DATA ITEM DESCRIPTION

Title: Key Management Plan (KMP)

Number: DI-MISC-81688
AMSC Number: 7603
DTIC Applicable: No
Office of Primary Responsibility: NS/I562
Applicable Forms: N/A

Approval Date: 14 AUG 2006
Limitation: N/A
GIDEP Applicable: No

Use/relationship. The Key Management Plan (KMP) 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 KMP 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.

This Data Item Description (DID) contains the format and content preparation instructions for the data product generated by the specific and discrete task requirement as delineated in the contract, as the Key Management Plan (KMP). A Guide to Acquiring Key and Signatures, dated 23 August 2004, provides information for submitting a new Key Specification.

Requirements:

1. References documents. None

2. Format. The KMP will have appropriate classification markings in accordance with service or agency-specific policies. The KMP will not contain proprietary information unless the vendor has developed the cryptographic application for which the KMP is written under a Commercial COMSEC Endorsement Program (CCEP).

The KMP will contain:

2.1. Title Page to include:

2.1.1. Program Name;

2.1.2. Program Manager's Name and Telephone Number;

2.1.1. NSA PMO;

2.1.2. and OPR-assigned KMP number.

2.2. Revision Page;

2.3. List of Reference Documents;

2.4. Table of Contents;

2.5. KMP Body Content and;

2.6. Definition of abbreviations and acronyms.

3. Content. This section outlines the specific information required for completing the KMP1, KMP2 and KMP3. Not all requested information is applicable to all cryptographic applications. Be complete and be concise.

Definitions. *Cryptographic engine* - a device that performs cryptographic functionality; it may be implemented in either a chip or module.
End Cryptographic Unit - the lowest level hardware unit containing cryptographic functionality that must be serviced by the KMI; it is the host assembly that embeds a cryptographic engine.
System - two or more cryptographic applications integrated into an architecture to provide a specific set of security services.

General instructions. Although the KMP process may be tailored to fit a cryptographic application, the standard KMP described in this document uses an incremental three-step process. This will allow early insight into the development of a cryptographic application and its key management requirements to assess compatibility with the current and planned KMI.

The three-step process includes:

1. *KMP 1, Cryptographic Application Description and Security Services* (delivered during the preliminary design phase);
2. *KMP 2, Key Management Products and Services Requirements* (delivered during the preliminary design phase);
3. *KMP 3, Total Key Management Plan* (delivered during the critical design phase).

KMP1, the Cryptographic Application Description and Security Services document provides a description of the cryptographic application functionality, background, and secure communication requirements. The following sections are required for KMP1:

3.1.1. Cryptographic Application Description and Background

3.1.1.1. Purpose of cryptographic application

3.1.1.2. New application, modification to application or existing application

3.1.1.3. Background information

3.1.1.3.1. Who initiated the cryptographic application?

3.1.1.3.2. Why was it initiated?

3.1.1.3.3. What are future upgrade capabilities (if applicable)?

3.1.1.4. Level of information (Type 0, Type 1, and Type 2) the cryptographic application is protecting

3.1.1.5. Brief description of security services (confidentiality, integrity, non-repudiation, access control, identification and authentication, and availability) the cryptographic application provides

3.1.1.6. Information concerning long-term and potential interim key management support (operational, test, contingency, maintenance key management products and services) for the cryptographic application

3.1.2. Communications Environment (include allied interoperability requirements)

3.1.2.1. Brief description of communications environment (Both secured and unsecured)

Examples: Data Network (internet, NIPRNet, SIPRNet),
Wired communication (telephone),
Wireless communication (satellite, radio frequency)

3.1.2.2. Requirement for allied interoperability?

3.1.2.2.1. Yes - Discuss overall strategy

3.1.2.2.2. No – Explain

KMP2, the Key Management Products and Services Requirements document, includes the key management products and services requirements and the revised KMP1 submission reflecting formal comments and recommendations received during the KMP1 review process. The following section is required for KMP2:

3.1.3. Key Management Products and Services Requirements *(Provide in tabular format)*

3.1.3.1. Key management products and services types

Examples: Keys
Certificates
Tokens for each of Type 0, 1 and/or 2
Operational, Test, Contingency, Maintenance

3.1.3.2. Key management products and services quantity per ECU to be keyed

3.1.3.3. Projected quantity of End Cryptographic Units (ECUs)

3.1.3.4. Key management products and services algorithm(s)

3.1.3.5. Key management products and services format

Either reference existing Key Specification or

Submit new Key Specification in accordance with A Guide to Acquiring Key and Signatures. A copy of this document is available from: NSA, 9800 Savage Road, Suite 6568, Ft. Meade, Md. 20755-6568

3.1.3.6. Description of cryptographic application's use of benign fill

If benign fill techniques are not being used, a waiver/exemption must be submitted with an acceptable justification in accordance with IAD Management Directive 10.

3.1.3.7. Crypto periods

3.1.3.8. Key management products and services classification levels

3.1.3.9. PKI certificate classes (class 3, 4, 5)

3.1.3.10. Tokens

3.1.3.11. Need dates

3.1.3.11.1. Operational

3.1.3.11.2. Test

3.1.3.11.3. Contingency

3.1.3.11.4. Maintenance

3.1.3.11.5. Project duration of need

3.1.3.12. Anticipated Controlling Authority

KMP3, the Total Key Management Plan, includes the key management products and services ordering, handling and distribution descriptions and folds in KMP1 and KMP2 and the associated comments and recommendations received during the KMP2 review process. The following sections are required for KMP3:

3.1.4. Key Management Products and Services Ordering – Describe ordering via KMI. Provide enough detail to permit determination of long-term support by the KMI.

3.1.5. Key Management Products and Services Generation – Describe key management products and services generated for and used by the cryptographic application. If none, identify the source that provides key management products and services used by the cryptographic application.

3.1.6. Key Management Products and Services Distribution – Describe the distribution and translation of key management products and services within the cryptographic application. The distribution plan will include:

3.1.6.1. When and where key management products and services are encrypted and unencrypted.

3.1.6.2. Their physical form (electronic, PROM, floppy, CD, paper, etc.).

3.1.6.3. How they are identified during distribution.

3.1.7. Key Management Products and Services Storage – Describes how the key management products and services for the cryptographic application are stored, to include:

3.1.7.1. Identifying during storage (EKMS 308 key tag, Distinguished Name).

3.1.7.2. Storage capacity.

3.1.8. Access Control – Describes how access to the cryptographic application is:

3.1.8.1. Authorized

3.1.8.2. Controlled

3.1.8.3. Validated to;

3.1.8.3.1. Request

3.1.8.3.2. Generate

3.1.8.3.3. Handle

3.1.8.3.4. Distribute

3.1.8.3.5. Store

3.1.8.3.6. Use key management products and services.

3.1.9. Accounting – Describe accounting of key management products and services used by the cryptographic application.

3.1.9.1. Detail the use of event logs to support the tracking of key management products and services.

3.1.9.1.1. Generation

3.1.9.1.2. Distribution

3.1.9.1.3. Storage

3.1.9.1.4. Use

3.1.9.1.5. Destruction

3.1.9.2. Describe the use of appropriate privileging to support the control of key management products and services used by the cryptographic application

3.1.9.3. Describe the directory capabilities used to support PKI cryptographic applications, if applicable

3.1.9.4. Identify where human and automated tracking actions are performed

3.1.9.5. Identify where two-person integrity is required, if applicable

3.1.10. Compromise Management and Recovery – Describes how secure communications can be restored in the event of the compromising of key management products and services used by the cryptographic application.

3.1.10.1. The recovery process description must include methods of re-key or replacement.

3.1.10.2. For PKI cryptographic applications, detail the implementation of:

3.1.10.2.1. Certificate Revocation Lists (CRLs)

3.1.10.2.2. Compromised Key Lists (CKLs)

3.1.10.2.3. Indirect Certificate Revocation Lists (ICRLs)

3.1.10.2.4. A description of how certificates will be reissued and renewed within the cryptographic application must be included.

3.1.11. Key Recovery (required for cryptographic applications that provide a key recovery capability) – Describes how previously unavailable confidentiality key can be recovered. The process description must include a discussion of the

3.1.11.1. generation

3.1.11.2. storage, and

3.1.11.3. access for the long-term storage key.

3.2.9.4 The process of transitioning from the current to future long-term storage key must be included.

4. Appendix A (optional). Use of standard key management products and services provided by the KMI is highly encouraged. However, a cryptographic application will identify requirements that are currently not supported by the KMI. This appendix, if applicable, addresses where improvements to the KMI are required in order to achieve the needed cryptographic application functionality. This will assist in identifying requirements for current or planned capability increments of the KMI. Even if a cryptographic application can be fully supported by the current or planned KMI, improvements to the KMI shall also be identified if they improve functionality of the cryptographic application, reduce user workload, or improve/reduce KMI functionality. Requirements identified in this appendix will be analyzed for potential upgrades to the KMI, based on available cost, schedule and performance constraints.

The following key management-related information for cryptographic engine developments is needed to determine and resolve potential impacts to the Key Management Infrastructure in a time frame that meets user requirements. Please provide yes/no responses to the following questions as well as additional information for each "yes" response.

4.1.1. Are unique key management products and services required by the cryptographic engine for proper operation? Are the unique key management products and services approved by the Cryptographic Products and Support Center?

4.1.2. Are there any cryptographic capabilities to be supported by the KMI that are fully programmable in the cryptographic engine?

4.1.3. Does the cryptographic engine implement standard IAD software download capability for importing updated cryptographic functions?

4.1.4. Does the cryptographic engine use any non-key material KMI products or services (such as CKL/CRLs, PAC/dePAC, seed key conversion, etc.)?

4.1.5. Does the cryptographic engine implement or have the capability to implement benign techniques?

4.1.6. Does the cryptographic engine design preclude use of any Cryptographic Algorithm Configuration Management Board (CACMB) approved cryptographic algorithm?

4.1.7. Does the cryptographic engine design preclude allied releasability?

5. END OF DI-MISC-81688.