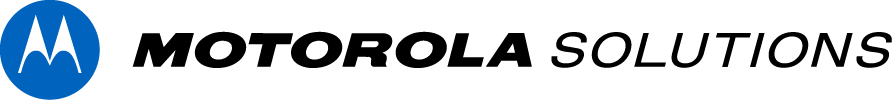
ATTACHMENT 1: Taiwan Indigenous Algorithm Encryption Modification Plan

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 Indigenous Algorithm

Encryption Modification Plan

6-Jan-25

Version: 0.7

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

**This document is subject to formal control procedure and will be stored electronically. The electronic version will be considered as the ‘Controlled’ copy. All printed copies will be considered as ‘Uncontrolled’.**

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Authors** | **Description** |
|  | 0.1 | C. Perrin/B. Pruss | Initial Creation |
| 10-January-2011 | 0.2 | C .Perrin | Updated according to inputs from Taiwan team. |
| 14-Jan-11 | 0.3 | C. Perrin | Updated training plan outline. |
| 17-Jan-11 | 0.4 | C. Perrin | Fixed training description. |
| 25-Jan-11 | 0.5 | C. Perrin | Chapter 2.1 description added.  Chapter 4.4 diagrams added.  Chapter 5 Training outline updated. |
| 21-Oct-24 | 0.6 | Steven Chiang | Content updated with latest equipment. |
| 6-Jan-25 | 0.7 | Steven Chiang | Content updated per NCSIST comment. |

References:

1. Taiwan Indigenous Algorithm Development Training
2. Taiwan System Test Plan

Table of Contents

[Revision History 10](#_Toc186207817)

[Table of Contents 11](#_Toc186207818)

[1 Introduction 12](#_Toc186207819)

[1.1 Abbreviations 12](#_Toc186207820)

[1.2 Definition 12](#_Toc186207821)

[2 Design Concept and Detail 13](#_Toc186207822)

[2.1 Design Concept 13](#_Toc186207823)

[2.2 Design Details 13](#_Toc186207824)

[2.2.1 Algorithm Development Kit (ADK) 14](#_Toc186207825)

[2.2.2 Configurable Parameters Provisioning Tool 14](#_Toc186207833)

[2.2.3 KVL5000 with Base Algorithm 15](#_Toc186207834)

[2.2.4 Tamper Mechanism 15](#_Toc186207835)

[2.2.5 Over-The-Air-Rekeying (OTAR) 15](#_Toc186207836)

[2.2.6 Data over CFX Audio 16](#_Toc186207837)

[3 Configurable Algorithm Parameters 16](#_Toc186207839)

[3.1 Substitution Box 16](#_Toc186207840)

[3.1.1 S-Box Background 16](#_Toc186207841)

[3.1.2 S-Box Modification Specification 17](#_Toc186207842)

[3.1.3 S-Box Solution 17](#_Toc186207843)

[3.2 Mix Columns 17](#_Toc186207844)

[3.2.1 Mix Columns Background 17](#_Toc186207845)

[3.2.2 Mix Columns Specification 18](#_Toc186207846)

[3.2.3 Mix Columns Solution 18](#_Toc186207847)

[3.2.4 Algorithm Modes 18](#_Toc186207848)

[4 Encryption Development Process 18](#_Toc186207849)

[4.1 Training 18](#_Toc186207850)

[4.2 Algorithm Development using the ADK 18](#_Toc186207851)

[4.3 Test and Validation 19](#_Toc186207852)

[5 Training Outline 21](#_Toc186207853)

**List of Figures**

[Figure 1 Customized Algorithm Concept 13](#_Toc186207806)

[Figure 2 Algorithm development cycle 13](#_Toc186207807)

[Figure 3 Algorithm ADK (Sample screen) 14](#_Toc186207808)

[Figure 4 Conversion of Customer Unique Settings for Loading into Target 15](#_Toc186207809)

[Figure 5 KVL5000 with Keyload port 15](#_Toc186207810)

[Figure 6 - Over-The-Air Rekeying (OTAR) 16](#_Toc186207811)

[Figure 7 S-Box 16](#_Toc186207812)

[Figure 8 Mix Column 17](#_Toc186207813)

[Figure 9 Test and Validation 19](#_Toc186207814)

[Figure 10 Encryption Verification System 密式驗證平臺 20](#_Toc186207815)

[Figure 11 Algorithm Modification Process 20](#_Toc186207816)

# Introduction

This document describes the concepts, processes and procedures for developing an indigenous algorithm (Encryption modification) using Motorola’s tools.

This document is broken in 5 sections as follows.

Section 1: Introduction.

Section 2: Outlines the design concept for the indigenous encryption algorithm, followed by a detailed description of the design concept and tools used to support the development. Then an overview of what is configurable by the customer and how they can make the changes will be explained. This allows the customer to understand the concept and how it is achieved.

Section 3: Outlines the configurable parameters in detail so the customer understands what facet of the algorithm will be unique.

Section 4: Outlines the development process from initial implementation in software to final testing on the products. This allows the customer to understand the order of development and the tools used.

Section 5: Outlines the training plan in terms of areas that will be covered. This allows the customer to understand what will be covered to allow them to create their unique algorithm without Motorola input.

## Abbreviations

AES Standard AES Algorithm

ADK 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

KVL Key Variable Loader

KMF Key Management Facility

KMM Key Management Messages

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

System Test Platform as System

A New Design Change Request

To

DISCUSS!!

V&V Vivian & Vincent International Trading Co., Ltd.

## Definition

Encryption Modification as 密式置換 in SOW.

Encryption Verification System as 密式驗證平臺 in SOW

KMM Test Platform as the machine for verified KMM messages.

System Test Platform as 系統測試平臺 in SOW.

# Design Concept and Detail

## Design Concept

The indigenous encryption algorithm development is based upon the concept of starting with a base algorithm, in this instance AES, then using software and tools to make modifications to a pre-determined set of customizable parameters. The end result is a unique algorithm specific to the customer.

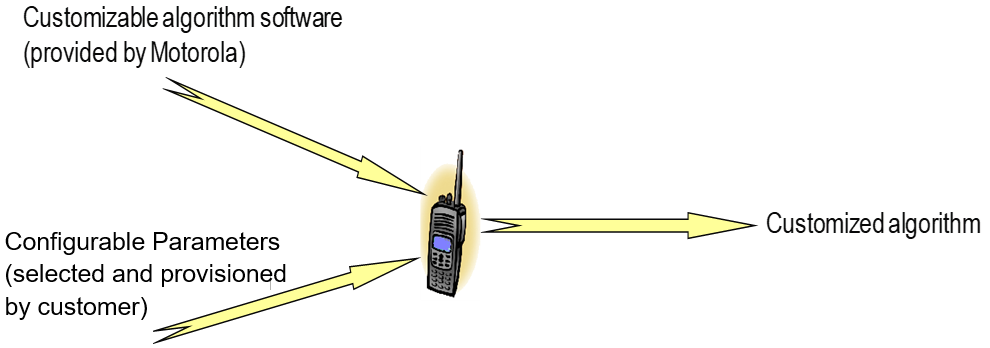


Figure Customized Algorithm Concept

The modifications to the configurable parameters are made by the customer without any knowledge or input from the vendor.

The modified AES algorithm will have performance that meets the P25 requirements for voice encryption.

Note: the settings for Standard AES and the modified AES with this specific algorithm implementation will have the same performance. Although the original algorithm implementation took advantage of known industry optimizations, the performance from this unit will meet the needs for P25.

## Design Details

The design concept is realized through the use of an algorithm software development kit that allows the customer to change the configurable parameters. Then the customer can test the changes and, once the final settings have been selected, program them into the subscribers and infrastructure equipment.

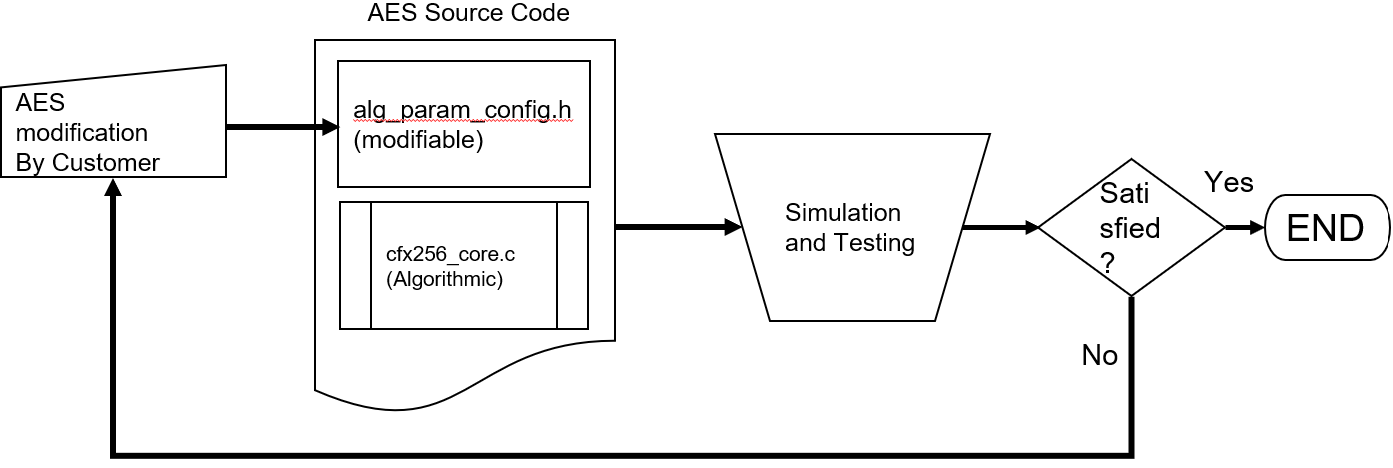


Figure Algorithm development cycle

The process is complete when the software is loaded into the subscribers and the infrastructure devices along with the customer specific algorithm settings.

The process is supported through the use of an ADK Computer as part of **Accessory software, hardware and tools related to Encryption密式置換相關附屬軟硬體及工具**. A computer installed with

1. ADK (Algorithm Development Kit) and
2. Configurable Parameter provisioning Tool that programs a KVL with the customer settings to be programmed into the target devices.

System Test Platform as System

A New Design Change Request

To DISCUSS!!

Each of these is outlined below.

### Algorithm Development Kit (ADK)

The initial development of the indigenous algorithm is completed using a ADK with a customized project from Motorola. The project contains the main code for the customizable algorithm. A snap shot is shown below.

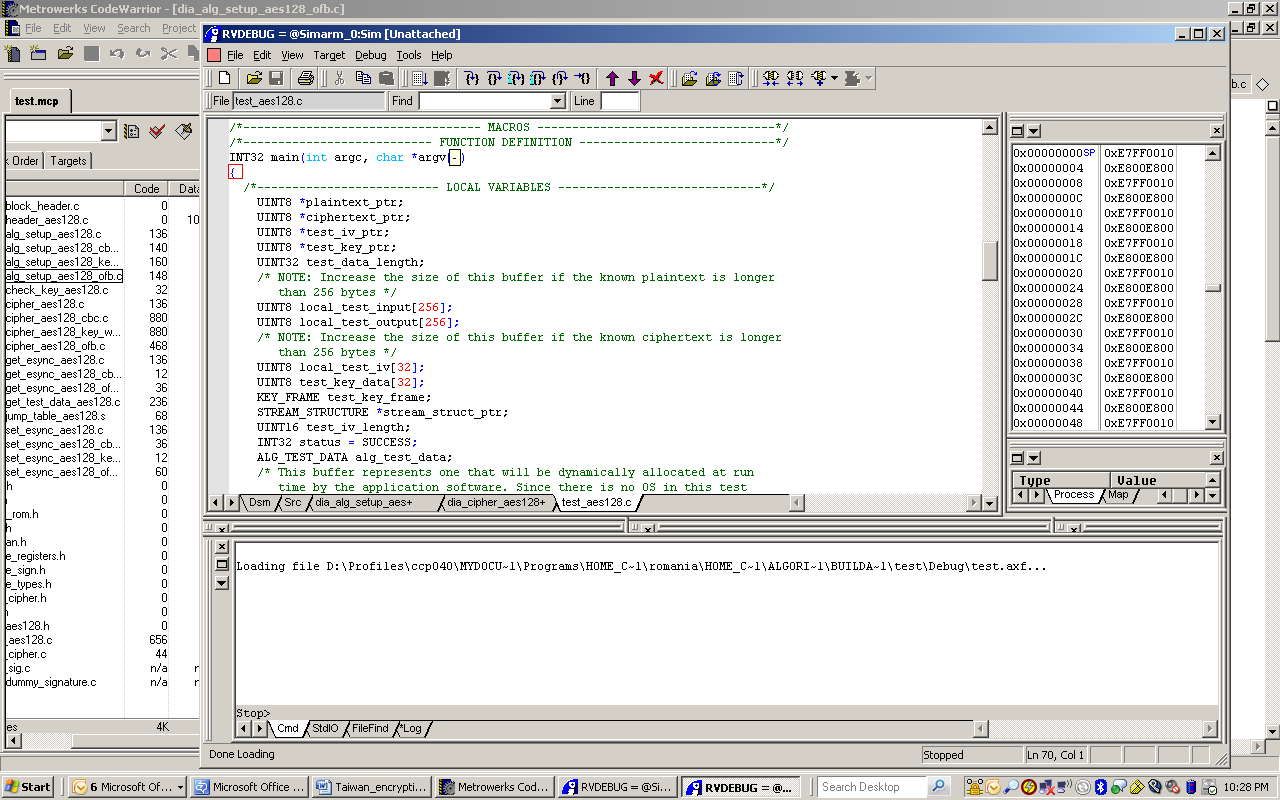


Figure Algorithm ADK (Sample screen)

### Configurable Parameters Provisioning Tool

Once the configurable parameters have been determined and verified using the ADK and the Simulator, the parameters are programmed into the subscribers and infrastructure devices using the configurable parameters provisioning tool and the KVL. The tool takes the values from the development kit and programs them (over RS-232) into the KVL ready for loading into a subscriber or infrastructure equipment that supports the customization.

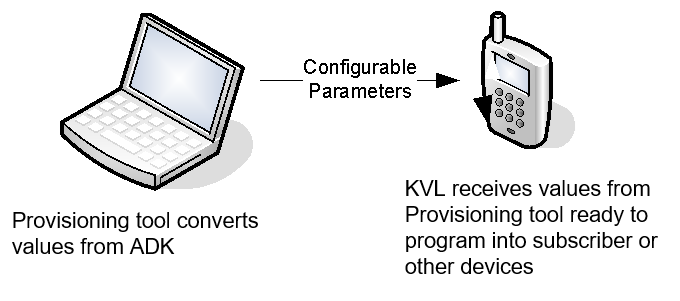


Figure Conversion of Customer Unique Settings for Loading into Target

### KVL5000 with Base Algorithm

The KVL5000 (“KVL”) is program with the base algorithm from Motorola that supports the customization. The KVL programs the target devices through the Keyload port on the KVL and the subscriber and infrastructure products.



Figure KVL5000 with Keyload port

### Tamper Mechanism

The CRYPTR-2 for KMF and the KVL both utilize a tamper mechanism associated with the crypto module. The KMF CRYPTR-2 hardware has a tamper detection mechanism. When the sealed, pressure-sensitive housing of the KMF CRYPTR-2 is opened or tampered with, the KMF CRYPTR-2 zeroizes all stored key material. In addition, there is an erase button which is available to clear key material manually.

The KVL has mechanism for tamper protection in that if personnel attempt to open the security unit, the critical security parameters are erased thus rendering the keys useless.

### Over-The-Air-Rekeying (OTAR)

OTAR provides the ability to rekey portable and mobile radios remotely over an RF channel. The KMF formulates and originates the OTAR messages and acts as the key manager for the system.

OTAR provides several benefits, including:

* Reducing the manpower and time in the field to rekey radio users manually, leading to improved productivity, and faster key changes.
* Offering an advanced key management solution that allows you to plan, generate, store, track, and maintain all encryption keys for the entire system using one central device instead of tracking everything on paper. This solution reduces key management resources.
* Providing the ability to change your encryption keys frequently that enhances the security of your system by eliminating security leaks.

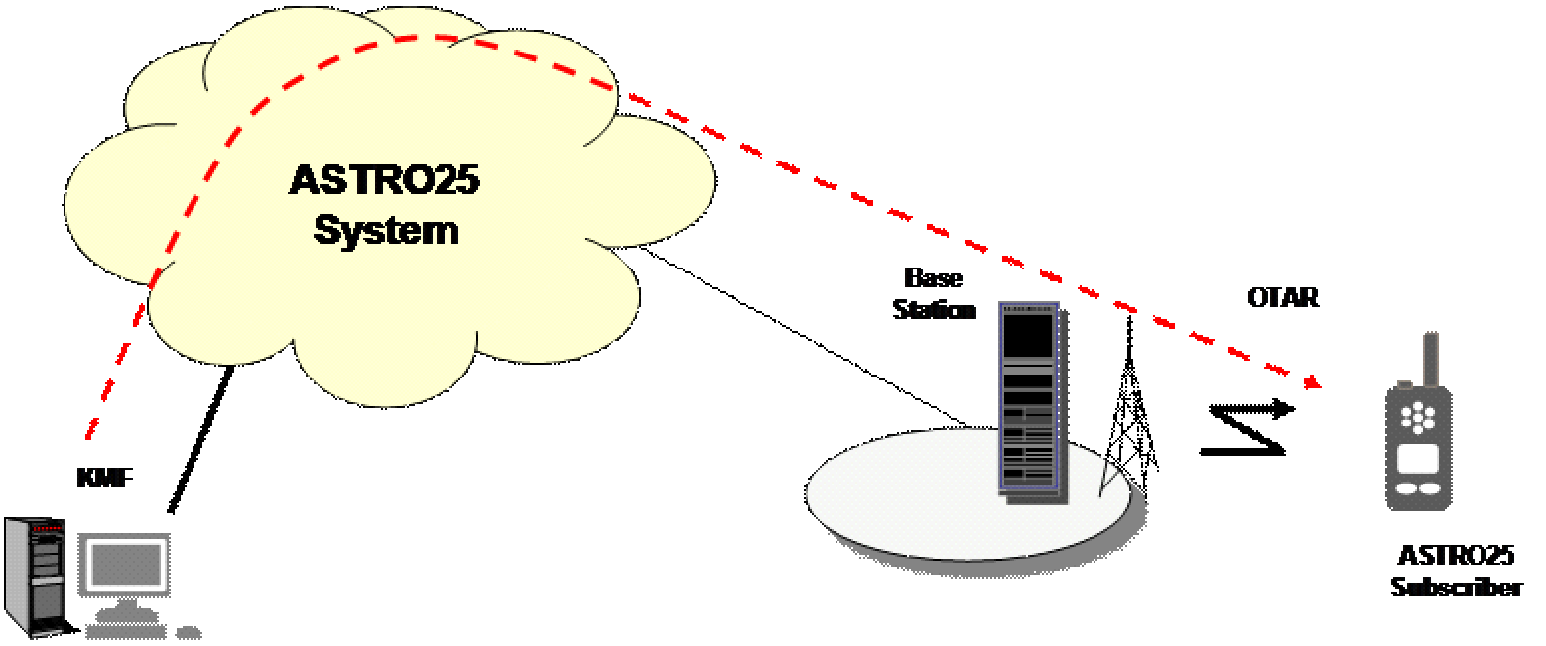
****

Figure - Over-The-Air Rekeying (OTAR)

### Data over CFX Audio

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.

# Configurable Algorithm Parameters

The ability to create a unique algorithm is the result of a base algorithm derived from AES combined with configurable algorithm parameters. These parameters have been selected because they allow a unique algorithm to be made that maintains the strong properties of AES while allowing customization.

## Substitution Box

### S-Box Background

The AES algorithm uses a Sub Bytes operation to modify the plaintext during the cipher. The Sub bytes operation is applied several times per cipher operation as part of a larger round.

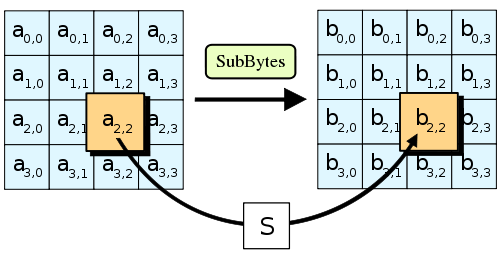


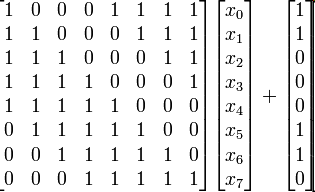
Figure S-Box

The sub bytes table is nominally set to the standard AES values but can be modified according to a set of rules outlined in Section 3.1.2.

### S-Box Modification Specification

The S-Box values are derived from a combination of two mathematical functions. These are outlined as follows:

1. Compute multiplicative inverse of the byte over a selected Finite Field with order of 28. The Finite Fields are defined by Polynomial values. The standard AES polynomial for this purpose is x8 + x4 + x3 + x + 1 however there are 29 other valid options are available.
2. Apply an Affine transformation to the result. This is defined here as multiplication by an 8x8 binary matrix, followed by addition of an 8-element binary vector. The standard AES matrix and vector is as follows:



There are other matrices available that are valid. The matrix must be invertible and the determinant must not be 0.

### S-Box Solution

The solution is that the S-Box is entered as the S-box constituent constants. These constants consist of the finite field polynomial (represented by irreducible polynomial, see note 1 on Section 3.2.3), the Affine Transformation Matrix (1 byte) and the Affine Transformation Vector (1 byte).

## Mix Columns

### Mix Columns Background

The mix columns functionality applies a linear transformation on each column of a state array. The transformation is applied several times per cipher as part of each round.

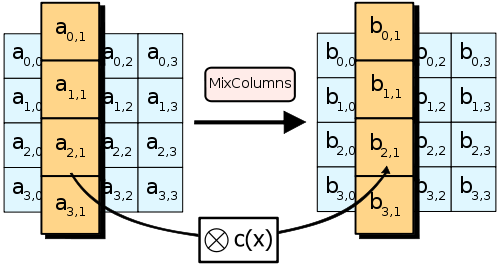


Figure Mix Column

### Mix Columns Specification

The mix columns transformation involves multiplication by a fixed polynomial modulo x4+1 over a Finite Field. The Polynomial must be invertible (thus implying that it must be coprime to x4+1). The modulo x4+1 will remain as per standard AES. Therefore, the steps are outlined as follows:

1. Specify the Galois Field Polynomial. (note: must be irreducible)
2. Specify the Forward MixColumns Polynomial.
3. Specify the Reverse MixColumns Polynomial.

### Mix Columns Solution

The MixColumns Matrix must be derived using the following mechanism:

* + GF Polynomial (see note 1)
  + Forward FirstColumn Polynomial (4 bytes)
  + Reverse FirstColumn Polynomial (4 bytes)

Validation will be performed on each parameter as follows:

* + GF Polynomial must be irreducible (30 options, validated by lookup table)
  + Two matrices Polynomials above will be multiplied together to validate that the product is the Identity Matrix

Note 1: The all 9 bits of the Irreducible Polynomial can allow to be specified. However, the code will need to reject all values that do not have the 9th bit set to 1. That is a mathematical necessity - the algorithm cannot generate usable output if that is not true.

### Algorithm Modes

The algorithm modes used associated with voice and key management are specified in document *“*TaiwanIndigenous Algorithm Development Training*”.*

# Encryption Development Process

The encryption development process consists of 3 stages:

1. Training on Motorola key management and encryption modes, ADK usage, testing and validation
2. Algorithm development using the ADK
3. Test and validation on the target devices (subscriber and infrastructure)

## Training

The first step for the development of the algorithm is to provide training on the software development kit, loading the algorithm into the target and testing the final product. The training will consist of 1 week in Taiwan with the customer and the prime contractor. Further support for training will be handled through the prime contractor.

## Algorithm Development using the ADK

The customer will use the identified tools to make changes to the configurable parameters according to their unique algorithm specification after the training is complete. The vendor will not be present at this time but will provide remote support for any questions or issues.

The process of development and the tools used are covered in detail in document *“*TaiwanIndigenous Algorithm Development Training*”.*

## Test and Validation

The testing and validation of the unique algorithm in the target devices will consist of two facets:

1. Verify that the encryption taking place in the products is cryptographically correct (refer to section 8 of document “Taiwan Indigenous Algorithm Development Training”).
2. Verify that the products communicate correctly in the system (clear, encrypted, Store and Forward keyloading), details are to be referred to document “Taiwan System Test Plan”.

**Procedure:**

Step 1: The customer will use the capability of the KMM Test Platform to log the plaintext and the ciphertext of key management messages with the unique algorithm. Noted KMM Test Platform is part of Encryption Verification System (密式驗證平臺) as illustrated in Figure 10. The logs will then be used to verify the ciphertext is correct from the plaintext KMMs for both the encrypt and decrypt functionality, in this regard the verification simulator allows the customer to verify that the plaintext was correctly encrypted or decrypted (depending on the KMM being transmitted or received by the verification platform).

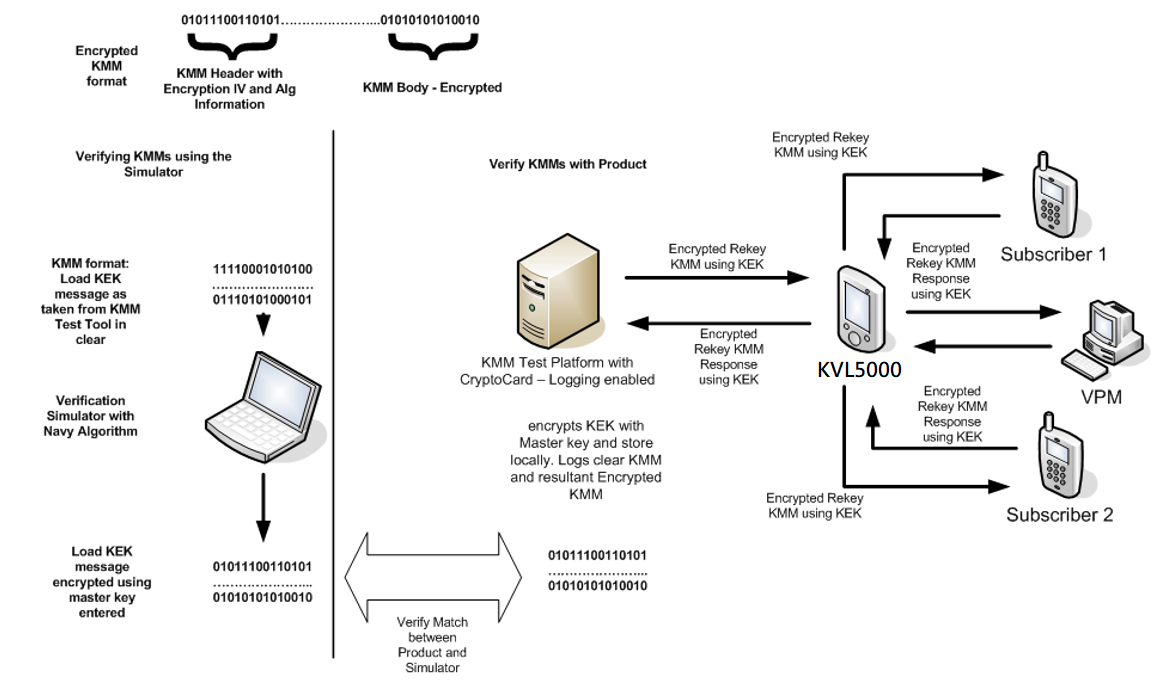
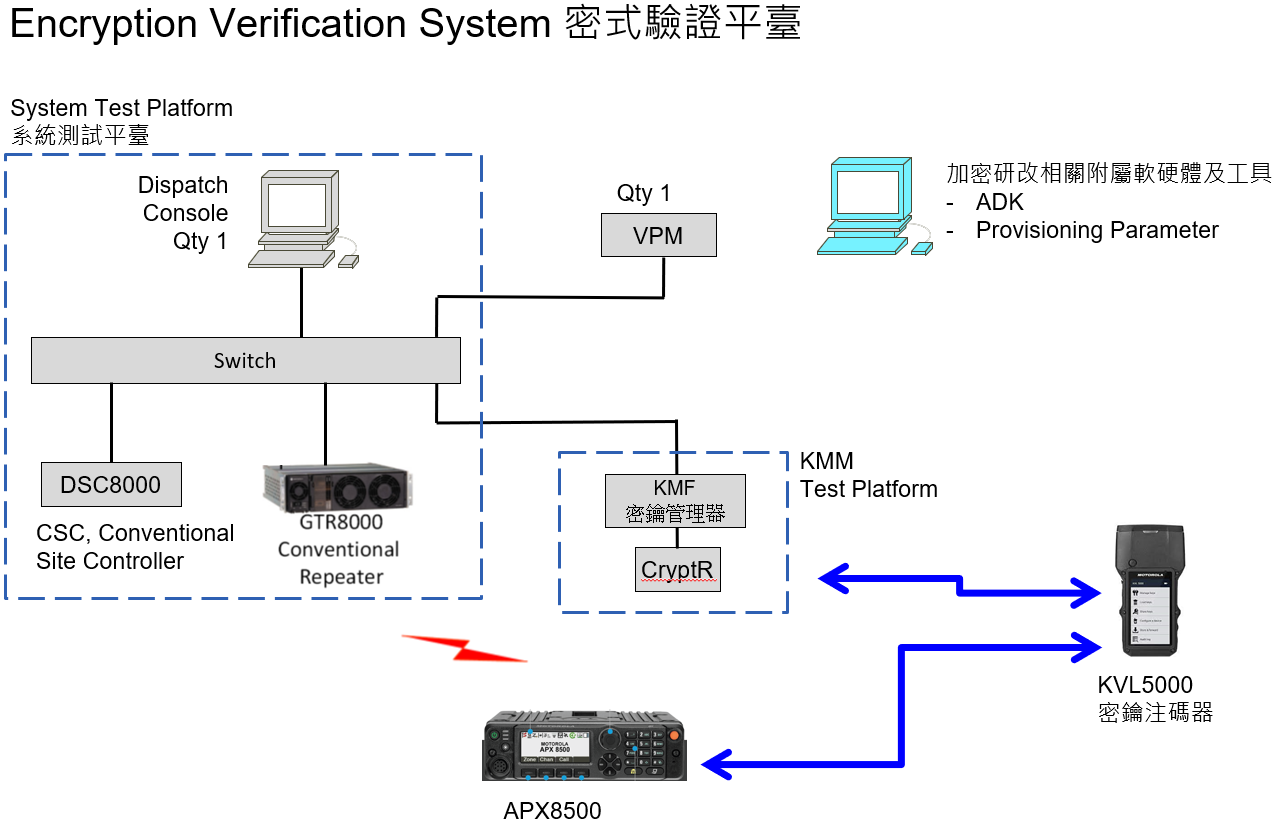


Figure Test and Validation

Step 2: This step is essentially to verify that the products communicate correctly in system (clear, encrypted, Store and Forward keyloading kind of standard system level functions). The customer can then verify that the target subscribers correctly decoded the key management message and stored the key by running an encrypted call through the two units. Once the customer is satisfied that the encryption is correct and that the subscriber has correctly decoded the key management messages, they can send new keys to the infrastructure (the voice processing module) and then try an encrypted call from the radio to the dispatch. This now verifies that the boxes all have the correct algorithm and process the keys and encryption correctly. Details are illustrated in Attachment 3 “Taiwan System Test Plan”.

Figure 10 illustrates Encryption Verification System (EVP) 密式驗證平臺, mainly consists of VPM, KMF, 加密研改相關附屬軟硬體及工具and System Test Platform (STP) 系統測試平臺. The STP works as integral part of EVP, and through EVP and KMF, allowing mutual encryption/decryption tests on mobile, dispatch stations or network management centers and system connectivity encryption verification.



System Test Platform as System

A New Design Change Request

To DISCUSS!!

Figure Encryption Verification System 密式驗證平臺

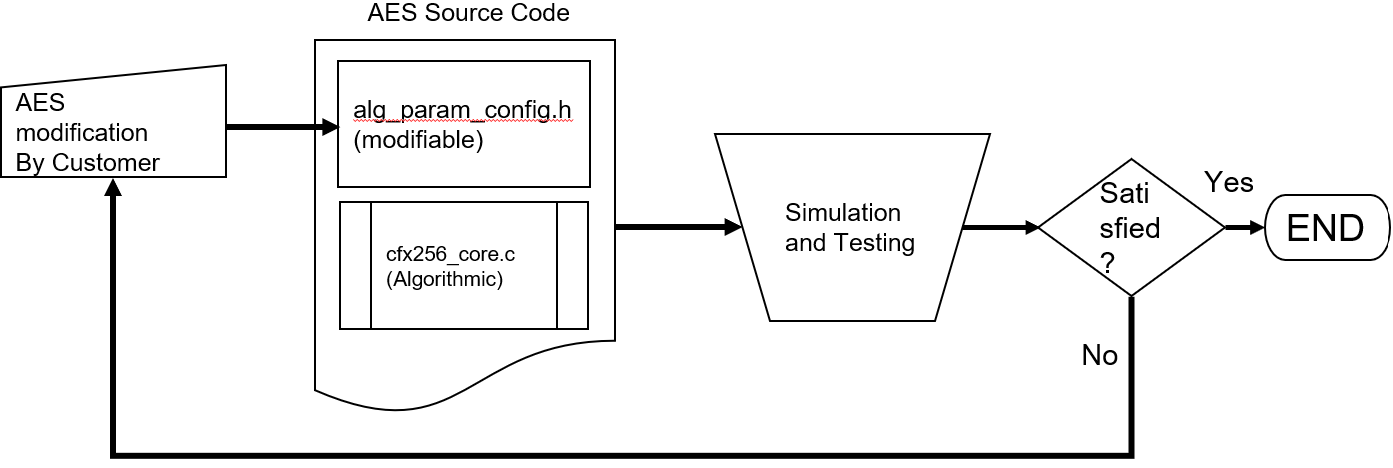


Figure Algorithm Modification Process

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

# Training Outline

Training will cover everything from understanding Motorola key management and encryption modes to programming and testing on the end product. The areas for training are documented in the table below.

| ****Training**** | ****Scope**** | ****Effort (Hrs)**** |
| --- | --- | --- |
| Motorola Encryption and Key Management | The Motorola key management and encryption mode training will focus on how keys are managed within a Motorola system and the modes of encryption used to encrypt the keys. The customer will then understand the basics of what types of keys exist within the system, how they are used (their role) and how they are distributed. The customer will also know the different modes of encryption applied to each key | 3 |
| ADK usage | The software development kit training will focus on how the software project is structured to define the base algorithm support and how the configurable parameters fit in the algorithm perspective. The training will then outline how the customer changes the configurable parameters, how to build the software for the simulation and, finally, how to verify the operation within the simulator. This allows the customer to understand what to change and how to test their configurable algorithm parameters before programming them into the target devices. | 3 |
| Motorola Home Algorithm Support (in ADK) | The training on the Motorola Home Algorithm Support will provide the customer with an understanding of the separation of the base algorithm for AES and how the software for the configurable parameters fits with the base algorithm. The customer will then understand the split of the functionality between the base algorithm that is provided and the parameters that they provide for the final algorithm. | 2 |
| Configurable Parameters and testing on simulator | The training on the configurable parameters outlines how the customer changes the configurable parameters, how to build the software for the simulation and, finally, how to verify the operation within the simulator. This allows the customer to understand what to change and how to test their configurable algorithm parameters before programming them into the target devices. | 2 |
| Practice run ADK Set up and usage | The practice run allows the customer to understand how the ADK works, how to make the changes associated with their algorithm and how to use the simulator for the verification of the algorithm.  Set up and basic use of ADK – 2 hrs  Configurable parameters modification – 2 hrs  Compile and test – 4 hrs  Running through simulator – 4 hrs  Testing and assistance – 6 hrs | 18 |
| Conversion of configurable parameters for target device Algorithm | The section on programming the configurable parameters into the target devices outlines the method and procedure to getting the final parameters from the ADK into the target devices that contain the Motorola base algorithm. | 4 |
| Practice run – system test | The section on system test execution outlines the process and procedure that the customer will follow to ensure that their final algorithm functions correctly within a Motorola system. This ensures that the standard functionality provided by Motorola products functions without issue with the customer algorithm.  Set up of system – 6 hrs  Test execution KMF – 6 hrs  Test execution radios – 4 hrs  Assistance – 4 hrs | 20 |
| Reviewing the KMF Logs | The system test encryption verification outlines the method used to verify the final encryption algorithm in the products within the system. The customer will learn how to run the system test, collect the necessary data, and validate the algorithm using the simulator and the collected data from the products. | 2 |
| Practice run alg verification | Customer uses tools to program and test on MACE and KMF - this allows the customer to see how the tools work and understand the mechanism for processing a key management message for verification. It also allows the customer to understand how to run the system to ensure that full functionality works with their algorithm.  KMM test platform set up – 4 hrs  Simulator to alg test system set up – 4 hrs  Running test – 5 hrs  Assistance – 5 hrs | 18 |