|  |
| --- |
| **encryption moDIfication plan**  **密式置換規劃書** |
|  |

**PO# PO27092401A‐GS**

System Test Platform to be a System

As NEW DESIGN CHANGE REQUEST,

TO DISCUSS!!

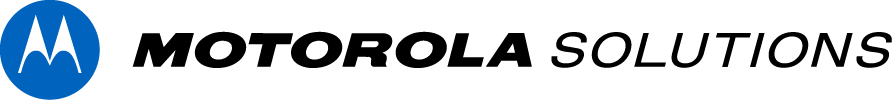
This document is for new design change discussion, out of Scope

Author: Steven Chiang

Number of Pages: 79

**Approval Signature for Motorola Solutions……….....………………………………………… Date……………………….**

**Printed name of representative.………………………………………………………………..**



Document Name: **Encryption Modification Plan**

Number of pages: 79

|  |  |
| --- | --- |
| 1. This document supersedes a previous document of different identity number? | No |
| 2. State the obsolete document number if answer to item 1 above is ‘Yes’. | N/A |

**Circulation Details:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Recipient** | **Address** | **No. of Copy** | **Sent By** | **Date Sent** |
| Mr. Tim Kao | Vivian & Vincent International Trading Co., Ltd. (V&V)  2F-4, No. 28, Lane 78, Xing-Ai Road, Nei-Hu Dist., Taipei City 11494, Taiwan R.O.C. | One |  |  |

Special notes:

Revision History

|  |  |  |
| --- | --- | --- |
| REV. | DATE | DESCRIPTION |
| A | 21 Oct. 2024 | First Motorola Issue to V&V for consolidation |
| B | 6 Jan. 2025 | 2nd Issue to V&V addressing with NCSIST Comments.  Attachment 2 renamed as “Taiwan Indigenous Algorithm Development Training”. |

Table of Contents

Revision History 3

Table of Contents 4

List of Attachments 4

1 Introduction 5

2 Abbreviations 6

List of Attachments

ATTACHMENT 1: Taiwan Indigenous Algorithm Encryption Modification Plan

ATTACHMENT 2: Taiwan Indigenous Algorithm Development Training

ATTACHMENT 3: Taiwan System Test Plan

ATTACHMENT 4: List of Equipment for System Test Platform and Accessories

ATTACHMENT 5: Encryption Modification Design and Verification – High Level Diagram

ATTACHMENT 6: Encryption Verification Standard Mapping List

System Test Platform to be a System

As NEW DESIGN CHANGE REQUEST,

TO DISCUSS!!

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

# Introduction

This document takes reference to:

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.

This document is elaborated in accordance with SOW Chapter 7.1.11 Encryption modification Plan 密式置換規劃書. This document describes the concepts, processes and procedures for developing an indigenous algorithm (Encryption modification) using Motorola’s tools.

The content mainly consists of 8 documents as listed below, each document does address a particular point of SOW and link one to another so the whole document package can fully covers SOW requirements.

Title: Taiwan Indigenous Algorithm Encryption Modification Plan

Version: 0.7

Enclosed to: Attachment 1

Title: Taiwan Indigenous Algorithm Development Training

Version: 0.9

Enclosed to: Attachment 2

Title: Taiwan System Test Plan

Version: D01.00.08

Enclosed to: Attachment 3

Title: List of Equipment for System Test Platform and Accessories for Encryption Modification

Version: 0.2

Enclosed to: Attachment 4

Title: Encryption Modification Design and Verification –High Level Diagram

Version: 0.1

Enclosed to: Attachment 5

Title: Encryption Verification Standard Mapping List

Version: 0.1

Enclosed to: Attachment 6

| **SOW Chapter 7.11 Clauses** | **Mapping to this document** |
| --- | --- |
| 1. Manufacturers must provide execution plans, processes, etc. for Encryption Modification.   廠商須提供「密式置換」執行規劃、流程等。 | Attachment 1. |
| 1. The manufacturer must provide the implementation method for Encryption Modification Training, which must include teachers, course content, hour allocation, etc. "   廠商須提供「密式置換技轉訓練」執行方式,需內含師資、課 程內容、時數配當等。 | Attachment 2. |
| 1. The manufacturer must provide the list and operation of the "System Test platform".   廠商須提供「系統測試平臺」清單及操作。 | Attachment 4.  Note: the manuals of respective equipment will be provided during Training session. |
| 1. The manufacturer must provide a list and operations of accessory software, hardware and tools related to Encryption Modification.   廠商須提供「密式置換相關附屬軟硬體及工具」清單及操作。 | Attachment 4.  Note: the manuals of respective equipment will be provided during Training session. |
| 1. The manufacturer must provide Description for operation and verification environment of Encryption Modification equipment.   廠商須提供密式置換裝備操作及驗證環境說明。 | Attachment 2 and 3.  Note: the manuals of respective equipment will be provided during Training session. |
| 1. Explain the encryption mechanism and key operation process.   說明加密機制與密鑰運作流程。 | Attachment 1 and 2. |
| 1. Describe key production management and related control actions.   說明密鑰產製管理與相關管控作為。 | Attachment 1 and 2. |
| 1. Explain the AES algorithm and parameter replacement (algorithm development environment and program code) methods and processes   說明 AES 演算法及參數置換(演算法開發環境與程式碼)方式與 流程。 | Attachment 1 and 2. |
| 1. Explain the flexibility and feasibility of Encryption Modification.   說明密式置換彈性與可行性範圍。 | Attachment 1 and 2. |
| 1. Explain the acceptance criteria for Encryption Modification, including testing and verification procedures.   說明密式置換驗收(含測試與驗證)程序。 | Attachment 3. |

# 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

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

SU Subscriber Radios

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

1. **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.

System Test Platform to be a System

As NEW DESIGN CHANGE REQUEST,

TO DISCUSS!!

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

ATTACHMENT 5: Encryption Modification Design and Verification – High Level Diagram