DATA ITEM DESCRIPTION

Title: Key and Certificate Management Plan (KCMP)

Number: DI-MISC-81688A
AMSC Number: 9760
DTIC Applicable: No
Preparing Activity: NS/I21/I213
Applicable Forms: N/A

Approval Date: 20170110
Limitation: N/A
GIDEP Applicable: No
Project Number: MISC-2017-001

Use/Relationship. The Key and Certificate Management Plan (KCMP) describes the use and control of cryptographic products and services used by a cryptographic application (cryptographic engine, cryptographic module, End Cryptographic Unit (ECU), or system) throughout its lifetime. The KCMP also identifies and documents the capabilities that the cryptographic application requires from the current and planned key management infrastructure.

a. KCMP Related Guidance**.** As the vendor of a cryptographic application may have very little insight into the items in the KCMP, the Information Assurance Certification Manager (IACM) will ensure the vendor uses the KCMP Template included as part of this DID and has the applicable Telecommunications Security Requirements Document (TSRD) cited under "Reference Documents." The TSRD is intended for use with the KCMP template to detail other related and relevant information not covered here.

b. This Data Item Description (DID) contains the content preparation instructions for the data product generated by the specific and discrete task requirement as delineated in the contract, as the Key and Certificate Management Plan (KCMP).

c. This DID supersedes DI-MISC-81688.

Requirements:

1. Reference Documents**:** The applicable issue of the documents cited herein, including their approval dates and dates of any applicable amendments, notices, and revisions, shall be as specified in the contract.

1.1 National Security Agency/Central Security Service (NSA/CSS) Policy Manual 1-52

1.2. Telecommunications Security Requirements (TSRD) Commercial Communications Security (COMSEC) Evaluation Program (CCEP), Section 2.9

1.3. TSRD User Participation Program (UPP), Section 2.9

1.4. Information Assurance Directorate (IAD) Management Directive 110 ("Cryptographic Key Protection")

1.5. Key and Certificate Management Plan (KCMP) Template, Version 1.0

1.6. CNSSI No. 4001, "Controlled Cryptographic Items (CCI)"

1.7. CNSSI No. 4031, “Cryptographic High Value Products (CHVP)”

1.8. CNSSI No. 4003, “Reporting and Evaluating COMSEC Incidents”

2. Format**.** The KCMP shall:

2.1 Be formatted strictly in accordance with the KCMP Template established for this purpose and that is referenced in paragraph 1.5 of this DID, under the “Reference Documents” section.

2.2 Be appropriately classified and portion marked in accordance with National Security Agency/Central Security Service (NSA/CSS) Policy Manual 1-52).

2.3. Be submitted in either Microsoft Word or Adobe PDF format. Adobe PDF format is preferred as it supports more efficient tracking and management of changes.

2.4. Not contain embedded files (i.e., Microsoft Visio drawings). All pictures and diagrams must be converted to a JPG or similar format.

2.5. Include a title page that minimally identifies the following:

a) Program Name
b) Contract Number
c) Contract Data Requirements List (CDRL) number
d) Revision and date
e) Program Manager’s name and telephone number and, if applicable, the NSA IACM’s name and office designator
f) Classification

2.6. Include a Revision Page, listing all past changes to the document in reverse chronological order.

2.7. Include a list of Reference Documents. This would include all documents used to develop the KCMP, approved key specifications used by the cryptographic application, and any special exceptions/waivers granted to the program.

2.8. Include a Table of Contents.

2.9. Include a Table defining all abbreviations and acronyms.

2.10. Total page count for the KCMP should not exceed 30 pages, with font size and type 12 Times New Roman. NSA reserves the right to return KCMPs numbering 30 or more pages with instructions to make them more concise and readable.

3. Content. The KCMP shall:

3.1. Be completed using the Key and Certificate Management Plan (KCMP) Template, Version 1.0, included in this DID. NOTE: Not all requested information will apply.

3.2. Contain only that information specifically requested. Including other information not specifically requested will lengthen the review time and consequently the approval of the KCMP.

4. The Key and Certificate Management Plan Template, Version 1.0, follows on the next page.

Key and Certificate Management Plan Template, Version 1.0

KEY AND CERTIFICATE MANAGEMENT PLAN FOR THE NAME OF THE PRODUCT/SYSTEM BEING CERTIFIED

UPA/MOA NUMBER: XXX
CDRL/ADRL: XXX
Project Classification: XXX
Submittal Date: XXX
Document ID: XXX
0N#: XXX
NSA IACM: XXX
Vendor Name POC: XXX
Vendor Name POC Phone #: XXX

ITAR Statement: (i.e., This technical data is controlled under the International Traffic in Arms Regulations (ITAR) and may not be exported to a Foreign Person, either in the U.S. or abroad, without proper authorization by the U.S. Department of State.)
Proprietary Statement: (i.e. Proprietary Rights are involved in the subject matter of this material and all manufacturing, reproduction, use and sales rights pertaining to such matter are expressly reserved. It is submitted in confidence for a specified purpose, and the recipient, by accepting this material, agrees that this material will not be used, copied or reproduced in whole or in part, nor its contents revealed in any manner, or to any person, except for the purpose delivered.)

Vendor Name
Address goes here

Revision Page

Rev	Description	Approval	Date
	Initial Release		

Table of Contents

1. INTRODUCTION

The Key and Certificate Management Plan (KCMP) describes the use and control of all key management products and services used by a cryptographic application (cryptographic engine, End Cryptographic Unit (ECU), or system) throughout its lifetime. The KCMP also documents the capabilities that the cryptographic application requires from the current and planned Key Management Infrastructure (KMI). This ensures that any lifecycle key management services are supportable by and available from the KMI.

1.1 Document Overview

This KCMP document is organized to conform to the requirements of NSA DI-MISC-81688A, Data Item Description (DID) for the Key and Certificate Management Plan. This KCMP document provides a description of the cryptographic application functionality, background, and secure communication requirements; includes the key management products and services requirements; concludes with a description of the requirements for key management products and services ordering, handling and distribution.

1.2 Referenced Documents

The documents in the following subsections are applicable to this KCMP.

1.2.1 Government Documents

- DI-MISC-81688A, Key and Certificate Management Plan (KCMP)
- TSRD ##-YY, Rev #.#, Month DD, YYYY for the Name of Product
- CDRL/ADRL ##-YY, Rev #.#, Month DD, YYYY for the Name of Product
- NSA IASRD for the Name of Product, Month DD, YYYY, Rev #.#, IASRD ##-YY
- Key Specification, etc. as appropriate

1.2.2 Non-Government Documents

- Etc. as appropriate

2. ABBREVIATIONS AND ACRONYMS

Table 1 lists and describes abbreviations and acronyms used in this document.

Table 1. Abbreviations and Acronyms

Abbreviation/ Acronym	Description
ADRL	Agreement Data Requirements List
CDRL	Contract Data Requirements List
DID	Data Item Description
ECU	End Cryptographic Unit
EKMS	Electronic Key Management System
IACM	Information Assurance Certification Manager
IASRD	Information Assurance Security Requirements Document
ITAR	International Traffic in Arms Regulation
KMI	Key Management Infrastructure
KCMP	Key and Certificate Management Plan (aka "KCMP")
LMD/KP	Local Management Device/Key Processor
MGC/AKP	Client Management/Advanced Key Processor
MOA	Memorandum of Agreement
N/A	Not Applicable
NSA	National Security Agency
POC	Point of Contact
TSRD	Telecommunications Security Requirements Document
UPA	User Partnership Agreement
Xxx	xxx
Xxx	xxx
Xxx	xxx
Xxx	xxx
Xxx	xxx

3. KEY AND CERTIFICATE MANAGEMENT PLAN PROCESS

3.1 Cryptographic Application Description and Security Services

3.1.1 Description/Purpose of Cryptographic Application

Provide a brief description of the purpose of the cryptographic application.

3.1.2 Level of Information the Cryptographic Application is Protecting

Describe all classification levels of information that the cryptographic application will be protecting.

3.1.3 Security Services the Cryptographic Application Provides

3.1.3.1 Confidentiality

Describe any requirements for confidentiality. If there are no requirements, state so.

3.1.3.2 Integrity

Describe any requirements for integrity. If there are no requirements, state so.

3.1.3.3 Non-repudiation

Describe any requirements for non-repudiation. If there are no requirements, state so.

3.1.3.4 Access Control

Describe any requirements for access control. If there are no requirements, state so.

3.1.3.5 Identification and Authentication

Describe any requirements for identification or authentication. If there are no requirements, state so.

3.1.3.6 Availability

Describe any requirements for availability. If there are no requirements, state so.

3.1.4 Operational Environment

Briefly describe the operational environment that the cryptographic application will be operated in. Examples of operational environments could be a field deployed tactical environment, a CONUS strategic SCIF environment, etc. Where will the device be used? Ships, the dessert, tactical, strategic, manpack, Humvee, SOC, controlled environments, etc.

3.1.5 Requirement for Allied/Coalition Interoperability

Describe any allied interoperability requirements. If there are interoperability requirements, discuss the overall allied interoperability strategy, particularly from a key distribution perspective. If there are none, state so and state why.

3.2 Key Management Products and Services Requirements

Table 2. Key Management Products and Services Requirements		
Paragraph	**Product/Service**	**Notes**
3.2.1 Key Management Products and Service Types	Example: Test Keys, Operational Keys, Contingency Keys, Certificates, Tokens	
3.2.2 Quantity/ECU to be Keyed	Example: # of keys per Key Type per ECU	
3.2.3 Projected Quantity of ECUs	Example: 1 EDM, 1 Qualification Unit, ~15 Production Units per year	
3.2.4 Algorithms	Example: Algorithm used with each type of product/service required. Specify which algorithm for which security service.	
3.2.5 Key Specification	Example: Identify the Key Specification for any keying product require.	
3.2.6 Protective Techniques	Example: Benign Fill, Black Key Fill, OTNK. If Red key is used, specify why. An IAD MD-110 waiver will be required.	
3.2.7 Key Period	Example: Crypto Period and Supersession Rate	
3.2.8 Classification	Example: UNCLASSIED Test Key, UNCLASSIFIED and SECRET Operational Key	
3.2.9 PKI Certificate Classes	Example: Medium S/W, Medium H/W	
3.2.10 Tokens	Example: Smart Card, USB Token, etc.	
3.2.11 Need Dates	Developmental – MM/YYYY (validated on MM/DD/YYYY)	
	Test – MM/YYYY	
	Maintenance – MM/YYYY	
	Operational – MM/YYYY	
	Contingency – MM/YYYY	
3.2.12 Controlling Authority	Example: NSA I22212 (COMSEC ID#880691)	

3.3 Key Management Products and Services Ordering

Provide enough detail to permit determination of long-term support for key orders. Who can order key? Will it always be the CONAUTH or which user can order? Authorized ID? Generation order? Distribution order?

3.4 Key Management Products and Services Generation

Describe where the key management products and services will be generated. Do you require Central Facility generation (i.e. NSA) or local generation (LMD KP/MGC AKP/Commercial Key Generation)?

3.5 Key Management Products and Services Distribution

Describe the distribution of key management products and services from the generation source until consumption by the cryptographic application. The distribution plan will include:

- When and where key management products and services are encrypted and unencrypted?
- Key Management Products form (electronic, PROM, floppy, CD, etc.) NOTE:

A requirement for key on physical media will require strong written justification, Consideration of such a request may significantly delay KCMP approval and consequently NSA certification/approval.

3.6 Future Upgrade Capabilities?

If you are relying upon legacy key management, such as physical key distribution, describe any future upgrade capabilities. If not applicable, i.e., you are already intending to use EKMS/KMI and have no upgrade requirements, then states so.

END OF DI-MISC-81688A