DATA ITEM DESCRIPTION

Title: Key Specification (KS)

Number: DI-TMSS-82312
AMSC Number: 10135
DTIC Applicable: No
Preparing Activity: NS
Applicable Forms: None

Approval Date: 20191218
Limitation: N/A
GIDEP Applicable: No
Project Number: TMSS-2020-003

Use/Relationship: The Key Specification (KS) describes the ordering, generation, distribution, and validation of the key material.

a. Key Generation: The KS should designate and describe all types, uses and formats of key required by the application. The KS should also describe the data format, encryption algorithms, parity, checkword algorithms, data constraints, and relationships of one cryptographic application key to another.
b. Key Distribution/Consumption: The KS should describe the type of key and Meta data or fill object the equipment/system will consume. The KS should tailor the mission key and supporting delivery data standards selected from the electronic key delivery references (Electronic Key Management System (EKMS) and Key Management Infrastructure (KMI)) for consumption by the equipment/system based on the Key and Certification Management Plan (KCMP). Note: Over-the-Network Keying is the recommended solution to ensure mission key confidentiality and integrity through distribution and use to ultimate destruction.
c. Key Validation: The KS should contain the results of associated tests to verify that the cryptographic key validation material received agree with the cryptographic key requirements stipulated in the KCMP and KS for the equipment/system. It details the test requirements, describes the tests performed and provides the associated test results and analysis. It is used by the Government to indicate format, function and compatibility acceptance of the cryptographic key software, developed from KS submittal, and resulting key material for use in the equipment/system.
d. This Data Item Description (DID) contains format and content preparation instructions for the data product generated by the specific and discrete task requirement as delineated in the legal agreement, as the KS.
e. This DID is applicable to systems and equipment requiring cryptographic key material.
f. This DID is related to the Tailored Security Design and Analysis Requirements Specification.
g. This DID supersedes prior reference to DI-MISC-80508B titled Technical Report-Study/Services.

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 legal agreement.
   1.1. National Security Agency/Central Security Service (NSA/CSS) Policy Manual 1-52
   1.2. Technical Security Requirements List (TSRD) for User Partnership Program (UPP), Commercial Communications Security Evaluation Program (CCEP), and Waveforms, Section 2.9
   1.3. Committee on National Security Systems (CNSS) Policy 30, Cryptographic Key Protection

1.4. KCMP Data Item Description, DI-MISC-81688A
1.5. KS Template, Version 1.0
1.6. KS Validation Report Appendix Template, Version 1.0
1.7. EKMS 300-399, Key Management Standards
1.8. EKMS 600-699, Interface Specifications
1.9. KMI 3000-3999, Technical Standards
1.10. CNSS Instruction (CNSSI) No. 4001, “Controlled Cryptographic Items (CCI)”
1.11. CNSSI No. 4031, “Cryptographic High Value Products (CHVP)”
1.12. CNSSI No. 4003, “Reporting and Evaluating COMSEC Incidents”

2. Format. The KS and KS Validation Report Appendix shall:
   2.1. Be formatted strictly in accordance with the KS and KS Validation Report Appendix Templates established for this purpose and referenced in paragraph 1.5 and 1.6 respectively 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 Cybersecurity Certification Manager’s (CSCM’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 KS, approved KCMP, and any supporting test validation documentation.
   2.8. Include a Table of Contents.
   2.9. Include a Table defining all abbreviations and acronyms.
   2.10. Total page count for the KS should not exceed 30 pages, with font size and type 12 Times New Roman. NSA reserves the right to return KSs numbering 30 or more pages with instructions to make them more concise and readable.

3. Contents. The KS and KS Validation Report Appendix shall:
   3.1. Be completed using the KS Template, Version 1.0 and the KS Validation Report Appendix Template Version 1.0, included in this DID. NOTE: Not all requested information will apply.

4. The Key Specification Template, Version 1.0, and Key Validation Report Appendix Template, Version 1.0, follow on the next page.

Key Specification Template, Version 1.0

Key Specification

For

Program Name

UPA/MOA Number: XXX
Contract Number: XXX
CDRL/ADRL: XXX
Project Classification: XXX
Submittal Date: XXX
Document ID: XXX
Document Revision: XXX
NSA Data Item: XXX
NSA CSCM: 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.)

Vendor Name: XXX
Vendor Address: XXX

Document Developer Company Name: XXX
Document Developer Company Address: XXX
Document Developer Company PM Name: XXX
Document Developer Company PM Phone XXX

Approvals (If applicable)

Revision History

Principal changes incorporated into each revision of this document are listed in the following table. Specific document section numbers refer to the preceding revision of the document (the revision of the document before the indicated change was incorporated), except for the newly added sections.

Version Change Table				
Revision	Document Section	Change Description	Approver Name	Date
0.1	N/A	Initial version.		

Table of Contents

1. Introduction

1.1 Purpose and Scope

Provide a description of the program and the cryptographic implementation that the product is providing. How keys will be distributed and any reference to a standard or equipment and where the keys will be generated (Tier 0, Tier 1 or 2)

1.2 Referenced Documents

Documents that are applicable to this Key Specification.

1.2.1 Government Documents

Provide a list of government documents applicable to this Key Specification.

1.2.2 Non-Government Documents

Provide a list of non-government documents applicable to this Key Specification.

2. Abbreviations/Acronyms

Described abbreviations and acronyms used in table form.

3. Key Types

Provide a list of the various key types in table form with a brief description, include figures if necessary. Clearly specify relationships between keys and parent/child relationships for any black key, include figures/diagrams if necessary. If no relationships exist, specify.

Sample charts:

Key	Used for	Security Algorithm	Key Specification	Generated by

4. Key Generation

Provide key specifics to include source of creation/generation. When applicable, include parity, check word or checksum generation.

4.1 Key Format

Provide the format, structure, and syntax of the key types and subfields. When applicable, include short titles schemes and algorithm specifications that apply.

4.1.1 Key Format Example

Provide examples of the key for further clarification.

4.2 Key Parity

Provide key parity, check word or checksum generation description, if applicable.

4.2.1 Key Parity Example

Provide examples of the key and parity for further clarification.

5. Key Tagging

Specify tagging requirements required beyond the standard tagging provided at Tier 1 and Tier 2. Include table, if necessary. If no additional inner tagging is required, specify.

Sample table:

DS-100-1 Attribute	**Value**
Short title	
Ownership	
Format Type	
Text Indicator	
Edition	
Caveat	
Register Number	
Segment Number	
Use	
Classification	
Use Expansion Subfield	
Classification Expansion Subfield	
Parity	
Data	
Optional text Field	

5.1.1 Key Tag Field Descriptions

Specify field descriptions and their associated values

Sample table:

Order	Field Name	Bit Length	Bit Position	Value

6. Key Production Requirements

6.1 Key Production

Specify production information.

6.1.1 Production Constraints

Specify any production constraints between keys. If none, specify that no production constraints exist.

6.1.2 Uniqueness Constraints

Specify any uniqueness constraints between keys (e.g. within an edition, between editions of the key, etc...). If none, specify that no uniqueness constraints exist.

6.2 Key Nomenclature

Identify means to perform accounting and key material control. Provide a list of associated short titles.

Sample table:

Key	Scope of Key	Platform types	Total Short titles

Pre-defined Short Titles			
Short Title	Classification	Additional Description	Equipment Type

6.3 Key Material Attributes

Specify allowable combinations of key material attributes.

Sample table:

Allowable Combinations of Key Material Attributes					
Usage	Purpose	SEGMENTS per EDITION	CRYPTO-PERIOD per SEGMENT	Caveat	Release

7. Distribution

Provide distribution information.

Sample table:

Key Usage Description	Key type	Short title	Media (EKMS, KMI)	Crypto Period	Classification and caveat
Keymat (US, Test or Operational)					
Keymat (US, Test or Operational)					

Key Validation Report Appendix

For

Program Name

Table of Contents

A.1 Introduction

This appendix contains the results of tests to verify that the cryptographic key validation material received agree with the cryptographic key requirements stipulated in the Key and Certification Management Plan (KCMP) and Key Specification (KS) for the equipment/system. It details the test requirements, describes the tests performed and provides the associated test results and analysis. It is used by the Government to indicate format, function and compatibility acceptance of the cryptographic key software, developed from KS submittal, and resulting key material for use in the equipment/system.

A.2 Abbreviations/Acronyms

Described abbreviations and acronyms used in table form.

NOTE: Section A.3 shall be repeated, in its entirety, for each cryptographic key tested.

A.3 Enter Cryptographic Key Name Key Validation

Date(s) on which validation was performed.

Cryptographic key(s) tested, including the short title and edition.

A.3.1 Key Validation Requirements

This section shall include the following, relating each to the prescribing contract requirement paragraph (key/certificate specification, standard, management plan, or work statement)

A.3.1.1 Test Requirements

Required tests and parameters to be measured for the cryptographic key.

A.3.1.2 Format Requirements

Format requirements, such as the key needs to be formatted in accordance with a specific specification or standard, the key needs to contain specific calculations (e.g. cyclic redundancy checks, parity, etc…) in accordance with a specific specification or standard, or the key needs to contain specific header or tagging information in accordance with a specific specification or standard.

A.3.1.3 Functionality Requirements

Functionality requirements, such as the key needs to load into the equipment/system successfully, or the key needs to enable the equipment/system to perform follow-on functions successfully.

A.3.1.4 Interoperability or Compatibility Requirements

Interoperability or compatibility requirements, such as the equipment/system needs to interoperate with another required equipment/system using either the same key or different key.

A.3.2 Key Validation Test Procedures

This section shall include an outline of the procedures and/or sequence of steps performed during the testing to satisfy the test requirements specified. If these procedures are contained in a previously delivered document, reference that document in lieu of repeating its contents.

A.3.3 Key Validation Test Results and Analysis

This section shall include the results of executing the test procedures specified, to include any follow-on analysis performed. If these test results and analysis are contained in a previously delivered document, reference that document in lieu of repeating its contents.

A.4 Validation References

The references shall include identification of the following, as applicable:

- Prior test reports on the same item.
- Test plan and procedure documents.
- Requirement specification and standards.

A.5 Validation Conclusions

The conclusions shall include statements addressing the following (distinguish between opinion and subjective):

- Effectiveness of the cryptographic key validation testing.
- Success or failure of the cryptographic key in meeting the test requirements.
- The need for repeat, additional, or alternative testing.
- The need for cryptographic key re-design or further development.

A.6 Validation Recommendations

The recommendations shall refer to the appropriate key validation test results and conclusions drawn. These could address such actions as:

- Acceptability of the cryptographic key validation.
- Additional testing required.
- Redesign required.
- Problem resolution.

A.7 Validation Signatory

The signatory shall include a physical or digital signature from an individual of power and authority in the Government Sponsor Program office indicating their endorsement of the report contents.

END OF DI-TMSS-82312