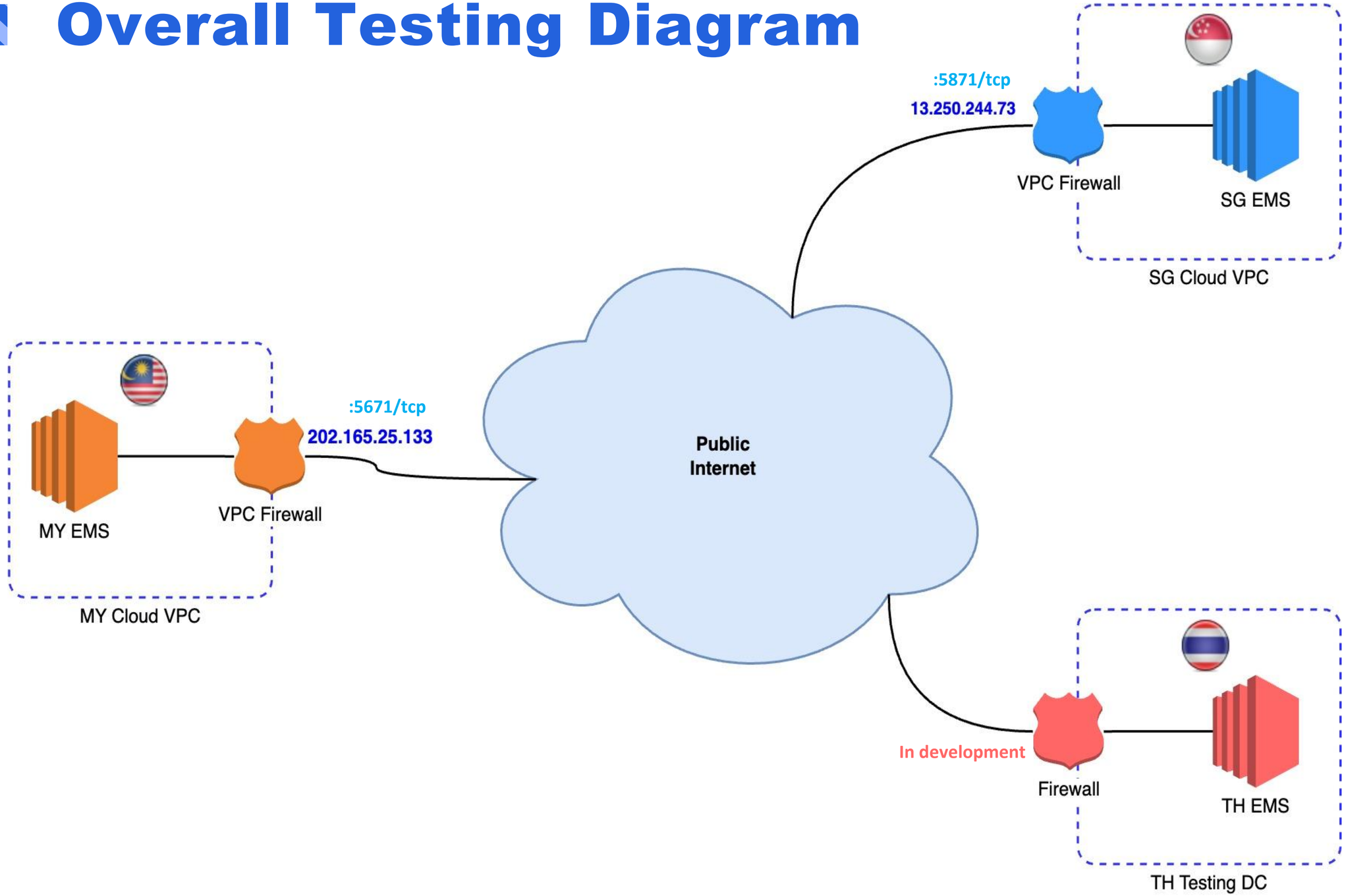
TESTING SCENARIO, SETUP & METHODS

Testing Environment

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

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

Overall Testing Diagram



Testing Resource Specification

- **MALAYSIA:**
  - Endpoint IP: 202.165.25.133
  - Hostname: gss-swim-test
  - TLS port: 5671/tcp
  - Non-TLS port: 5672/tcp
  - Server specs: 8 vCPU, 16 GB RAM
  - Infra: TM Cloud Alpha Edge

- **SINGAPORE**
  - Endpoint IP: 13.250.244.73
  - Hostname: swim-cloud-ez-message-broker-2.iep.caas.gov.sg
  - TLS port: 5871/tcp
  - Non-TLS port: 5872/tcp
  - Server specs: 2 vCPU, 8 GB RAM
  - Infra: SG Gov AWS
  - Remarks: Only incoming whitelisted IP are allowed

Testing Scenarios

- **Test 1: Plain TCP connection with no TLS/SSL:**
  - To evaluate the throughput and latency of message exchange using a plain connection as a benchmark.

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

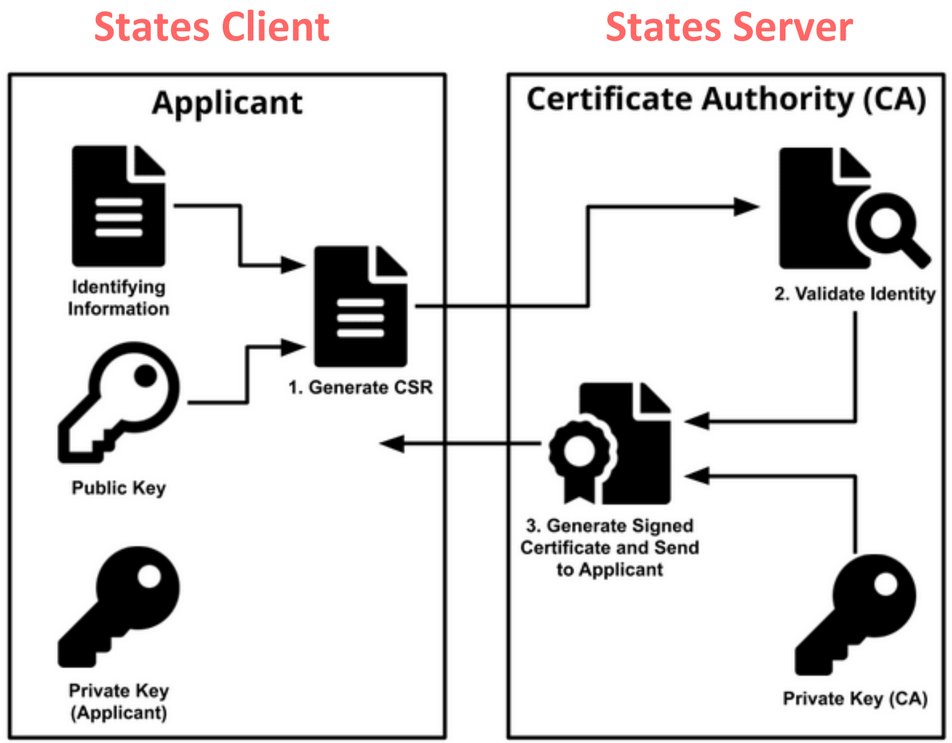
- **Test 3: With TLS + message signing:**
  - To incorporate message signing for non-repudiation.

- **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.

Cert. Generation & Distribution

- 2 methods identified earlier:
  - **No CSR:** States ‘server’ generate both ‘private key’ and ’public cert’ for states client
  - **CSR:** States ‘client’ generate ‘private key’ privately, but send Certificate Signing Request (CSR) to states ‘server’, so that server can use the CSR file to generate ‘public cert’ to states ‘client’

- Preferred method:
  - **Using CSR method**, where ‘private key’ never leave the origin country
- Must be both way: State A generate cert for state B, and state B generate cert for state A. Thus:
  - [A] → tls-connect → [B] and
  - [B] → tls-connect → [A]



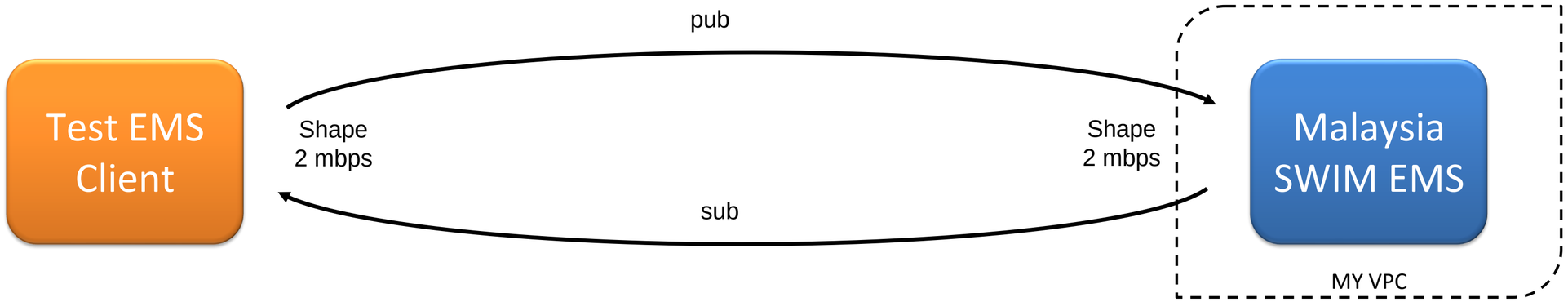
Tools Used

- Message testing tools:
  - Quiver: https://github.com/ssorj/quiver
  - New tools derived from Quiver that can cover all 4 test scenarios: https://github.com/siagalabs/amqp-kamehameha

- Network bandwidth shaper/emulator:
  - tc: simple for outgoing, but for incoming, need to play around with linux module & redirection
    * workaround: both states use tc in outgoing only to emulate full duplex 2mbps shaper
  - wondershaper: wrapper around tc to simplify outgoing/incoming, some issue reported in certain cloud environment
  - OR: L3 device (router/firewall) that limit/shape the bandwidth

RESULTS

1st Test: Within Malaysia



- SUMMARY: Pump huge amount of messages to the EMS and measure the performance (eg. time duration, latency etc)
- The client act as a publisher/sender and consumer/receiver
- Test all 4 testing scenarios: No-TLS, TLS, Signing & Encrypted Msg
- Message size and amount tested:
  - Small payload: Dummy data (11 bytes) – 10,000 messages
  - Medium payload: FPL TAC (237 bytes) – 10,000 messages
  - Large payload: FPL FIXM (41.7 KB) – 1,000 messages

Within Malaysia: Small Payload

	Test 1: No TLS Connection	Test 2: TLS Connection	Test 3: TLS/Digital Signature	Test 4: TLS/Digital Signature/Encryption
Establishing Connection	5175 ms	226 ms	200 ms	237 ms
Sender Duration	12384 ms	6,890 ms	42489 ms	76012 ms
Message Sending Rate	1386 msg / sec	1492 msg / sec	236 msg / sec	132 msg / sec
Sender Message Size	56 bytes	56 bytes	438 bytes	841 bytes
Establishing Receiver Link	5244 ms	265 ms	224 ms	289 ms
Receiver Duration	7.02 seconds	6.57 seconds	37.91 seconds	70.89 seconds
Received Message Size	121 bytes	121 bytes	491 bytes	894 bytes
Message Throughput	1425.11 msg / sec	1521.38 msg / sec	263.78 msg / sec	141.06 msg / sec
Average Latency	771.60 ms	726.28 ms	4409.10 ms	8501.42 ms

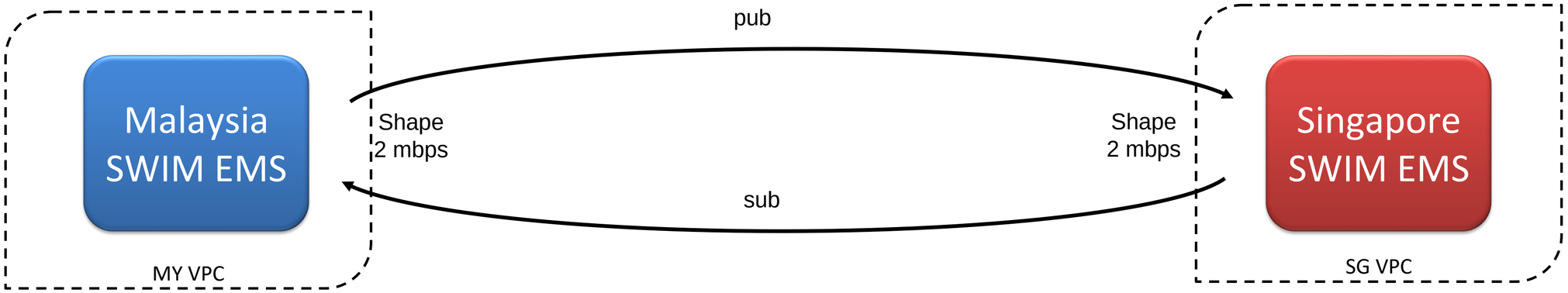
Within Malaysia: Medium Payload

	Test 1: No TLS Connection	Test 2: TLS Connection	Test 3: TLS/Digital Signature	Test 4: TLS/Digital Signature/Encryption
Establishing Connection	71 ms	296 ms	628 ms	227 ms
Sender Duration	19282 ms	29159 ms	55392 ms	81474 ms
Message Sending Rate	519 msg / sec	346 msg / sec	182 msg / sec	123 msg / sec
Sender Message Size	282 bytes	282 bytes	664 bytes	1065 bytes
Establishing Receiver Link	86 ms	33 ms	708 ms	266 ms
Receiver Duration	19.12 seconds	28.79 seconds	50.89 seconds	76.64 seconds
Received Message Size	347 bytes	347 bytes	717 bytes	1118 bytes
Message Throughput	522.93 msg / sec	347.39 msg / sec	196.51 msg / sec	130.48 msg / sec
Average Latency	2204.67 ms	2932.73 ms	5753.84 ms	8092.70 ms

Within Malaysia: Large Payload

	Test 1: No TLS Connection	Test 2: TLS Connection	Test 3: TLS/Digital Signature	Test 4: TLS/Digital Signature/Encryption
Establishing Connection	107 ms	200 ms	161 ms	214 ms
Sender Duration	203477 ms	230199 ms	195513 ms	180241 ms
Message Sending Rate	5 msg / sec	4 msg / sec	5 msg / sec	5 msg / sec
Sender Message Size	42756 bytes	42756 bytes	43138 bytes	43548 bytes
Establishing Receiver Link	167 ms	236 ms	177 ms	289 ms
Receiver Duration	213.88 seconds	241.34 seconds	211.49 seconds	189.00 seconds
Received Message Size	42821 bytes	42821 bytes	43191 bytes	43601 bytes
Message Throughput	4.68 msg / sec	4.14 msg / sec	4.73 msg / sec	5.29 msg / sec
Average Latency	209385 ms	138680.79 ms	105640.95 ms	95778.01 ms

2nd Test: From Malaysia to Singapore



- SUMMARY: Pump huge amount of messages to the EMS and measure the performance (eg. time duration, latency etc)
- The client act as a publisher/sender and consumer/receiver
- Test 3 scenarios: TLS, Signing & Encrypted Msg
- Message size and amount tested:
  - Small payload: Dummy data (11 bytes) – 10,000 messages
  - Medium payload: FPL TAC (237 bytes) – 10,000 messages
  - Large payload: FPL FIXM (41.7 KB) – 1,000 messages

MY to SG: Small Payload

	Test 1: No TLS Connection	Test 2: TLS Connection	Test 3: TLS/Digital Signature	Test 4: TLS/Digital Signature/Encryption
Establishing Connection	-	220 ms	211 ms	249 ms
Sender Duration	-	9131 ms	40791 ms	67001 ms
Message Sending Rate	-	1124 msg / sec	246 msg / sec	150 msg / sec
Sender Message Size	-	56 bytes	426 bytes	903 bytes
Establishing Receiver Link	-	238 ms	228 ms	267 ms
Receiver Duration	-	8.84 seconds	37.02 seconds	62.57 seconds
Received Message Size	-	56 bytes	426 bytes	903 bytes
Message Throughput	-	1130.71 msg / sec	270.10 msg / sec	159.82 msg / sec
Average Latency	-	938.46 ms	4347.34 ms	7162.74 ms

MY to SG: Medium Payload

	Test 1: No TLS Connection	Test 2: TLS Connection	Test 3: TLS/Digital Signature	Test 4: TLS/Digital Signature/Encryption
Establishing Connection	-	196 ms	228 ms	216 ms
Sender Duration	-	18522 ms	50106 ms	74389 ms
Message Sending Rate	-	545 msg / sec	200 msg / sec	135 msg / sec
Sender Message Size	-	282 bytes	652 bytes	1053 bytes
Establishing Receiver Link	-	212 ms	248 ms	235 ms
Receiver Duration	-	18.28 seconds	46.37 seconds	69.98 seconds
Received Message Size	-	282 bytes	652 bytes	1127 bytes
Message Throughput	-	546.93 msg / sec	215.65 msg / sec	142.89 msg / sec
Average Latency	-	2000.86 ms	5290.69 ms	7887.69 ms

MY to SG: Large Payload

	Test 1: No TLS Connection	Test 2: TLS Connection	Test 3: TLS/Digital Signature	Test 4: TLS/Digital Signature/Encryption
Establishing Connection	-	219 ms	202 ms	221 ms
Sender Duration	-	206214 ms	223683 ms	205569 ms
Message Sending Rate	-	3 msg / sec	3 msg / sec	5 msg / sec
Sender Message Size	-	42756 bytes	43126 bytes	43536 bytes
Establishing Receiver Link	-	237 ms	219 ms	239 ms
Receiver Duration	-	287.28 seconds	300.82 seconds	216.04 seconds
Received Message Size	-	42756 bytes	43126 bytes	43610 bytes
Message Throughput	-	3.48 msg / sec	3.32 msg / sec	4.63 msg / sec
Average Latency	-	165305.00 ms	175747.86 ms	104799.66 ms

Observation Summary

- No performance differences and no significant impact between using TLS (Test 2) vs plain no TLS (Test 1)

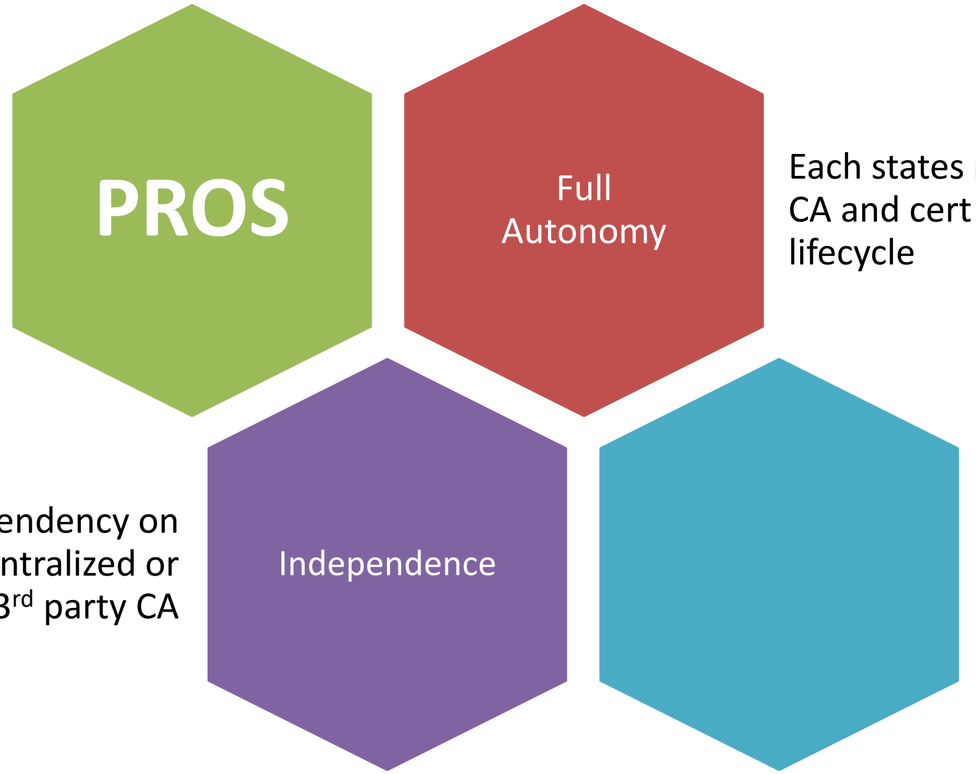
- Additional features such as message signing (Test 3) and message payload encryption (Test 4) introduce additional processing overhead, thus impacting performance

- Message size has an impact on bandwidth requirement and performance

- For large message size, there was minimal performance difference between no TLS (Test 1), using TLS (Test 2), message signing (Test 3) and message payload encryption (Test 4)

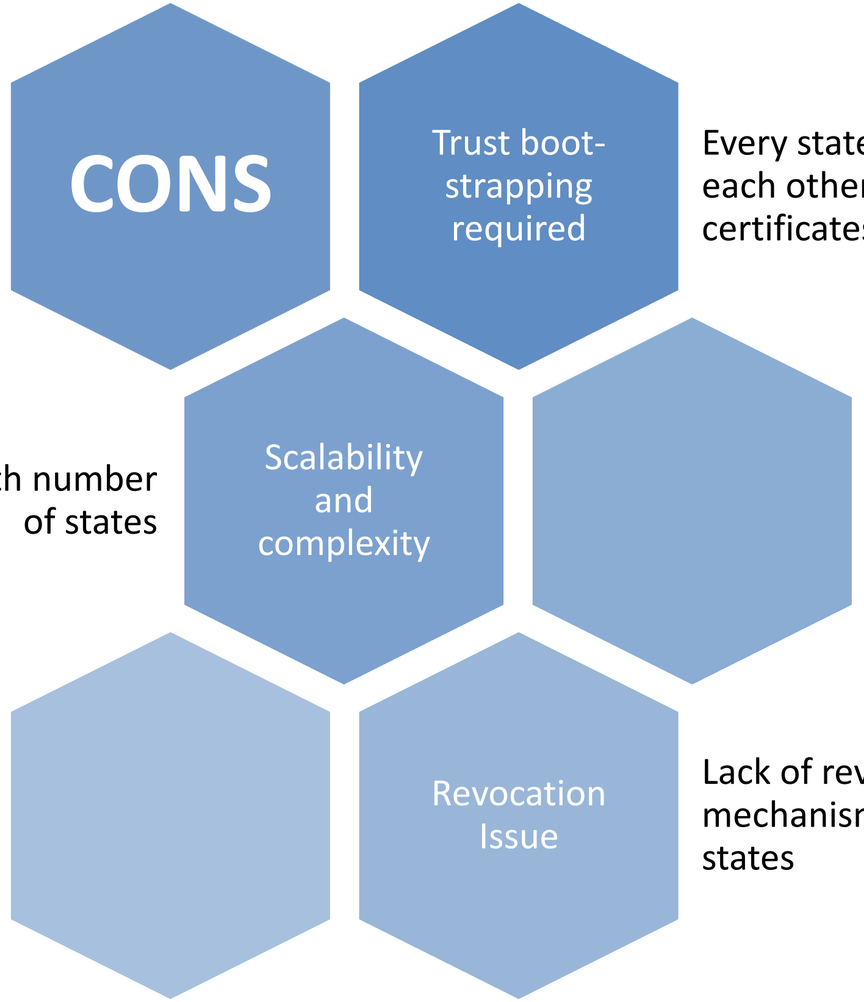
LESSONS LEARNED

The Pros and Cons



Each states manage its own CA and cert issuance lifecycle

No dependency on centralized or 3rd party CA



Every states must trust each other's root certificates manually

Increase with number of states

Lack of revocation mechanisms across states

Challenges

Trust Management

- Each states need to distribute its root cert, etc to others and keep it up to date
- During test we exchange via email

Certificate Rotation

- Requires coordinated updates between states

THANK YOU