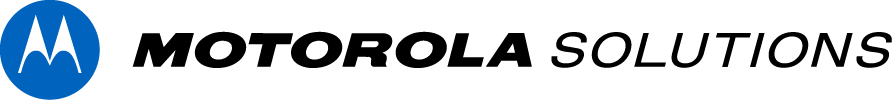
ATTACHMENT 3: Taiwan System Test Plan

System Test Platform to be a System

As NEW DESIGN CHANGE REQUEST,

TO DISCUSS!!

This Attachment is for new design change discussion, out of Scope



|  |  |
| --- | --- |
| Radio Solutions  Secure Products Group |  |

Taiwan System Test Plan

Version R01.00.08

Date: January 6, 2025

System Test Platform to be a System

As NEW DESIGN CHANGE REQUEST,

TO DISCUSS!!

This Attachment is for new design change discussion, out of Scope

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version # | Date | Author | Description |
| D01.00.01 | 11/9/10 | B. Pruss | Initial Revision |
| D01.00.02 | 12/2/10 | B. Pruss | Updates for second review |
| R01.00.03 | 12/8/10 | B. Pruss | Post-FTR updates |
| R01.00.04 | 1/11/11 | C. Perrin | Modified for System test |
| R01.00.05 | 1/14/11 | C. Perrin | Added Key Erase procedure through tamper |
| R01.00.06 | 1/25/11 | C. Perrin | Section 2.3: Clear / Coded Receive Indication Test Case corrected |
| R01.00.07 | 4/21/11 | C. Perrin | Section 2.1: Manual Loading of Algorithm Configuration Vectors and Traffic Key and Rejection of Invalid Algorithm Configuration Vectors Test Cases are removed. |
| R01.00.08 | 01/06/25 | Steven Chiang | Updated for latest equipment. |

References:

1. Taiwan Indigenous Algorithm Encryption Modification Plan
2. Taiwan Indigenous Algorithm Development Training

Table of Contents

[Revision History 58](#_Toc187165674)

[Table of Contents 59](#_Toc187165675)

[1 Introduction 60](#_Toc187165676)

[1.1 Purpose 60](#_Toc187165677)

[1.2 Scope of testing 60](#_Toc187165678)

[1.3 Definitions 60](#_Toc187165679)

[1.4 References 61](#_Toc187165680)

[1.5 Test System 61](#_Toc187165681)

[1.6 Entry Criteria 61](#_Toc187165682)

[2 Test Cases 62](#_Toc187165683)

[2.1 KVL Features 62](#_Toc187165684)

[2.2 Radio Features 63](#_Toc187165685)

[2.3 VPM (Console) Feature 64](#_Toc187165686)

[2.4 Key Erase/Tamper Test Cases 66](#_Toc187165687)

[2.5 Key Management Facility (KMF) 67](#_Toc187165688)

[2.6 Additional Test Case (OTAR) 70](#_Toc187165689)

[2.7 Additional Test Case (Data over CFX Audio) 71](#_Toc187165690)

**List of Figures**

[Figure 1 Encryption Verification System 密式驗證平臺 61](#_Toc186204151)

# Introduction

## Purpose

This document captures the test cases to be used for customer testing of the Taiwan Home-Country Algorithm and the products using it. This algorithm will be a configurable form of AES, where various constants used in the encryption computation may be input as Algorithm Configuration Vectors in the form of a System Key.

In test cases where an algorithm is not specified, the Taiwan algorithm is to be used. Also, note that the KVL will load its configured Config Vectors / System Key automatically whenever a traffic key is loaded.

Where possible and applicable, the testing is to be performed on a Digital Trunking system, in order to match the customer’s system.

The goal of the testing is to cover the following:

* Loading of product updates for each box if required.
* Regression testing of all secure functionality.

## Scope of testing

Test cases will cover the following products:

* APX8500 (MACE)
  + Three required
* KVL5000
  + One required
* KMF / CRYPTR-2
  + One required
* VPM (Console, AIS)
  + One each required
* PC with Indigenous algorithm config tool (as Accessory software, hardware and tools related to Encryption Modification 「密式置換相關附屬軟硬體及工具)
  + One required

## Definitions

AES Standard AES Algorithm

ADK Advanced Algorithm Development Kit

BTS RF Base Station

CAP P25 Compliance Assessment Program

CFX Taiwan Home-Country Algorithm, currently in use by Navy

CSIST National Chung-Shan Institute of Science and Technology

EVS Encryption Verification System 密式驗證平臺

KMF Key Management Facility

KMM Key Management Messages

KVL Key Variable Loader

MACE Subscriber Motorola Advanced Crypto Engine

MSTL Motorola Solutions Taiwan Limited

NCSIST National Chung-Shan Institute of Science and Technology 國家中山科學研究院

NIST National Institute of Standards and Technology

OTAR Over-The-Air-Rekeying

SOW NCSIST SC12060P-CS移動臺等10項 工作說明書

STP System Test Platform

SU Subscriber Radios

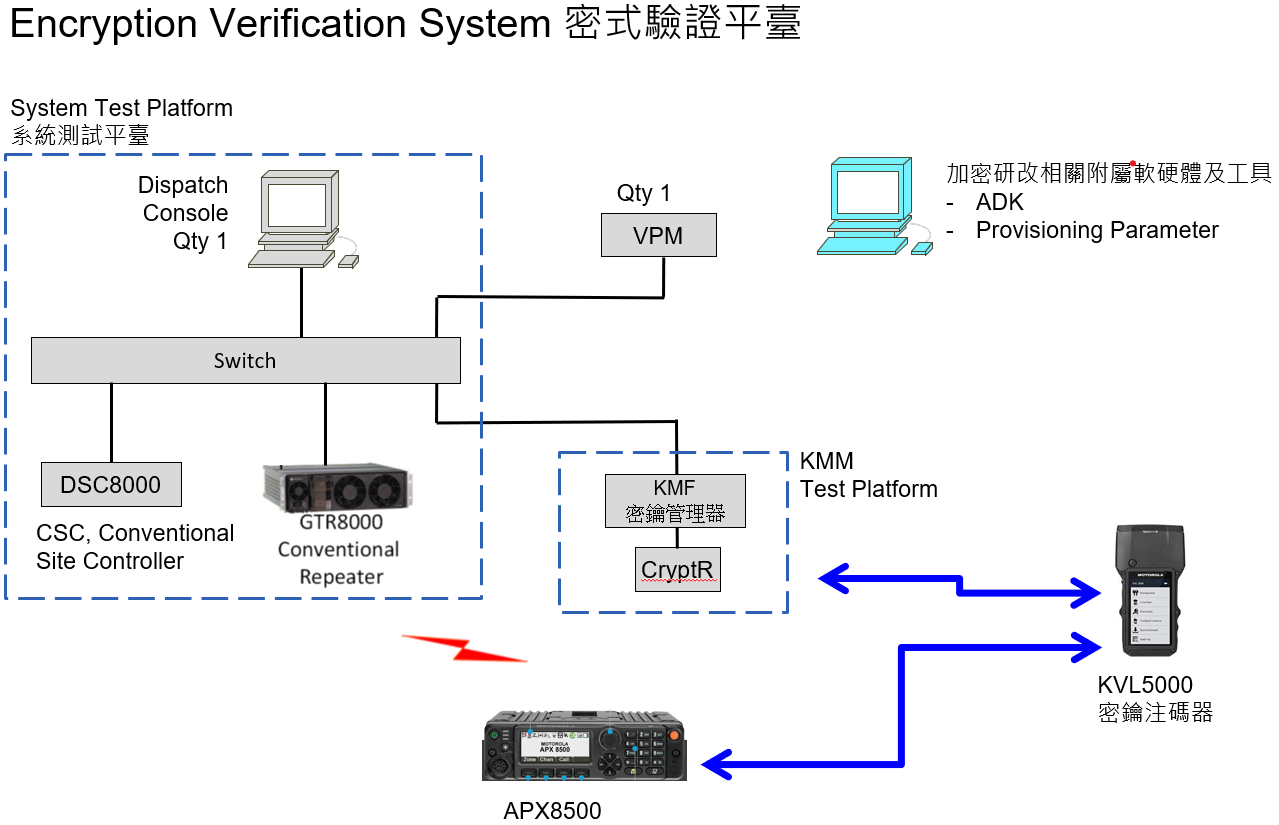
## References

1. NCSIST SC12060P-CS移動臺等10項 工作說明書 (hereafter refers as SOW).

2. SOW Chapter 7.1 Encryption Verification Work Items密式驗證配合事項.

## Test System

The testing will be performed in Taiwan using Encryption Verification System (密式驗證平臺) as illustrated in Figure 1 below.



System Test Platform as System

A NEW DESIGN CHANGE REQUEST

TO DISCUSS!!

Figure Encryption Verification System 密式驗證平臺

To mimic the customer’s desired setup, the system will be setup to use both AES256 and the Taiwan Algorithm CFX256 together. All test cases should be performed at least once with each algorithm. In cases requiring the use of subscribers, the tests should also be performed at least once with mobiles.

## Entry Criteria

The following criteria must be met before the start of testing

* DIA development must be complete
  + Code updates must be completed, reviewed, built, and regression tested at the box level.
* Application updates are complete for each box under test
  + Development teams must provide appropriate upgrade media with the new DIA and updated application software to the test team. The test team will use these to perform the upgrades as part of testing.
  + Update media must allow loading of the new DIA alongside AES256. All testing will be performed on both algorithms.

# Test Cases

## **KVL Features**

**Algorithm Verification**

1. **DESCRIPTION**

Verify that the KVL can be loaded with the algorithm alongside standard AES, and that it reports the correct name and properties for both afterwards.

**SETUP**

KVL-1 – Taiwan Algorithm equipped

Keyload cable

1. **TEST**

Step 1. Power on the KVL.

Step 2. Verify that the Taiwan Algorithm is present in the KVL, and activate it. Verify further that AES256 is also present and activated.

**Automatic Entry of Algorithm Configuration Vectors**

1. **DESCRIPTION**

Verify that the KVL can accept Config Vectors from over its RS-232 port.

**SETUP**

KVL-1 – Taiwan Algorithm equipped

PC – Contains Taiwan Algorithm configuration loading tool, with a valid set of non-default vectors loaded.

SU-1 - Taiwan Algorithm equipped

SU-2 - Taiwan Algorithm equipped

Keyload cable

1. **TEST**

Step 1. Revert the KVL to the default system key. Input a new traffic key, and load it into two radios. Verify that they can communicate.

Step 2. Connect the KVL to the PC using an RS-232 cable. Execute the loading tool and verify that it indicates success. Input the same traffic key as before, and load it into one of the radios. Verify that the radios cannot communicate and gollywobbles are heard. Load the key into the other radio, and verify that the radios can now communicate successfully.

## **Radio Features**

**Algorithm Verification**

1. **DESCRIPTION**

Verify that the Subscriber MACE can be loaded with the algorithm alongside standard AES256, and that it reports the correct name and properties afterwards for both.

**SETUP**

KVL-1

RADIO-1

Keyload cable

1. **TEST**

Step 1. Power on the Radio.

Step 2. Enter Service Mode on the Subscriber. Verify that the Taiwan Algorithm and AES256 are both reported.

**Coded Mode**

1. **DESCRIPTION**

Subscribers can communicate to each other through on a channel in a conventional system in a coded or clear manner. selectable via the TMSS switch. The radios must be configured to be selectable (secure or clear).

**SETUP**

RADIO-1 – Channel 1 (SECURE)

RADIO-2 – Channel 1 (SECURE)

RADIO-3 – Channel 1

RADIO-3 should not be secure-capable, should not have a key loaded or should have a different encryption key than RADIO-1 and RADIO-2.

1. **TEST**

Step 1. Initiate a call on RADIO-1 in the coded mode on a conventional system, using a Taiwan Algorithm key and algorithm configuration vectors (select encryption on the TMSS switch).

Step 2. Verify communications on RADIO-2 (coded).

Step 3. Verify that RADIO-3 does not hear the conversation even though it is on the same channel as RADIO-1 & RADIO-2.

Step 4. Initiate a call on RADIO-1 in the clear mode.

Step 5. Verify RADIO-2 and RADIO-3 hear the conversation.

Step 6. Repeat steps 1-6 with standard AES-256.

## **VPM (Console) Feature**

**Algorithm Verification**

1. **DESCRIPTION**

Verify that the VPM MACEs loaded with the algorithm alongside standard AES256, and that it reports the correct name and properties afterwards for both.

**SETUP**

KVL-1

VPM-1

Keyload cable

1. **TEST**

Step 1. Verify that the Taiwan Algorithm and AES256 are reported.

**Clear / Coded Receive Indication**

1. **DESCRIPTION**

A call from a subscriber unit to a VPM console is indicated on each dispatch operator position that has a Channel Resource associated with the channel the subscriber unit is transmitting on. Any time the console receives audio in a different mode from the configured setting for console transmit, a cross mode icon will be displayed.

**SETUP**

RADIO-1 – Channel 1

CONSOLE-1 Channel 1

1. **TEST**

Step 1. Select resource by moving the cursor over the Channel Resource's name and clicking the left mouse button.

Step 2. Verify that the resource is set for clear. A "pad lock" icon represents the clear/coded option. If the pad lock icon is open the outbound transmission is in the clear mode. If the pad lock icon is in the closed "lock" position, the outbound transmission is in the coded mode.

Step 3. Initiate a coded call from RADIO-1.

Step 4. Verify that the call icon, represented by the speaker icon, displays when the console receives audio. If the Channel Resource is selected, audio is heard through the Select speaker. If the Channel Resource is not selected, audio is heard through the Unselect speaker.

Step 5. In addition to the call indication, the user should see a cross mode indication on the screen.

Step 6. De-key RADIO-1. Verify that the call indication is no longer displayed, and that the cross mode indication ends.

Step 7. PTT on the selected channel. Verify that the radio can hear the VPM (RADIO-1 must be configured to allow clear or encrypted calls).

Step 8. Verify steps 1-7 for an incoming clear call when console is set to coded as needed and that RADIO-1 can hear the clear call.

Step 9. Verify steps 1-7 for an incoming encrypted call when console is set to encrypted but ensure no cross-mode indication is seen. Verify that the PTT from the VPM can be heard on RADIO-1

Step 10. Verify steps 1-7 for standard AES-256.

## **Key Erase/Tamper Test Cases**

**Key Erase through Power Removal in Subscriber**

1. **DESCRIPTION**

Verify that the loses keys after removing power for sufficient time.

**SETUP**

KVL-1

2 APX8500 Subscribers (RADIO 1 and RADIO 2) provisioned with Taiwan algorithm and configurable parameters

Keyload cable.

Infinite Key Retention disabled.

1. **TEST**

Step 1. Load the same key into RADIO 1 and RADIO 2. Verify that encrypted calls can be made.

Step 2. Remove the power from RADIO 1. For 10 minutes.

Step 3 Replace the power in RADIO 1 and turn on the radio.

Step 4 Ensure RADIO 1 TMSS is set to secure. Verify that the Secure Fail tone is emitted. Verify that the screen shows Key Fail with the tone.

**Key Erase through Control Panel on Subscriber**

1. **DESCRIPTION**

Verify that the keys loss from the unit.

**SETUP**

KVL-1

2 APX8500 Subscribers (RADIO 1 and RADIO 2) provisioned with Taiwan algorithm and configurable parameters, infinite key retention disabled.

Keyload cable.

1. **TEST**

Step 1. Load the same key into RADIO 1 and RADIO 2. Verify that encrypted calls can be made.

Step 2. Remove the keys from the radio by the its control panel.

Step 3 Verify that the Secure Fail tone is emitted.

## **Key Management Facility (KMF)**

**Algorithm Loading**

1. **DESCRIPTION**

Verify that the KMF CRYPTR-2 loaded with the algorithm alongside standard AES256, and that it reports the correct name and properties afterwards for both.

**SETUP**

KVL-1

KMF-1

Keyload cable

1. **TEST**

Step 1. Verify that the Taiwan HCA and AES256 are reported.

**Adding Keys to the Key Kettle**

1. **DESCRIPTION**

A Key Kettle is a repository for keys. Keys can be entered into and extracted from the Key Kettle as needs determine. The KMF allows encryption keys to be stored two different ways in the KMF system: with or without Key ID (KID) numbers. Encryption keys stored in the KMF without KIDs show up in a Key Kettle - one kettle per algorithm. Keys are then added to the KMF database from the Kettle, at which point, the key disappears from the Kettle, a KID is assigned to it, and it shows up inside the Keys list.

In this test, 5 Keys will be added to the Key Kettle.

**SETUP**

Load a Taiwan HCA Master key into the KMF CRYPTR-2. This will also load the Algorithm Configuration Parameters (System Key) into the KMF system.

1. **TEST**

Step 1. From the KMF Client window, select the Security menu and then the Kettle Keys menu item.

Step 2. Select the desired Algorithm for which keys will be added. (type - AES for example).

Step 3. Click the button that corresponds to the input method, in this case 'Keyboard.'

Step 4. Enter the Key Data in the Key Kettle dialog box.

Step 5. Click on the 'Save and New.'

Step 6. Add four additional Keys by repeating Steps 4 and 5.

Step 7. Click the 'Close' button.

**Creating Unique Key Encryption Keys (UKEKs)**

1. **DESCRIPTION**

The KMF client operator must create Unique Key Encryption Keys (UKEKs) for all valid Store and Forward system subscribers. The Unique Key Encryption Key (UKEK) is a unique key used to perform inner-layer encryption. It is assigned to a radio for encrypting keys within Key Management Messages (KMMs).

**SETUP**

There should be at least one key available in the Key Kettle corresponding to the Algorithm being used.

1. **TEST**

Step 1. From the KMF Client window, select the Security menu and then the Keys menu item.

Step 2. Click the 'New' button.

Step 3. Create the Key Name.

Step 4. Choose the Key Source as 'Keyboard.'

Step 5. Select the Key Algorithm from the drop down menu or type in the correct algorithm. (type - AES).

Step 6. Select the Key Type of UKEK.

Step 7. Type in the Key Data.

Step 8. Click on the 'Save and Close' button.

Step 9. Repeat Steps 2-8 with a Key Source of 'Key Kettle.'

**Creating Traffic Encryption Keys (TEKs)**

1. **DESCRIPTION**

The KMF client operator must create Traffic Encryption Keys (TEKs) for all valid Store and Forward Common Key References (CKRs). The Traffic Encryption Key (TEK) is used to encrypt voice, data, or Key Management Messages (KMMs), and is assigned to CKRs.

In this test, six TEKs will be created.

**SETUP**

There should be at least two keys available in the Key Kettle corresponding to the Algorithm being used.

1. **TEST**

Step 1. From the KMF Client window, select the Security menu and then the Keys menu item.

Step 2. Click the 'New' button.

Step 3. Create the Key Name.

Step 4. Select the Key Algorithm. (type - AES).

Step 5. Select the Key Type of TEK.

Step 6. Choose the Key Source as 'Keyboard.'

Step 7. Type in the Key Data.

Step 8. Click on the 'Save and Close' button.

Step 9. Repeat Steps 2-8 with a Key Source of 'Key Kettle.'

Step 10. Repeat Steps 2-9 twice for an additional 4 TEKs. These TEKs will be used in later tests.

## **Additional Test Case (OTAR)**

**Full Update to Subscriber (OTAR)**

1. **DESCRIPTION**

The entire set of encryption keys (in addition to other state parameters) are sent to a radio using the Full Unit Update command.

Note: The devices under test must have a valid air address registered with the KMF and must be accessible on the data system.

**SETUP**

RADIO-1 - TALKGROUP 1 (Secure Mode)

RADIO-2 - TALKGROUP 1 (Secure Mode)

RADIO-2 will be a reference radio.

Note: It is assumed that both radios under test are current with the KMF.

1. **TEST**

Step 1. Delete both TEKs from the CKR assigned to the talkgroup under test, from RADIO-1.

Step 2. Using RADIO-1, verify when the subscriber is set to secure mode, the radio indicates a key fail.

Step 3. Go to the Radio Management page of the KMF.

Step 4. Select RADIO-1 from the list.

Step 5. Initiate a Full Update operation.

Step 6. Go to the Operation Status page of KMF, verify that RADIO-1’s Full Update operation is shown. The operation is complete when the Operation Status is “Completed.” Note that a warmstart operation will occur if the TEK selected for the OTAR session is one of the TEKs assigned to CKR.

Step 7. Now that RADIO-1 contains the keys in the CKR, verify secure communications between RADIO-1 and RADIO-2.

## **Additional Test Case (Data over CFX Audio)**

**Data over CFX Audio**

1. **DESCRIPTION**

Data over CFX Audio is achieved through a Data-Audio conversion that convert between data and Audio stream for further sending over voice channel with CFX encryption.

From Verification of CFX Encryption perspective, the way of verification for Data over CFX Audio is the same as CFX Audio based voice call to and from Mobile radio.

Data-Audio conversion tool is abbreviated as (“Tool”)

**SETUP**

RADIO-1 - TALKGROUP 1 (CFX Mode), connected with Tool 1

RADIO-2 - TALKGROUP 1 (CFX Mode), connected with Tool 2

RADIO-2 will be a reference radio.

1. **TEST**

**Both radios using CFX algorithm**

Step 1. Tool 1 converts data into audio and send to Radio-1. Radio-1 transmit this audio via CFX256 encryption

Step 2. Radio-2 receives this Audio and send to Tool 2. Tool 2 convert Audio into data.

**Radio-2 changes to AES256 algorithm**

Step 3. Tool 1 convert data into audio and send to Radio-1. Radio-1 transmit this audio via CFX256 encryption

Step 4. Radio-2 in AES256 cannot receive this Audio. Therefore, Tool 2 cannot convert Audio into data.