Next Generation Load Device – Medium (NGLD-M)

Date:

Prepared by:

Product Lead COMSEC
Project Lead, Network Enabler
Aberdeen Proving Ground, MD 21005

DISTRIBUTION STATEMENT X:
Distribution authorized to U.S. Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with regulations implementing 10 U.S.C. 140c. Other requests must be referred to SFAE-CCC-MC.

Authenticated by:

First Name MI. Last Name
Chief or Lead Engineer
Day Month Year
(Ex: 01 May 2019)

Approved by:

First Name MI. Last Name
Program Manager
Day Month Year
(Ex: 01 May 2019)

CHANGE HISTORY

Change	Version	Date
Initial - RFI	**1.0**	**01/10/2019**
Draft RFP	**2.0**	**05/20/2019**
Draft RFP - Final	3.0	05/29/2019

Contents

(U) TABLE OF FIGURES

(U) TABLE OF TABLES

1. (U) SCOPE

(U//FOUO) This System Requirements Document (SRD) establishes the functional, performance, and verification requirements for the Next Generation Load Device (NGLD)-Medium (NGLD-M). The SRD identifies requirements to develop the NGLD-M and its interfaces. The document expands upon the requirements providing helpful detail on how the NGLD-M is expected to operate given the defined context of functional operations. The requirements in this document are based on the Capability Production Document (CPD) for NGLD-M Version (v) 1.05, dated 22 April 2013.

1.1 (U) System Identification

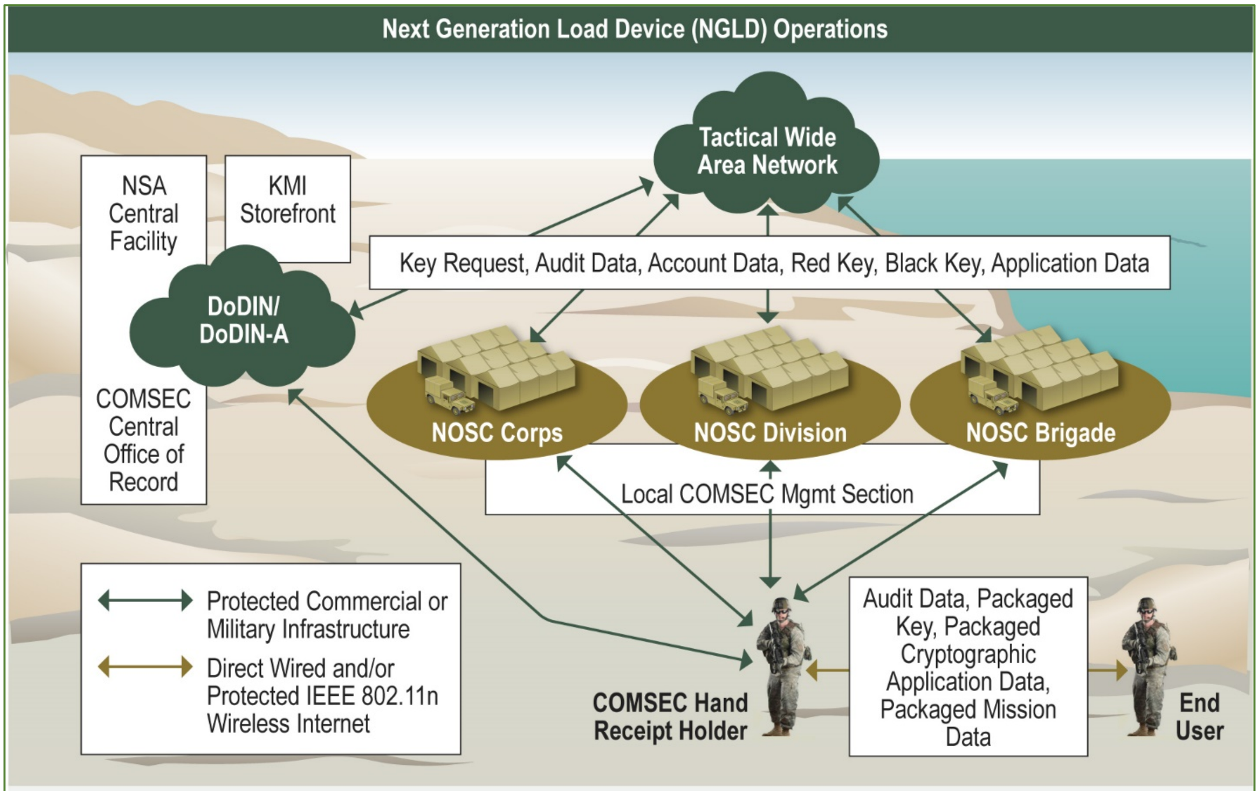
(U//FOUO) The Army NGLD consists of a family of devices intended to be eventually fielded in several platform designs (small, medium, and large) to support capabilities ranging from single key fill to loading extensive mission data and configuration files. This SRD applies to the NGLD-M device, *the medium device*. The NGLD-M primary objective is to operate as a National Security Agency (NSA)-certified cryptographic key load device with both High Assurance (HA) and Medium Assurance (MA) capabilities. This capability replaces the current key load device, the Simple Key Loader (SKL), meets the cryptographic modernization initiatives issued by NSA, and extends cryptographic product distribution through the NSA's Key Management Infrastructure (KMI).

1.2 (U) System Overview

(U//FOUO) The NGLD-M is part of the United States (US) Army's future family of systems for improved cryptographic product distribution to End Cryptographic Units (ECUs) including, but not limited to tactical radios, network encryption devices, and link encryptors. As a replacement for the SKL, the NGLD-M will also be used by Department of Defense (DoD) services and Civil Agencies.

(U//FOUO) The NGLD-M makes use of modernized loading capabilities delivered with KMI and associated Over-the-Network-Keying (OTNK) mechanisms using an embedded cryptographic design incorporating approved NSA high assurance and medium assurance algorithms. The NGLD-M receives, manages, and distributes cryptographic products and network configuration files over the external interfaces depicted in figure 7, has a modern Operating System (OS) with required security enhancements, and contains a User Application Software (UAS) providing navigation optimized for finger press support. The NGLD-M interoperates with both legacy devices and modern KMI-Aware equipment. NGLD-M can be operated via a medium assurance mode without an enabled high assurance cryptographic module; thus relying on NSA information assurance, cryptographic protections, and defense in depth strategies to maintain a robust security posture, limiting high assurance operations to only those times where it is needed most. To enable the NGLD-M for high assurance operations a high assurance cryptographic ignition key (CIK) is used to fully activate the NGLD-M system and complete sensitive operations that require high assurance algorithm use.

(U//FOUO) The NGLD-M will initially augment the current Army fill device inventory and eventually become the replacement item for early version of the Army SKL v1 and v2 and Data Transfer Devices (DTDs). The NGLD-M will leverage external interfaces to mission planning and key management sources (Automated Communications Engineering Software [ACES], Joint Enterprise Network Manager [JENM], Intermediary Application [iApp], Joint Mission Planning System [JMPS], etc.), KMI-Awareness, and legacy interfaces to obtain key and data products to load ECUs.


Next Generation Load Device (NGLD) Operations
Tactical Wide Area Network
NSA Central Facility
KMI Storefront
Key Request, Audit Data, Account Data, Red Key, Black Key, Application Data
DoDIN/ DoDIN-A
COMSEC Central Office of Record
NOSC Corps
NOSC Division
NOSC Brigade
Local COMSEC Mgmt Section
Protected Commercial or Military Infrastructure
Direct Wired and/or Protected IEEE 802.11n Wireless Internet
COMSEC Hand Receipt Holder
Audit Data, Packaged Key, Packaged Cryptographic Application Data, Packaged Mission Data
End User

Next Generation Load Devices (NGLD) are intended to operate across all tactical echelons from Corps, Divisions, and Brigade down to COMSEC Hand Receipt Holders and Cryptographic End Users at all echelons.

Local COMSEC Management Sections, typically employed with their parent Network Operations and Security Center (NOSC), utilize the physically protected Tactical Wide Area Network and the protected Global Information Grid communications infrastructure to exchange data with the NSA Central Facility and the COMSEC Central Office of Record.

Data exchanges between the Local COMSEC Management Section and the assigned COMSEC Hand Receipt Holder is typically performed using direct wired connections and/or embedded and protected IEEE 802.11n wireless internet protocols.

The COMSEC Hand Receipt Holder then provides accounting and distribution operations to ensure the Cryptographic End User has the proper Packaged Cryptographic Application Data, Packaged Key, and Packaged Mission Data needed to conduct operations.

NGLD-M-10

Figure 1- (U) High-Level Operational Concept Diagram (OV-1) – Next Generation Load Device

1.3 (U) Document Overview

(U) The contents within this SRD are organized according to the following sections:

1. (U) Section 1 – Scope: Defines the general NGLD-M SRD content.
2. (U) Section 2 – Applicable Documents: Lists referenced documents applicable to the NGLD-M system requirements.
3. (U) Section 3 – System Requirements: Requirements detailed by system function, derived from the CPD.

4. (U) Section 4 – Verification Provisions: Outlines the methods of verification applicable to the NGLD-M system requirements.
5. (U) Section 5 – Requirements Traceability: Documented NGLD-M requirements to unique identifier, SRD section, qualification method, and tagged as Threshold (required) or Objective (desired).
6. (U) Section 6 – Notes: Lists definitions and acronyms used in the SRD.
7. (U) Section 7 – Appendices: Provided as necessary to convey amplifying information and enhance overall SRD readability.

2. (U) APPLICABLE DOCUMENTS

(U) The following table lists the documents applicable to NGLD-M and those documents referenced in this SRD.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Version Number	Title
ANSI X9.31	Cryptographic Token Interface Standard, RFC 3566
ANSI X9.42-2003	Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, R2013
ANSI X9.62:2005	Public Key Cryptography for the Financial Services Industry: ECDSA
CPD	Capability Production Document For Next Generation Load Devices Family (NGLD) v 1.05, dated 22 April 2013
EKMS 217	EKMS Benign Techniques Specification, dated 21 December 2001
EKMS 308	Data Tagging and Delivery Standard, EKMS 308 (0N481180), National Security Agency, Revision C, dated 25 October 2000 and Revision F dated 16 April 2008
EKMS 322B	EKMS Firefly Specification Revision A, National Security Agency, Information Assurance Directorate, dated 5 April 2002
EKMS 603B	AN/CYZ-10(V)3 Data Transfer Device Interface Specification, Document Number 0N477312, Revision B, dated 28 October 1998 and C
FIPS-140-2	Security Requirements for Cryptographic Modules, dated December 3, 2002, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=902003,
FIPS 180-4	Secure Hash Standard (SHS), dated 5 Aug 2015
FIPS 197	ADVANCED ENCRYPTION STANDARD (AES), dated 26 November 2001
FIPS 186-4	Digital Signature Standard (DSS) dated July 2013, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
IASRD	NSA Tailored Information Assurance Security Requirements Document (IASRD)
ITU RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, dated May 2008

Version Number	Title
IETF Standard 62	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, dated Dec 2002
IETF Standard 78	Simple Network Management Protocol (SNMP) Context Engine ID Discovery, dated Sept 2008, https://tools.ietf.org/html/std78
KMTG-0003-003	Software Signature (S2) Implementation Guide
KM-TG-0002-96	The Standard for Signing and Obtaining a Hash word for a Software Package to Support INFOSEC Applications, Rev 9, dated 24 April 1997
KMI-3300	Over-the-Network-Keying (OTNK) Specification, version 2.2, dated 29 July 2016
KMI-3001	Compact Electronic Serial Number Standard, dated 17 August 2005
KMI-3001 Annex A	Compact Electronic Serial Number Standard Annex A, dated August 2010
KMI-3240	Securing FTP with TLS, dated Oct 2005
KMI-3350	OTNK Specification v0.2, dated 30 Oct 2009
KM-TG-0001-87 Rev 4 Supplement	ACCORDION 1.3, dated October 30, 1987
MIL-STD-810G	Department of Defense Test Method Standard: Environmental Engineering Considerations and Laboratory Tests, dated31 Oct 2008
MIL-STD-461F	Department of Defense Interface Standard: Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment, dated December 10, 2007
MIL-STD-2169B	Department of Defense Interface Standard: High-altitude Electromagnetic Pulse (HEMP) Environment, dated19 Jan 2012, http://everyspec.com/MIL-STD/MIL-STD-2000-2999/MIL-STD-2169B_NOTICE-1_40674/
MIL-STD-188-114A	Military Standard: Electrical Characteristics of Digital Interface Circuits, dated30 Sep 1985, http://everyspec.com/MIL-STD/MIL-STD-0100-0299/MIL-STD-188-114A_21120/
MIL-STD-271F	Military Standard: Requirements for Nondestructive Testing Methods, dated27 Jun 1986, http://everyspec.com/MIL-STD/MIL-STD-0100-0299/MIL-STD-271F_21047/
NIST SP 800-56A Rev 3	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, dated April 2018, https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final
NSA 90-02A	Interface Specification for Thornton Smart Fill, dated 1 September 1993
NSA R21-TECH-03-02	NSA MEDLEY Implementation Standard: An ACCORDION MEDLEY, dated 7 February 2002
NSA Policy Number 3-9	Cryptographic Modernization Initiative Requirements for Type 1 Cryptographic Products
NSA R21-TECH-02-03A	MAYFLY Specification

Version Number	Title
NSA SPEC 2000-4	The ACCORDION 3.0 Algorithm – Suite A/B, dated 17 May 2003
NSA R21-TECH-13-00	ACCORDION 3.0 Specification , dated August 2000
NSA R21-TECH-34-05	WATARI algorithm, dated 20 December 2005
NSA Specification R2-TECH-35-15)	SAFEBOX-E Classification: S/REL USA,FVEY, Rev 1, dated 31 August 2015
NSA Specification R2-TECH-36-15	SAFEBOX-S Classification: S/REL USA,FVEY, Rev 1, dated 11 September 2015
NSA Specification ALDERFLY II	ALDERFLY II Classification: S/REL USA,FVEY, Rev 2, dated 25 September 2015
NSA Specification R2-TECH-42-15	SPONDULIX-E Classification: S/REL USA,FVEY, Rev 1, dated 24 November 2015
NSA R21-TECH-31-05	WATARI algorithm Implementation
NSA Doc. NAG-16F	Field Generation and Over-the-Air Distribution (OTAD) of COMSEC Key In Support of Tactical Operations and Exercises, dated May 2001, https://info.publicintelligence.net/NSA-NAG-16F.pdf
PKCS #1 v2.2 RSA Cryptography Standard	PKCS #1 v2.2 RSA Cryptography Standard, dated 27 October 2012,
N/A	The Galois/Counter Mode of Operation (GCM), dated 31 May 2005
RFC 4217	Securing FTP with TLS, dated Oct 2005, https://www.rfc-editor.org/rfc/rfc4217.txt
RFC 4634	US Secure Hash Algorithms (SHA and HMAC-SHA), dated July 2006, https://www.rfc-editor.org/rfc/rfc4634.txt
RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2, dated Aug 2008, https://www.rfc-editor.org/rfc/rfc5246.txt
RFC 5934	Trust Anchor Management Protocol, dated August 2010, http://www.rfc-base.org/txt/rfc-5934.txt
RFC 3447	Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications version 2.1, February 2003, http://www.rfc-editor.org/rfc/rfc3447.txt
RFC 2404	The Use of HMAC-SHA-1-96 within ESP and AH, dated November 1998, http://www.rfc-editor.org/rfc/pdfrfc/rfc2404.txt.pdf
RFC 3686	Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP), dated January 2004, https://www.rfc-editor.org/rfc/rfc3686.txt
RFC 2451	The ESP CBC-Mode Cipher Algorithms, dated November 1998, http://www.rfc-editor.org/rfc/rfc2451.txt
RFC: 6234	US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF, dated May 2011 http://www.rfc-editor.org/rfc/rfc6234.txt

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Version Number	Title
SF-153	COMSEC Material Report Form
SP 800-53 Rev. 4	Security and Privacy Controls for Federal Information Systems and Organizations, dated 22 January 2015
SSCSD-CT3-ICD-3.20	Interface Control Document for the Common Tier 3 (CT3), Version 3.20, dated 15 June 2004
R03C02 Revision 01 for KMI ACC	Tier 2- Tier 3 XML Black Key Distribution, dated march 2018
NIST SP 800-38F	National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, December 2012, https://csrc.nist.gov/publications/detail/sp/800-38f/final

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Table 1 – (U) Applicable Documents

3. (U) SYSTEM OR SUBSYSTEM REQUIREMENTS

(U) This section identifies the basic system requirements for the NGLD-M. Each requirement is assigned a project-unique identifier (to support testing and traceability). The requirements for the various subsections are summarized in section 0 – 5. (U) REQUIREMENTS TRACEABILITY. Here they are annotated with associated verification method(s) (reference (U) Section 4 – Verification Provisions: Outlines the methods of verification applicable to the NGLD-M system requirements.) along with a mapping to the CPD. Requirements below represent the characteristics of the NGLD-M that are conditions for system acceptance.

(U) Throughout this document we refer to the concept of a Cryptographic Ignition Key (CIK). This is not to imply a design input or constraint, but rather a concept to satisfy the security requirements of the device. In accordance with security requirements, the NGLD-M is required to incorporate a valid methodology by which the cryptographic subcomponents will be activated. The cryptographic subcomponent of NGLD-M provides appropriately privileged users with access to High Assurance and Medium Assurance cryptographic services. The NGLD-M cryptographic subcomponent are not to be operable without a valid, security approved activation implementation.

3.1 (U) Required States and Modes

(U//FOUO) The NGLD-M is required to transition into and out of several modes and states in support of operational capabilities. The high-level modes of operation of the NGLD-M are found in 0 (U) High-Level Modes and include fundamental modes of: Off, Power-Up, Authentication-Authorization-Accounting (AAA), Built-In Test and Health Status, Normal Operations: Interactive, Normal Operations: Discrete, Alarm, Zeroize, and Power-Down. The NGLD-M is required to support cross-cutting modes related to the secure operation of the system in either High Assurance mode or a Medium Assurance mode and deals with the High Assurance cryptographic sub-system of the NGLD-M. Description of these cross-cutting modes are found in sections 3.1.2 and 3.1.3. The NGLD-M can operate in a Medium Assurance mode as early as after Power-Up and lasting until the system is Off. The NGLD-M can be ignited for High Assurance mode operations after the user is authenticated and has inserted a valid Cryptographic Ignition Key (CIK) with High Assurance capability. The capabilities of the High Assurance cryptographic subsystem can then be utilized.

3.1.1 (U) High-Level Modes

(U//FOUO) Figure 2 – (U) NGLD-M High-Level Modes and Triggers provides an initial high-level view of the NGLD-M with respect to the system lifecycle, from power-up to power-down, that supports secure user activities centered on the key management mission. Within this illustration lay two critically important cross-cutting security modes: *Medium Assurance Mode* (section 3.1.2) and *High Assurance Mode* (section 3.1.3).These two security modes identify how to operate within and across the high-level modes and allow the authorized users to have the flexibility to activate and deactivate the high assurance cryptographic subsystem on-demand.

(U//FOUO) The modes depicted in Figure 2 – (U) NGLD-M High-Level Modes and Triggers are illustrated as rounded rectangles and are given abstract labels that represent user-driven and automated outcomes. The outcomes enable sets of use-case-based system capabilities to be utilized or manipulated. These modes support organizational processes and procedures and enable an authorized user to command and control NGLD-M to achieve mission objectives. Between each mode are a set of numbered triggers that are driven by the user or automated processing to exit a mode and enter another mode. The numbered triggers supplied in Figure 2 – (U) NGLD-M High-Level Modes and Triggers correspond with information provided in Table 2 – (U) High-Level Modes and Triggers.

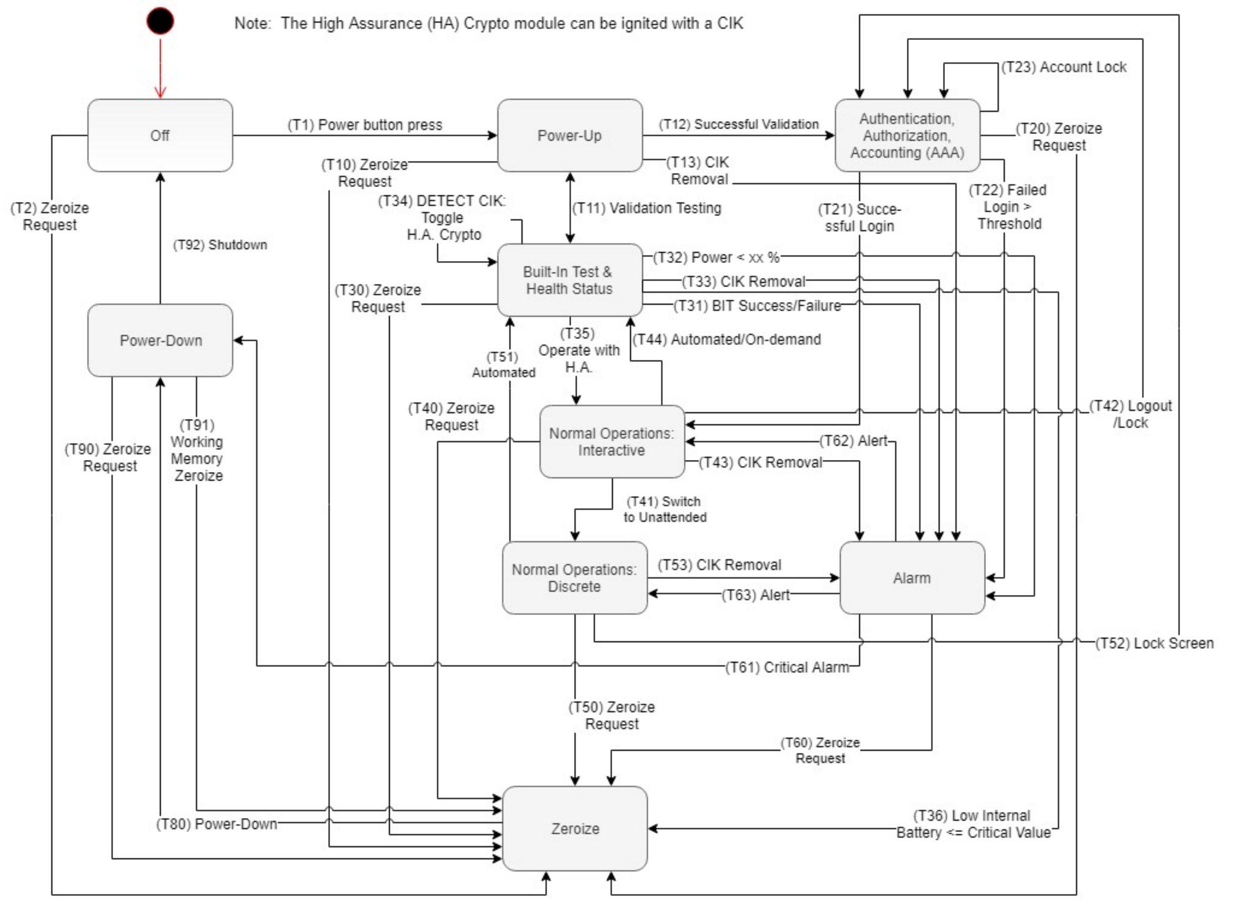
(U//FOUO) These modes are tailorable during design.

(U//FOUO) The modes shown in Figure 2- (U) NGLD-M High-Level Modes and Triggers include:

- **Off.** Off mode is the NGLD-M turned off and placed into a secured state.
- **Power-Up**. Power-up mode is characterized by the activities required to bring the system up and allow it to become ready for user login.
- **Authentication, Authorization, Accounting (AAA)**. AAA mode is characterized by the activities to control user access into the system after NGLD-M achieves power-up. The NGLD-M can power-up without the use of a CIK with High Assurance ignition material loaded into it; which results in the NGLD-M being made ready for Medium Assurance mode of operations.
- **Built-In Test & Health Status**. Built-In Test & Health Status mode is characterized by validation testing and monitoring of many subsystems. An important aspect of the NGLD-M is its ability to operate in cross-cutting modes of Medium Assurance Mode (section 0) and High Assurance Mode (section 0). NGLD-M can power-up into Medium Assurance Mode when a CIK is not yet inserted into the system. The system can be used for Medium Assurance operations while the High Assurance cryptographic module lay dormant and not ignited. The NGLD-M monitors for the presence of valid CIK and authorized user before being allowed to toggle the High Assurance cryptographic module on and enter High Assurance mode.

- **Normal Operations: Interactive**. Normal Operations: Interactive mode is characterized by the activities that a user can perform or initiate while operating the device (e.g., interacting with the NGLD-M through physical and logical external interfaces to accomplish mission goals). The majority of work done in interactive mode involves receiving, managing, and distribution key and key related materials.
- **Normal Operations: Discrete**. Normal Operations: Discrete mode is characterized by the system being locked to user interaction and is able to perform a limited set of network-centric operations that are expected to take longer periods of time to complete; such as data download and software/firmware updates and serve as a PDE storefront or Last-Mile API (LMA). This mode addresses the capabilities that need to be executed without direct user intervention when a device is connected to a network.
- **Alarm**. Alarm mode is characterized by the handling of conditions that require direct notification and action by the system or user.
- **Zeroize** mode is characterized by the direct and secure deletion of data contained within NGLD-M when specific conditions exist.
- **Power-Down**. Power-Down mode is characterized by the activities required to bring the system down in a stable manner and place it into an Off mode.

(U//FOUO)



(U//FOUO)

Figure 2- (U) NGLD-M High-Level Modes and Triggers

UNCLASSIFIED / FOR OFFICIAL USE ONLY

Current Mode	Triggering Event Number	Triggering Event Condition	Next Mode
Off	T1	Power button press	Power-Up
Off	T2	Zeroize Request (button press)	Zeroize
Power-Up	T10	Zeroize Request (button press)	Zeroize
Power-Up	T11	Validation Testing	Built-In Test & Health Status
Power-Up	T12	Successful Validation	Authentication, Authorization, Accounting (AAA)
Power-Up	T13	CIK Removal	Alarm
Authentication, Authorization, Accounting (AAA)	T20	Zeroize Request (button press)	Zeroize

Current Mode	Triggering Event Number	Triggering Event Condition	Next Mode
Authentication, Authorization, Accounting (AAA)	T21	Successful Login	Normal Operations: Interactive
Authentication, Authorization, Accounting (AAA)	T22	Failed Login > Threshold	Alarm
Authentication, Authorization, Accounting (AAA)	T23	Account Lock	Authentication, Authorization, Accounting (AAA)
Built-In Test & Health Status	T30	Zeroize Request (button press)	Zeroize
Built-In Test & Health Status	T31	BIT Success/Failure	Alarm
Built-In Test & Health Status	T32	Power < xx %	Alarm
Built-In Test & Health Status	T33	CIK Removal	Alarm
Built-In Test & Health Status	T34	DETECT CIK: Toggle H.A. Crypto	Built-In Test & Health Status
Built-In Test & Health Status	T35	Operate H.A.	Normal Operations: Interactive
Built-In Test & Health Status	T36	Low Internal Battery <= Critical Value	Zeroize
Normal Operations: Interactive	T40	Zeroize Request (button press [physical or logical])	Zeroize
Normal Operations: Interactive	T41	Switch to Discrete	Normal Operations: Discrete
Normal Operations: Interactive	T42	Logout/Lock	Authentication, Authorization, Accounting (AAA)
Normal Operations: Interactive	T43	CIK Removal	Alarm
Normal Operations: Interactive	T44	Automated/On-Demand	Built-In Test & Health Status
Normal Operations: Discrete	T50	Zeroize Request (button press)	Zeroize
Normal Operations: Discrete	T51	Automated	Built-In Test & Health Status
Normal Operations: Discrete	T52	Lock Screen	Authentication, Authorization, Accounting (AAA)

UNCLASSIFIED / FOR OFFICIAL USE ONLY

Current Mode	Triggering Event Number	Triggering Event Condition	Next Mode
Normal Operations: Discrete	T53	CIK Removal	Alarm
Alarm	T60	Zeroize Request (button press)	Zeroize
Alarm	T61	Critical Alarm	Power-Down
Alarm	T62	Alert	Normal Operations: Interactive
Alarm	T63	Alert	Normal Operations: Discrete
Zeroize	T80	Power-Down	Power-Down
Power-Down	T90	Zeroize Request (button press)	Zeroize
Power-Down	T91	Working Memory Zeroize	Zeroize
Power-Down	T92	Shutdown	Off

Table 2 – (U) High-Level Modes and Triggers

3.1.2 (U//FOUO) NGLD-M and Medium Assurance Mode

(U//FOUO) The NGLD-M is required to operate normally in either a Medium Assurance mode or High Assurance mode. Figure 3 leverages the high-level modes defined in section 3.1.1 and focuses on NGLD-M operating in a Medium Assurance mode; denoted by the absence of a valid High Assurance CIK being present in the NGLD-M. Numbered triggers are supplied in Figure 3 (with corresponding information provided in Table 3) and they represent entry and exit conditions into and out of a mode. A darkened rectangle is provided to indicate the status of the High Assurance cryptographic module, which is marked as deactivated in this illustration because no High Assurance CIK is inserted into the system.

(U//FOUO) The NGLD-M is authorized to power-up into Medium Assurance mode if there is not a valid High Assurance CIK inserted. The NGLD-M requires the Medium Assurance mode of operation to allow for the ability to perform cryptographic functions without the use of the High Assurance cryptographic module. This includes, but is not limited to, connections to varied classification networks (e.g. SIPRNET, NIPRNET, Tactical Secret, JWICS (Objective)), OTNK compliant Storefronts, KMI-Aware ECUs, other NGLD-Ms, Last Mile API (LMA) capable systems, which support encrypted (i.e., black) package operations. While in Medium Assurance mode, the NGLD-M uses KMI signed Medium Assurance certificates that are stored and managed outside the High Assurance cryptographic boundary. The ability to perform this operation allows many functional use cases to be realized, without the operational overhead that accompanies use of the High Assurance cryptographic module. The authorized user can demand transition into a High Assurance mode from Medium Assurance mode by inserting a valid CIK into the NGLD-M and passing validation tests.

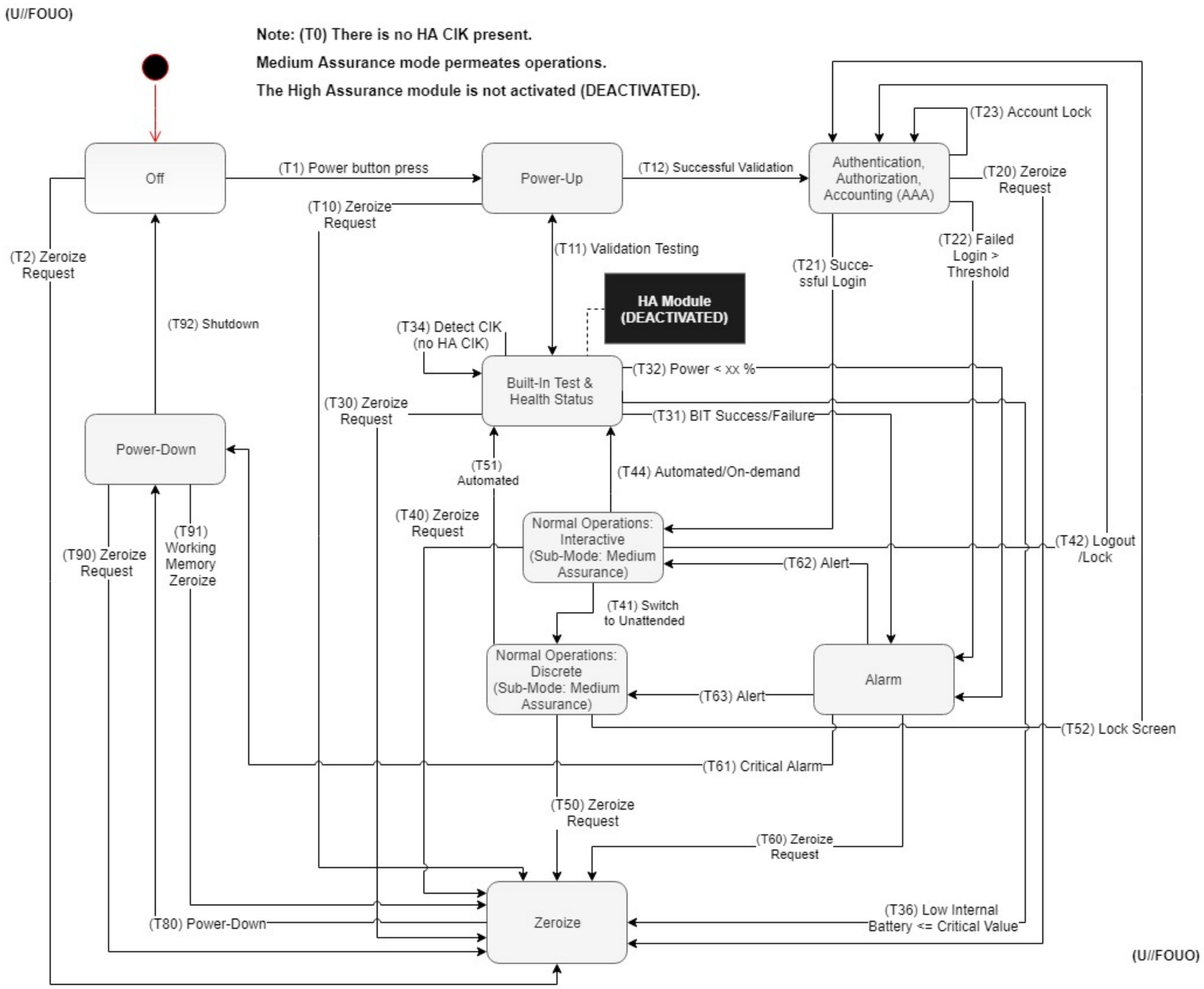

(U//FOUO)
Note: (T0) There is no HA CIK present.
Medium Assurance mode permeates operations.
The High Assurance module is not activated (DEACTIVATED).
Off
(T1) Power button press
Power-Up
(T12) Successful Validation
Authentication, Authorization, Accounting (AAA)
(T23) Account Lock
(T20) Zeroize Request
(T10) Zeroize Request
(T2) Zeroize Request
(T11) Validation Testing
(T21) Succe-ssful Login
(T22) Failed Login > Threshold
HA Module (DEACTIVATED)
(T92) Shutdown
(T34) Detect CIK (no HA CIK)
Built-In Test & Health Status
(T32) Power < xx %
(T30) Zeroize Request
(T31) BIT Success/Failure
Power-Down
(T51) Automated
(T44) Automated/On-demand
(T40) Zeroize Request
Normal Operations: Interactive (Sub-Mode: Medium Assurance)
(T42) Logout /Lock
(T90) Zeroize Request
(T91) Working Memory Zeroize
(T62) Alert
(T41) Switch to Unattended
Normal Operations: Discrete (Sub-Mode: Medium Assurance)
Alarm
(T63) Alert
(T52) Lock Screen
(T61) Critical Alarm
(T50) Zeroize Request
(T60) Zeroize Request
(T36) Low Internal Battery <= Critical Value
(T80) Power-Down
Zeroize
(U//FOUO)

Figure 3 – (U//FOUO) Operating in Medium Assurance mode; High Assurance Module is Deactivated

UNCLASSIFIED / FOR OFFICIAL USE ONLY

Current Mode	Triggering Event Number	Triggering Event Condition	Next Mode
N/A	T0	No HA CIK is plugged in	N/A
Off	T1	Power button press	Power-Up
Off	T2	Zeroize Request (button press)	Zeroize
Power-Up	T10	Zeroize Request (button press)	Zeroize
Power-Up	T11	Validation Testing	Built-In Test & Health Status
Power-Up	T12	Successful Validation	Authentication, Authorization, Accounting (AAA)
Authentication, Authorization, Accounting (AAA)	T20	Zeroize Request (button press)	Zeroize

Current Mode	Triggering Event Number	Triggering Event Condition	Next Mode
Authentication, Authorization, Accounting (AAA)	T21	Successful Login	Normal Operations: Interactive
Authentication, Authorization, Accounting (AAA)	T22	Failed Login > Threshold	Alarm
Authentication, Authorization, Accounting (AAA)	T23	Account Lock	Authentication, Authorization, Accounting (AAA)
Built-In Test & Health Status	T30	Zeroize Request (button press)	Zeroize
Built-In Test & Health Status	T31	BIT Success/Failure	Alarm
Built-In Test & Health Status	T32	Power < xx %	Alarm
Built-In Test & Health Status	T34	Detect CIK (no HA CIK)	Built-In Test & Health Status
Built-In Test & Health Status	T36	Low Internal Battery <= Critical Value	Zeroize
Normal Operations: Interactive	T40	Zeroize Request (button press [physical or logical])	Zeroize
Normal Operations: Interactive	T41	Switch to Discrete	Normal Operations: Discrete
Normal Operations: Interactive	T42	Logout/Lock	Authentication, Authorization, Accounting (AAA)
Normal Operations: Interactive	T44	Automated/On-Demand	Built-In Test & Health Status
Normal Operations: Discrete	T50	Zeroize Request (button press)	Zeroize
Normal Operations: Discrete	T51	Automated	Built-In Test & Health Status
Normal Operations: Discrete	T52	Lock Screen	Authentication, Authorization, Accounting (AAA)
Alarm	T60	Zeroize Request (button press)	Zeroize
Alarm	T61	Critical Alarm	Power-Down
Alarm	T62	Alert	Normal Operations: Interactive
Alarm	T63	Alert	Normal Operations: Discrete
Zeroize	T80	Power-Down	Power-Down
Power-Down	T90	Zeroize Request (button press)	Zeroize

UNCLASSIFIED / FOR OFFICIAL USE ONLY

Current Mode	Triggering Event Number	Triggering Event Condition	Next Mode
Power-Down	T91	Working Memory Zeroize	Zeroize
Power-Down	T92	Shutdown	Off

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Table 3- (U) Triggers and Modes of Medium Assurance mode

3.1.3 (U) NGLD-M and High Assurance Mode

(U//FOUO) The NGLD-M can be activated into a High Assurance mode as illustrated in Figure 4. Numbered triggers are supplied in Figure 4 (with corresponding information provided in Table 4) and they represent entry and exit conditions into and out of a mode. A rectangle is provided to indicate the status of the High Assurance cryptographic module, which is marked as activated in this illustration because a valid HA CIK is inserted into the system.

(U//FOUO) When a valid CIK is not inserted, the NGLD-M can be operated by authorized users in Medium Assurance mode. To transition into High Assurance mode a valid Cryptographic Ignition Key (CIK) must be physically inserted into the NGLD-M and a valid user initiates transition to High Assurance mode, on-demand. NGLD-M validates the CIK and user and, if successful, the cryptographic module capable of High Assurance operations can be used and the system can be operated with High Assurance logic (as well as with Medium Assurance logic); enabling capabilities for High Assurance receiving, processing, management, and distribution of cryptographic key and key-related material. This includes, but is not limited to, connections to varied classification networks (e.g. SIPRNET, NIPRNET, Tactical Secret, JWICS (Objective)), OTNK compliant Storefronts, KMI-Aware ECUs, other NGLD-Ms, Last Mile API (LMA) capable systems, which perform encrypted (i.e., black) and unencrypted (i.e. red) operations also involving Legacy Interfaces/Backward Compatibility. While in High Assurance mode, the NGLD-M uses KMI signed High Assurance certificates that are stored and managed inside the High Assurance cryptographic boundary and can also utilize legacy High Assurance (formerly Type 1) algorithms. Medium Assurance capabilities can also be used when High Assurance mode is active. The NGLD-M can be transitioned into Medium Assurance mode via the removal of CIK that ignited High Assurance mode.

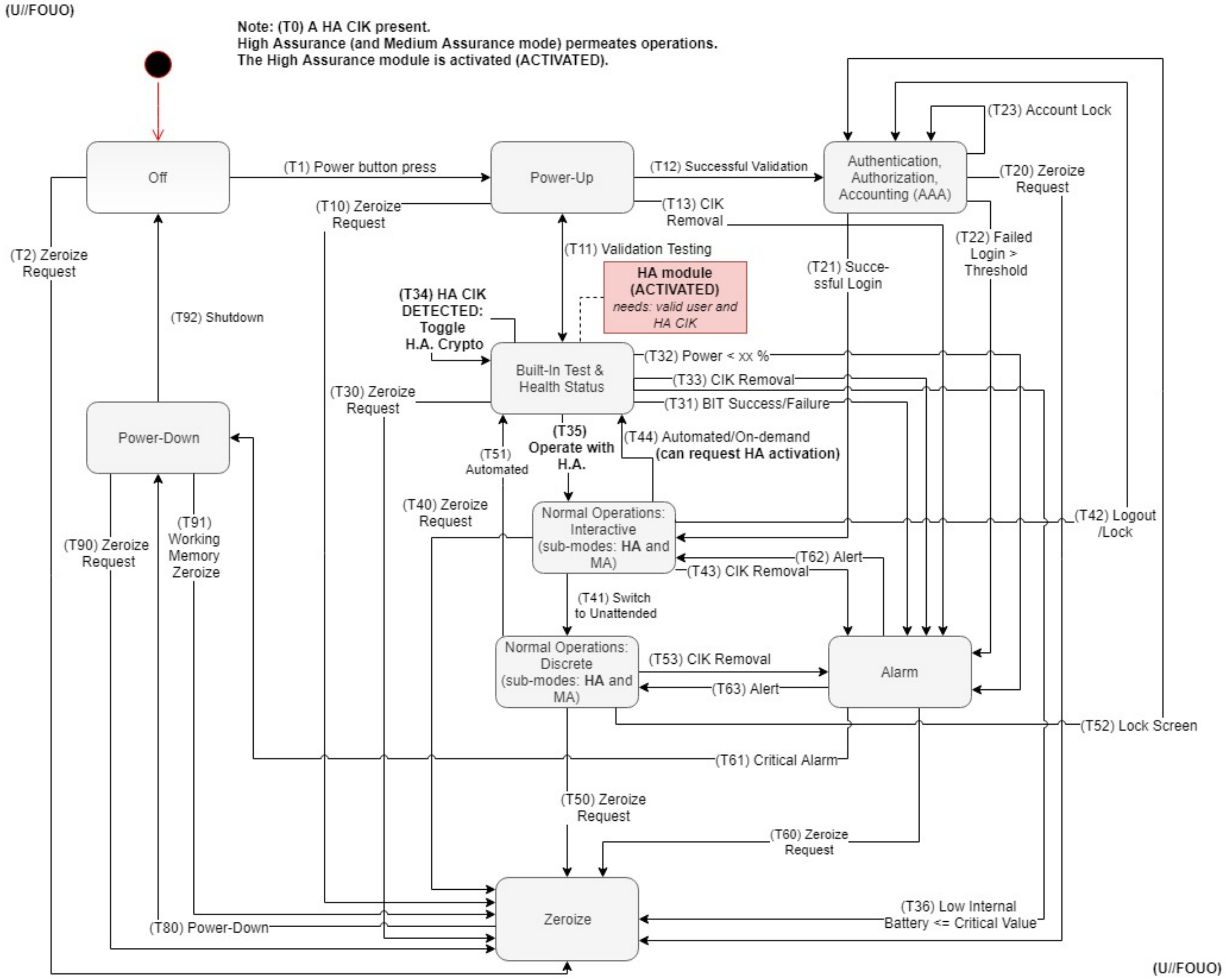

(U//FOUO)
Note: (T0) A HA CIK present.
High Assurance (and Medium Assurance mode) permeates operations.
The High Assurance module is activated (ACTIVATED).
Off
(T1) Power button press
Power-Up
(T12) Successful Validation
Authentication, Authorization, Accounting (AAA)
(T23) Account Lock
(T20) Zeroize Request
(T22) Failed Login > Threshold
(T21) Successful Login
(T2) Zeroize Request
(T10) Zeroize Request
(T13) CIK Removal
(T11) Validation Testing
HA module (ACTIVATED)
needs: valid user and HA CIK
(T34) HA CIK DETECTED: Toggle H.A. Crypto
(T92) Shutdown
Built-In Test & Health Status
(T32) Power < xx %
(T33) CIK Removal
(T31) BIT Success/Failure
(T30) Zeroize Request
Power-Down
(T51) Automated
(T35) Operate with H.A.
(T44) Automated/On-demand
(can request HA activation)
(T40) Zeroize Request
Normal Operations: Interactive (sub-modes: HA and MA)
(T42) Logout /Lock
(T62) Alert
(T43) CIK Removal
(T90) Zeroize Request
(T91) Working Memory Zeroize
(T41) Switch to Unattended
Normal Operations: Discrete (sub-modes: HA and MA)
(T53) CIK Removal
(T63) Alert
Alarm
(T52) Lock Screen
(T61) Critical Alarm
(T50) Zeroize Request
(T60) Zeroize Request
(T36) Low Internal Battery <= Critical Value
(T80) Power-Down
Zeroize
(U//FOUO)

Figure 4 – (U//FOUO) Transition from Medium Assurance mode to High Assurance mode; while retaining Medium Assurance capability

UNCLASSIFIED / FOR OFFICIAL USE ONLY

Current Mode	Triggering Event Number	Triggering Event Condition	Next Mode
N/A	T0	An HA CIK is plugged in	N/A
Off	T1	Power button press	Power-Up
Off	T2	Zeroize Request (button press)	Zeroize
Power-Up	T10	Zeroize Request (button press)	Zeroize
Power-Up	T11	Validation Testing	Built-In Test & Health Status
Power-Up	T12	Successful Validation	Authentication, Authorization, Accounting (AAA)
Power-Up	T13	CIK Removal	Alarm
Authentication, Authorization, Accounting (AAA)	T20	Zeroize Request (button press)	Zeroize

Current Mode	Triggering Event Number	Triggering Event Condition	Next Mode
Authentication, Authorization, Accounting (AAA)	T21	Successful Login	Normal Operations: Interactive
Authentication, Authorization, Accounting (AAA)	T22	Failed Login > Threshold	Alarm
Authentication, Authorization, Accounting (AAA)	T23	Account Lock	Authentication, Authorization, Accounting (AAA)
Built-In Test & Health Status	T30	Zeroize Request (button press)	Zeroize
Built-In Test & Health Status	T31	BIT Success/Failure	Alarm
Built-In Test & Health Status	T32	Power < xx %	Alarm
Built-In Test & Health Status	T33	CIK Removal	Alarm
Built-In Test & Health Status	T34	(T34) HA CIK DETECTED: Toggle H.A. Crypto	Built-In Test & Health Status
Built-In Test & Health Status	T35	Operate with H.A.	Normal Operations: Interactive
Built-In Test & Health Status	T36	Low Internal Battery <= Critical Value	Zeroize
Normal Operations: Interactive	T40	Zeroize Request (button press [physical or logical])	Zeroize
Normal Operations: Interactive	T41	Switch to Discrete	Normal Operations: Discrete
Normal Operations: Interactive	T42	Logout/Lock	Authentication, Authorization, Accounting (AAA)
Normal Operations: Interactive	T43	CIK Removal	Alarm
Normal Operations: Interactive	T44	Automated/On-Demand (can request HA activation)	Built-In Test & Health Status
Normal Operations: Discrete	T50	Zeroize Request (button press)	Zeroize
Normal Operations: Discrete	T51	Automated	Built-In Test & Health Status
Normal Operations: Discrete	T52	Lock Screen	Authentication, Authorization, Accounting (AAA)

UNCLASSIFIED / FOR OFFICIAL USE ONLY

Current Mode	Triggering Event Number	Triggering Event Condition	Next Mode
Normal Operations: Discrete	T53	CIK Removal	Alarm
Alarm	T60	Zeroize Request (button press)	Zeroize
Alarm	T61	Critical Alarm	Power-Down
Alarm	T62	Alert	Normal Operations: Interactive
Alarm	T63	Alert	Normal Operations: Discrete
Zeroize	T80	Power-Down	Power-Down
Power-Down	T90	Zeroize Request (button press)	Zeroize
Power-Down	T91	Working Memory Zeroize	Zeroize
Power-Down	T92	Shutdown	Off

UNCLASSIFIED / FOR OFFICIAL USE ONLY

Table 4 – (U//FOUO) Transitioning from Medium Assurance to High Assurance mode (while retaining Medium Assurance mode capability).

3.2 (U) System or Subsystem Functional Requirements

(U//FOUO) The NGLD-M is an Army-sponsored load device used by all DoD Military Services as well as Civil Agencies for performing operations involving cryptographic product retrieval from data sources such as the KMI and distribution to ECUs. The NGLD-M allows users to perform common load device actions such as distributing and receiving cryptographic products, performing planning activities with platforms/equipment/payloads, reviewing audit logs and device health information, and other activities as defined by the NGLD-M system requirements. Figure 5 - (U) NGLD-M Context depicts a high-level operational view of the NGLD-M in a context relative to external actors with which it communicates.

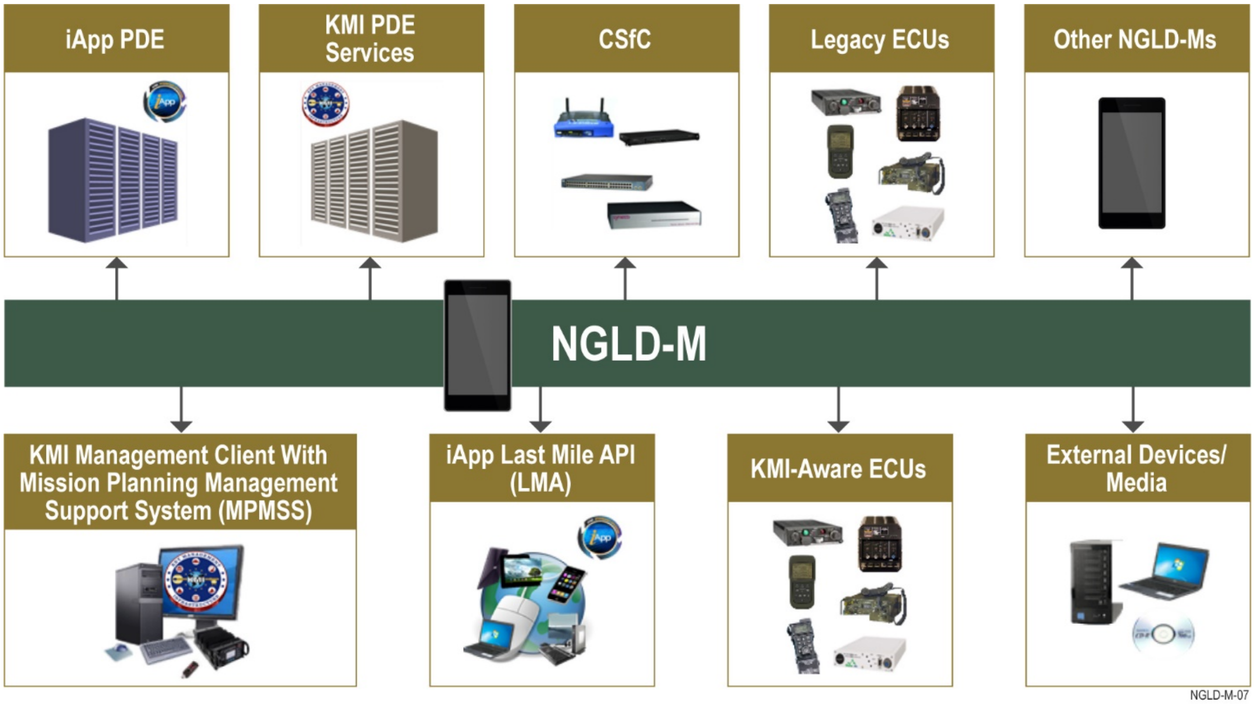
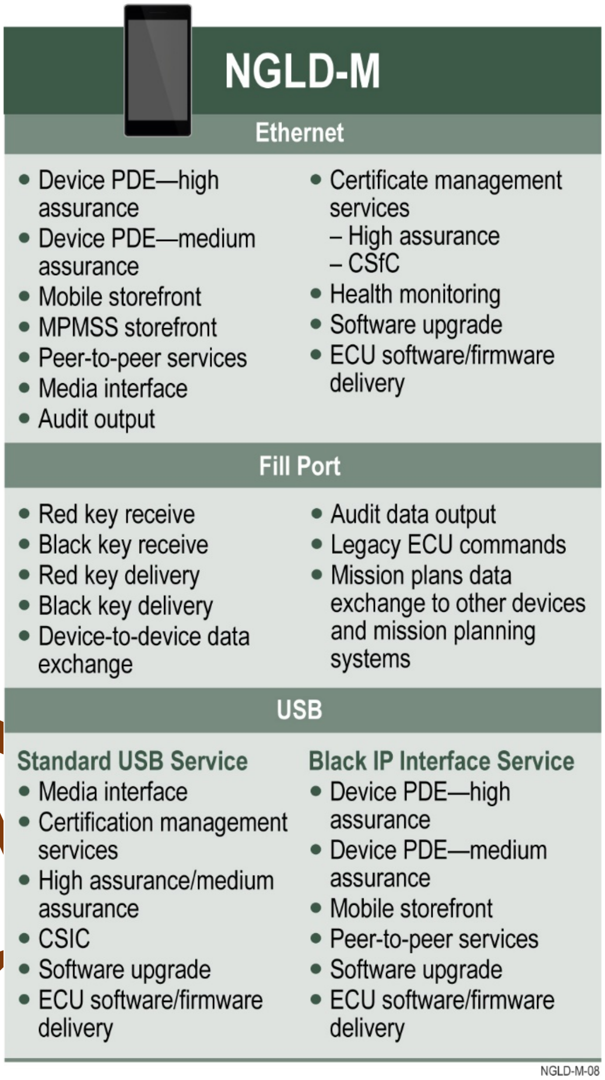


Figure 5 - (U) NGLD-M Context Diagram

(U//FOUO) As depicted on the external data sources depicted, the NGLD-M utilizes different load device physical port interfaces depending on the activity the user needs to support. This figure provides an overview of the activities supported through the physical port interfaces available on the NGLD-M. The interfaces supported include Ethernet, Fill Port, and USB.

(U//FOUO) The requirements to support these functions for the NGLD-M are delineated in the following sections of this document.


NGLD-M

Ethernet

- Device PDE—high assurance
- Device PDE—medium assurance
- Mobile storefront
- MPMSS storefront
- Peer-to-peer services
- Media interface
- Audit output
- Certificate management services
  - High assurance
  - CSfC
- Health monitoring
- Software upgrade
- ECU software/firmware delivery

Fill Port

- Red key receive
- Black key receive
- Red key delivery
- Black key delivery
- Device-to-device data exchange
- Audit data output
- Legacy ECU commands
- Mission plans data exchange to other devices and mission planning systems

USB

Standard USB Service

- Media interface
- Certification management services
- High assurance/medium assurance
- CSIC
- Software upgrade
- ECU software/firmware delivery

Black IP Interface Service

- Device PDE—high assurance
- Device PDE—medium assurance
- Mobile storefront
- Peer-to-peer services
- Software upgrade
- ECU software/firmware delivery

Figure 6 - (U) NGLD-M Interface Examples

3.2.1 (U) Power-Up

(U//FOUO) The NGLD-M is required to reach a Power-Up state when physically initiated by the user. The system will securely boot up and protect from intrusion by disabling all external data transfer interfaces. It is recognized that not all security features may be available during the Power-Up mode. Power-Up will occur within 30 seconds and Power-Up status will be physically indicated to the user. Once the Power-Up state is successfully reached, the user is presented with a login display including useful information (e.g., the software and hardware version information for the unit). Automatic brightness adjustments allow the display to be readable.

3.2.2 (U) User (Human User and Device User) Management

(U//FOUO) NGLD-M User and Device Management provides the capability to manage users and the NGLD-M within the device. It provides for the addition, modification, deletion, and displaying of users. The device enforces user authentication per the requirements in the Risk Management Framework (RMF) and the Information Assurance Security Requirements Document (IASRD). NGLD-M provides role based access control (RoBAC) so that users can be privileged to provide separation of duties.

3.2.2.1 (U) Human User Management

(U//FOUO) One type of user that the NGLD-M supports is the human user. The Human User is a user of the device that logs into the device to perform their operational duties. The NGLD-M allows for the creation and management of these users in the system. The NGLD-M also stores all of the credentials and certificates that the user needs to access other systems and networks.

3.2.2.2 (U) Device User Management

(U//FOUO) The NGLD-M also supports a second type of user called a Device User. The Device Users are the NGLD-M itself and external devices that connect to the NGLD-M. The Device Users hold their own KMI issued High and Medium Assurance Credentials and are therefore able to access the KMI OTNK compliant Storefronts and retrieve products wrapped for the device.

3.2.2.3 (U) Access Control

(U//FOUO) The NGLD-M enforces RoBAC in the device. After a user logs into the system only operations that are privileged to the role are offered by the NGLD-M for execution. The capability is required to comply with security doctrine definition of separation of duties for sensitive operations.

3.2.3 (U) Managing

(U//FOUO) The NGLD-M Managing capability provides methods for the user to perform various operations (add, edit, view, delete, etc.) on the contents (mission plan data, keys/key tags, non-key data, etc.) stored in the NGLD-M system.

3.2.3.1 (U) Certificate Management

(U//FOUO) Certificates are used in the NGLD-M to perform various operations such as authentication, decryption and signature verification of CMS packages. In order for the NGLD-M to fully utilize all the services provided by KMI and OTNK, the NGLD-M must be provisioned with an X.509 certificate set from KMI. NGLD-M is responsible for building its own private/unsigned-public key pair and certificate signing requests for medium and high assurance certificates. The certificate set from KMI includes KMI Trust Anchors, the KMI signed NGLD-M Identity certificate (IA), and the KMI signed Key Encryption (KE) certificate. The NGLD-M uses the IA certificate to authenticate into the KMI web services and uses the KE certificate to validate and unwrap products that are addressed to the NGLD-M. When the NGLD-M has both an IA(I) certificate and a KE(I) certificate, it is considered KMI-Aware. This awareness gives the NGLD-M the ability to request a Product Availability List (PAL) and subsequently obtain any product listed on the PAL.

(U//FOUO) NGLD-M Certificate Management includes:

- Registration of the NGLD-M as a KMI-Aware device by using its Electronic Serial Number (ESN) to obtain the required IA(I) certificate used for High Assurance secure communications with KMI or its Virtual ESN (VESN) for Medium Assurance.
- Managing both high and medium assurance certificates, including public/private key pair generation, certificate signing request generation, trust anchor management, signed certificate management, rekey, and certificate revocation rules.
- Providing mechanisms and logic for export, import, and viewing of certificate registration data and details (e.g., ESN, VESN, distinguished name, public key, fingerprints, key usage, extended key usage).

3.2.3.1.1 (U) Certificate Revocation List (CRL) Management

(U//FOUO) A CRL is a listing of the revocation of certificates that a given Certificate Authority (CA) issued. It is maintained by a CA that the NGLD-M trusts, and made available via various means, in the KMI case via the KMI Storefront (or downstream OTNK-compliant storefronts). NGLD-M retains current copies of the CRL and allocates adequate storage space. CRLs are used to ascertain the validity and revocation status of a certificate issued by the CA, used on the NGLD-M to check the validity of signed CMS packages by authenticating that the signer's certificate is valid and whenever certificates are used. NGLD-M also provides the capability to distribute CRL data.

(U//FOUO) The CRL Management capability provides the methods to:

- View CRLs
- Delete CRLs

3.2.3.1.1.2 (U) Authority Revocation List (ARL) Management

(U//FOUO) An ARL is a listing of revocation of CA certificates. It is maintained by the CA infrastructure that the NGLD-M trusts and made available via the same means as a CRL. NGLD-M retains current copies of the ARL and allocates adequate storage space. The ARL is used to ascertain the validity and revocation status of a CA certificate issued by the CA infrastructure, used on the NGLD-M to check the validity of signed CMS packages by authenticating that the signer's certificate is valid and whenever certificates are used. NGLD-M is also required to provide the capability to distribute ARL data.

(U//FOUO) The ARL Management capability provides the methods to:

- View ARLs
- Delete ARLs

3.2.3.2 (U) Connection Management

(U//FOUO) The NGLD-M supports communications with a variety of external interfaces as outlined in section 0 - 3.3.3 (U) Logical (Networked) External Interfaces. Many of these interfaces are supported by establishing and managing connections to allow communications. Managing connections allows users to setup / configure connection information that can be used throughout the NGLD-M to perform interfacing actions.

(U//FOUO) The Connection Management capability provides the methods to:

- Create Connections
- View Connections
- Edit Connections
- Delete Connections

3.2.3.3 (U) Cryptographic Product Management

(U//FOUO) The NGLD-M manages a variety of cryptographic products. This includes keys as well as other products such as software, certificates and CRLs. In addition to keys, the NGLD-M supports a concept of key tags to allow minimal planning when a key is not yet resident on the device.

3.2.3.3.1 (U) Cryptographic Keys / Key Tag Management

(U//FOUO) NGLD-M manages a variety of cryptographic products. This includes cryptographic keys as well as key tags. Cryptographic keys in the NGLD-M include encrypted and unencrypted symmetric and asymmetric products. These products are received into the NGLD-M system via the *Receive* capability. Cryptographic key tags are created so that the user can perform last mile mission planning in advance of loading and/or receiving the key material.

Cryptographic Key tags can also be received via the Receive capability from mission planning systems or fill devices that support the Common Tier 3 (CT3) specification.

(U//FOUO) The Cryptographic Keys/Key Tags Management capability provides the methods to:

- Create Key Tags
- View Keys/Key Tags
- Edit Key/Key Tag
- Delete Keys/Key Tags
- View Expired Keys/Key Tags
- Assign Keys/Key Tags
- Unassign Keys/Key Tags
- Effective Date Management
- File Header Management

3.2.3.4 (U) Mission Plan Management

(U//FOUO) The NGLD-M manages the mission plan data in support of mission planning operations such as managing effective dates, assignments of mission data that was either received into the system or manually created by the user on the NGLD-M. Mission plans are received into the NGLD-M system via various formats such as 87-27, Tier 3 XML, SINCGARS Loadset, etc. from various mission planning systems such as iApp, ACES, JENM, etc. The mission plans may contain Platform Groups, Platforms, Devices, Cryptographic keys/key tags, EP Data, Message Data, Benign Fill (BF) messages, Radio Configuration Files (RCFs), HAVEQUICK, Single Operating Instruction (SOI) data, Single Channel Ground Air Radio System (SINCGARS) loadset, etc.

3.2.3.4.1 (U//FOUO) Platform Group Management

(U//FOUO) A Platform Group is a user-defined item that represents a grouping of Platforms used for mission planning purposes.

(U//FOUO) The Manage Platform Group capability provides the methods or options to:

- Create Platform Groups
- View Platform Groups
- Edit Platform Groups
- Delete Platform Groups

3.2.3.4.2 (U//FOUO) Platform Management

(U//FOUO) A Platform is a user-defined item that represents a grouping of devices used for mission planning purposes.

(U//FOUO) The Manage Platform capability provides the methods or options to:

- Create Platforms
- View Platforms
- Edit Platforms
- Delete Platforms
- Assign Platforms
- Unassign Platforms

3.2.3.4.3 (U//FOUO) Device Management

(U//FOUO) A Device is a user-defined instance of a particular device type that is supported by the NGLD-M and used for mission planning purposes.

(U//FOUO) The Manage Device capability provides the methods or options to:

- Create Device
- View Device
- Edit Device
- Delete Device
- Assign Device
- Unassign Device

3.2.3.4.4 (U) Signal Operating Instruction (SOI) Data Management

(U//FOUO) SOI Data includes network groups, networks, time period, call signs, call words, cue and manual frequencies, suffixes, expanders, signs, countersigns, pyrotechnic and smoke signals, and quick references.

(U//FOUO) The SOI Data Management capability provides the methods to:

- Display SOI Data
- Delete SOI Data

3.2.3.4.5 (U) Benign Fill (BF) Message Management

(U//FOUO) BF messages are mainly used to support the F-22 and Advanced Extremely High Frequency (AEHF) benign keying, benign rekeying, and BF operations. These BF Messages include Credential Request (CREDRQ), ECU Response (ECURS), Application Key Material Delivery (AKDELIV), and Key_Replacement Delivery (KRDELIV).

(U//FOUO) The manage BF capability provides the methods or options to:

- View BF Message
- Delete BF Message
- Assign BF Message
- Unassign BF Message

3.2.3.4.6 (U) Electronic Protection (EP) Data Management

(U//FOUO) EP data is considered non-cryptographic key content leveraged to support an Electronic Counter Measure (ECM) resistant/frequency-hopping system used for jam resistance and to protect military radio traffic. EP Data includes Integrated COMSEC (ICOM) Hopsets, Non-ICOM Hopsets, Lockouts, Single Channel Frequency, Cue Frequency.

(U//FOUO) The manage EP Data capability provides the methods to:

- View EP Data
- Delete EP Data
- Assign EP Data
- Unassign EP Data

3.2.3.4.7 (U) Message Data Management

(U//FOUO) The NGLD-M provides the user the capability to create B1 and B2 Message Data targeted for specific ECUs. The Message Data type is non-cryptographic key used with HAVEQUICK (WOD, MWOD), Time of Day (TOD) from the Global Positioning System (GPS) system, Word of the Day (WOD), which serves as a key, and Network Identification (Net ID) on airborne devices.

(U//FOUO) The Message Data Management capability provides the methods to:

- View Message Data
- Delete Message Data
- Assign Message Data
- Unassign Message Data

3.2.3.4.8 (U) Radio Configuration Files (RCF) Management

(U//FOUO) RCFs are created for specific networks for IP-based software defined radios. These RCFs are generated to configure a radio, and the NGLD-M provides the capability to download the correct RCFs to the radio.

(U//FOUO) The RCFs Management capability provides the methods or options to:

- View RCF
- Delete RCF
- Assign RCF
- Unassign RCF

3.2.3.5 (U) Audit Data Management

(U//FOUO) The NGLD-M Audit Data consists of important security events that are automatically captured and stored in the Audit Log. Events that are captured include but not limited to:

- Audit Trail Initialized
- Audit Trail Full
- Audit Upload
- Card Zeroized
- Connect to Device
- Successful Login
- Unsuccessful Login
- Host Mismatch
- Host File Uploaded
- Host Generated Requests
- Host Software / Firmware Update / Receive
- Alarm
- Software Update Received
- User Account Created
- User Account Password Changed
- User Account Deleted

- Maximum Login Attempts
- Date/Time Changed
- CIK Configured
- Benign Fill for Transmit
- Benign Fill for Receive
- Benign Fill for Delete
- Benign Fill Zeroized
- Key Received
- Key Transmitted
- Key Updated
- Key Deleted
- Keys Zeroized
- COMSEC Device Connection (Association and Exchange Identifiers (AXID) parameters)

(U//FOUO) The Fill Device Audit Data Management capabilities are only available to a privileged user with the appropriate role. This capability provides the methods to:

- View Audit Data
- Upload Audit Data
- Reset/Clear Audit Data

3.2.3.6 (U) F-22 ECU Management

(U//FOUO) The NGLD-M supports the capabilities to manage the benign keying and benign fill process for the F-22 ECUs.

(U//FOUO) The F-22 ECU Management capability provides the methods to:

- Manage the F-22 ECU benign keying process
- Manage the F-22 ECU benign fill process
- Manage the F-22 ECU benign rekeying process
- Manage the various states of the F-22 ECUs in the benign keying, rekeying and benign fill process
- Manage the F-22 ECU Emergency Rekey (REDBALL) process

3.2.3.7 (U) TrKEK Management

(U//FOUO) The NGLD-M supports the capabilities to manage TrKEKs that are filled into the NGLD-M for the purpose of decrypting TrKEK encrypted keys during the key fill process into the ECUs.

(U//FOUO) The TrKEK Management capability provides the methods to:

- View filled TrKEKs
- Delete filled TrKEKs

3.2.3.8 (U) File Management

(U//FOUO) The NGLD-M supports the capabilities to manage files that are received through the various interfaces to include but not limited to USB or Ethernet. Files brought in are stored on the NGLD-M and the user can view, rename and delete the files.

(U//FOUO) The Files Management capability provides the methods to:

- View File
- Edit File (rename)
- Delete File

3.2.3.9 (U) NGLD-M System Management

(U//FOUO) NGLD-M is required to support authorized management and control of local system components and capabilities. These local system components are intended for a limited subset of users that are privilege controlled to interact with the NGLD-M to perform system management duties that include, but are not limited to, external physical interfaces control, software/firmware update management, date/time adjustment, crypto subsystem status, and backup and recovery management.

3.2.3.10 (U) NGLD-M Mobile Device Storefront Management

(U//FOUO) NGLD-M offers an OTNK-compliant device PDE Storefront, covered in section 0 - 3.3.3.6 (U) NGLD-M Mobile Device PDE Storefront (PUI:NMDPDE) covers the external interface requirement portion of the mobile device storefront on the NGLD-M. This section covers the requirements for managing that Storefront and its contents on the NGLD-M, as well as the internal capabilities of the Storefront itself. Managing this storefront allows NGLD-M users to add and remove products to the Storefront and authorize external devices to access / retrieve them.

3.2.4 (U) Receiving

(U//FOUO) The NGLD-M Receive capability provides the methods or options to receive cryptographic key, non-cryptographic key content, and mission plan data into the system.

(U//FOUO) Cryptographic keys include:

- Encrypted and unencrypted symmetric and asymmetric keys in varied formats (e.g., 87-27, Tier 2 XML, Tier 3 XML, CMS package) may be obtained over varied interfaces (e.g. Ethernet, DS-101, DS-102, RS-232, USB, etc.).

(U//FOUO) Mission plan data includes:

- Platform Groups, Platforms, Devices, Cryptographic Keys/Key Tags, HAVEQUCK (WOD, MWOD), frequency hopping data such as EP Data, Message data, benign fill messages, SOI data, Radio Configuration Files (RCFs), and SINCGARS Loadset may be received over a variety of interfaces (e.g., 87-27, Ethernet, DS-101, DS-102, RS-232, USB, etc.).

(U//FOUO) Other non-key data includes:

- Certificates, CRLs, ARLs, ECU Commands, Health and Monitoring Data, RCFs, Device Configuration Settings, Software/Firmware, Information Assurance Vulnerability Alert (IAVA) Patches received over various interfaces (e.g. Ethernet, USB interfaces, DS-101, etc.).

(U//FOUO) The NGLD-M provides the capability to receive cryptographic key, non-cryptographic key content, and mission plans data into the system using defined protocols and formats identified in Table 5 – (U) NGLD-M Receiving Data Types and Interfaces.

Type of Data	Interface	Data Format	Specification
Platform Group, Platform, Device Sets (i.e., payload data)	DS-101/RS-232, Ethernet, USB, Wireless	87-27	CT3 ICD
Platform Group, Platform, Device Sets (i.e., payload data)	Ethernet, USB, Wireless	Tier 3 XML	CT3 ICD
Key Tag/Key Material	DS-101/RS-232, DS-102, Ethernet, USB, Wireless	87-27	CT3 ICD EKMS-308
Key Tag/Key Material	Ethernet, USB, Wireless	Tier 2 XML	XML BKD ICD
Key Tag/Key Material	Ethernet, USB, Wireless	Tier 3 XML	Tier 3 XML Schema
Key Material	CFDI (KYK-13)	CFDI	EKMS-308
Key Material	CFDI (KOI-18)	CFDI	EKMS-308
Key Material	CFDI (KYX-15), OTAT	CFDI	EKMS-308
Key Material (Benign Fill)	DS-101/RS-232 Ethernet, USB, Wireless	87-27	EKMS-217
Benign Fill Messages (non-key material)	DS-101/RS-232, Ethernet, USB, Wireless	87-27	EKMS-217
EP Data	DS-101/RS-232, Ethernet, USB, Wireless	87-27	CT3 ICD
EP Data	Ethernet, USB, Wireless	Tier 3 XML	Tier 3 XML Schema
Message Data	DS-101/RS-232, Ethernet, USB, Wireless	87-27	CT3 ICD
Message Data	Ethernet, USB, Wireless	Tier 3 XML	Tier 3 XML Schema
SOI	DS-101/RS-232, Ethernet, USB, Wireless	87-27	CT3 ICD
SOI	Ethernet, USB	Tier 3 XML	Tier 3 XML Schema
Radio Configuration File (RCF)	Ethernet, USB, Wireless	87-27	Tier 3 XML Schema
HAVEQUICK	DS-101/RS-232, Ethernet, USB, Wireless	87-27	CT3 ICD
HAVEQUICK	Ethernet, USB, Wireless	Tier 3 XML	Tier 3 XML Schema
SINCGARS Loadset	DS-101/RS-232, Ethernet, USB, Wireless	87-27	SINCGARS
ECU Commands	DS-101/RS-232, Wireless	87-27	EKMS-308
CMS Package	Ethernet, USB, Wireless	CMS	OTNK
Certificates	Ethernet, USB, Wireless	X.509	OTNK
Certificate Revocation Lists (CRL)	Ethernet, USB, Wireless	X.509	OTNK
Authority Revocation Lists (ARL)	Ethernet, USB, Wireless	X.509	OTNK
Health and Monitoring Data	Ethernet, Wireless	SNMP	SNMP LMA API

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Type of Data	Interface	Data Format	Specification
Device Configuration Settings	Ethernet, USB, Wireless	SNMP	SNMP LMA API
Software/Firmware	Ethernet, USB, Wireless	CMS, Signed Data	OTNK
Files	Ethernet, USB, Wireless	Various	Various

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Table 5 – (U) NGLD-M Receiving Data Types and Interfaces

(U//FOUO) The NGLD-M provides the capability to receive key data and non-key mission data from the equipment specified in Table 6 – (U) NGLD-M Legacy Device Key Sources.

Device Type	Protocol	Device Type	Protocol
KYK-13	DS 102	KGX-93	DS102
KOK-13	DS102	KYX-15	DS102
KGX-93A	DS102	MX-18290	DS102
KOI-18	DS102	KW46-OT	DS102
DTD/SDS/SKL	DS101	KY-57	DS102
KY-100	DS102	KY-58	DS102
RT-1523	DS102	KY-67	DS102
RT1523-B	DS102	KY-99A	DS102
KG-83	DS102	KW-46	DS102
ARC-234	DS101/102	HGX-83	DS102
KOK-22/32 (KP)	DS101	KOK-23	DS101
Workstations: WKS-2400, WKS-9600, STE-2400, STE-9600, DKLIF, Ethernet			

Table 6 – (U) NGLD-M Legacy Device Key Sources

3.2.4.1 (U) Receive Mission Plan Data

(U//FOUO) The NGLD-M Receive Mission Plan Data capability provides the method to receive various data contained in the mission plan, SINCGARS Loadset, etc. Data contained in the mission plan may include CT3 payload items such as Platform Group, Platform, Devices and Keys/Key Tags/EP Data/Message Data assigned to Devices, Benign Fill messages, SOI Data, RCFs, etc. Data in the SINCGARS Loadset may contain COMSEC key and Frequency Hoping (FH) data (hopset/lockout, Transmission Security Key (TSK), net sync date/time and net IDs). Mission Plan Data may be received over a variety of interfaces (e.g., 87-27, Ethernet, DS-101, DS-102, RS-232, USB, etc.).

3.2.4.1.1 (U) Receive Platform Group

(U//FOUO) A Platform Group is a user-defined item that represents a grouping of Platforms used for mission planning purposes. The NGLD-M Receive Platform Group capability provides the method to receive Platform Groups into the system. Platform Groups are received into the NGLD-M via the 87-27 and Tier 3 XML formats from iApp only. Platform Group may have one or more Platforms assigned to it.

3.2.4.1.2 (U) Receive Platform

(U//FOUO) A Platform is a user-defined item that represents a grouping of Devices used for mission planning purposes. The NGLD-M Receive Platform capability provides the method to receive Platforms into the system. Platforms are received into the NGLD-M via the 87-27 and

Tier 3 XML formats from CT3 compatible systems. Platform may have one or more Devices assigned to it.

3.2.4.1.3 (U) Receive Device

(U//FOUO) A Device is a user-defined instance of a particular device type supported by the NGLD-M used for mission planning purposes. The NGLD-M Receive Device capability provides the method to receive Devices into the system. Devices are received into the NGLD-M via the 87-27, Tier 3 XML formats or SINCGARS Loadsets from CT3 compatible systems. A Device may have one or more Keys/Key Tags/EP Data/Message Data/RCFs assigned to it.

3.2.4.1.4 (U) Receive Cryptographic Key/Key Tag

(U//FOUO) Cryptographic Key include encrypted and unencrypted symmetric and asymmetric keys. The NGLD-M Receive Cryptographic Key/Key Tag capability provides the method to receive encrypted and unencrypted symmetric and asymmetric keys in varied formats (e.g., 87-27, Tier 2 XML, Tier 3 XML, CMS package, SINCGARS Loadset over varied interfaces (e.g. Ethernet, DS-101, DS-102, RS-232, USB, etc.). Unencrypted symmetric keys may also be received from various legacy ECUs identified in Table 6 – (U) NGLD-M Legacy Device Key Sources. Key tags are created so that the user can perform last mile mission planning in advance of having the key material. The NGLD-M Receive Cryptographic Key/Key Tag capability also provides the method to receive Key Tags into the NGLD-M via the 87-27, Tier 3 XML formats from CT3 compatible systems.

3.2.4.1.5 (U) Receive EP Data

(U//FOUO) EP Data is considered non-cryptographic key content leverage as support an Electronic Counter Measure (ECM) resistant/frequency-hopping system used for jam resistance and to protect military radio traffic. EP Data includes Integrated COMSEC (ICOM) Hopsets, Non-ICOM Hopsets, Lockouts, Single Channel Frequency, Cue Frequency. The NGLD-M Receive EP Data capability provides the method to receive EP Data into the NGLD-M via the 87-27, Tier 3 XML formats and SINCGARS Loadsets from CT3 compatible systems.

3.2.4.1.6 (U) Receive Message Data

(U//FOUO) Message Data type is non-cryptographic key used with HAVEQUICK, Time of Day (TOD) from the Global Positioning System (GPS) system, Word of the Day (WOD) which serves as a key, and Network Identification (Net ID) on airborne devices for anti-jamming. Message Data are received into the NGLD-M via Tier 3 XML, 87-27 formatt from various systems. The NGLD-M Receive Message Data capability provides the method to receive Message Data into the NGLD-M via the 87-27 and Tier 3 XML formats from CT3 compatible systems.

3.2.4.1.7 (U) Receive Benign Fill (BF) Message

(U//FOUO) BF Messages are mainly used to support the F-22 and Advanced Extremely High Frequency (AEHF) benign keying, benign rekeying, and BF operations. These BF Messages include Credential Request (CREDRQ), ECU Response (ECURS), Application Key Material Delivery (AKDELIV), Key Replacement Delivery (KRDELIV). The NGLD-M Receive Benign Fill Message capability provides the method to receive Benign Fill Messages into the NGLD-M via the 87-27, Tier 3 XML formats from CT3 compatible systems.

3.2.4.1.8 (U) Receive SOI Data

(U//FOUO) SOI Data includes network groups, networks, time period, call signs, call words, cue and manual frequencies, suffixes, expanders, signs, countersigns, pyrotechnic and smoke signals, and quick references. The NGLD-M Receive SOI Data capability provides the method to receive SOI Data into the NGLD-M via the 87-27 format from CT3 compatible systems.

3.2.4.1.9 (U) Receive RCF

(U//FOUO) RCFs are created for specific networks for IP-based software defined radios. These RCFs are generated to configure a radio, and the NGLD-M provides the capability to download the correct RCFs to the radio. The NGLD-M Receive RCF capability provides the method to receive RCF into the NGLD-M via the 87-27, Tier 3 XML formats from CT3 compatible systems.

3.2.4.1.10 (U) Receive SINCGARS Loadset

(U//FOUO) SINCGARS loadset includes COMSEC key and Frequency Hoping (FH) data (hopset/lockout, Transmission Security Key (TSK), net sync date/time and net IDs). The NGLD-M Receive SINCGARS Loadset capability provides the method to receive SINCGARS Loadsets into the NGLD-M via the SINCGARS Loadset formats from systems such as ACES that generate SINCGARS Loadsets.

3.2.4.2 (U) Receive Non-Key Data

(U//FOUO) The NGLD-M Receive Non-Key Data capability provides the method to receive non-key data such as Audit Data, Certificates, CRLs, ARLs, ECU Commands, Health and Monitoring Data, Device Configuration Settings, Software/Firmware, Information Assurance Vulnerability Alert (IAVA) Patches received over various interfaces (e.g. Ethernet, USB interfaces, DS-101, etc.).

3.2.4.2.1 (U) Receive Audit Data

(U//FOUO) The NGLD-M Audit Data consists of important security events that are automatically captured and stored in the Audit Log. There are several external interfaces discussed in section 0 - 3.3 (U) System External Interface Requirements and its sub-sections that involve the sharing of this audit data with external systems to support operational requirements.

3.2.4.2.2 (U) Receive Certificate Products

(U//FOUO) Certificates are used in the NGLD-M to perform a variety of operations such as Transport Layer Security (TLS) establishment, authentication, signature verification services and decryption of CMS packages. The NGLD-M uses the IA certificate to authenticate into the KMI web services and uses the KE certificate to validate and unwrap products that are addressed to the NGLD-M. When the NGLD-M has both an IA(I) certificate and a KE(I) certificate, it is considered KMI-Aware. This awareness gives the NGLD-M the ability to request a Product Availability List (PAL) and subsequently obtain any product listed on the PAL. There are several external interfaces discussed in section 0 - 3.3 (U) System External Interface Requirements and its sub-sections that involve the sharing of this Certificate with external systems to support operational requirements.

3.2.4.2.3 (U) Receive CRLs

(U//FOUO) A CRL is a listing of the revocation of certificates that a given Certificate Authority (CA) issued. It is maintained by a CA that the NGLD-M trusts, and made available via various means, in the KMI case via the KMI Storefront. The CRL is used to ascertain the validity and revocation status of a certificate issued by the CA, used on the NGLD-M to check the validity of signed CMS packages by authenticating that the signer's certificate is valid and whenever certificates are used. There are several external interfaces discussed in section 0 - 3.3 (U) System External Interface Requirements and its sub-sections that involve the sharing of CRLs with external systems to support operational requirements.

3.2.4.2.4 (U) Receive ARLs

(U//FOUO) An ARL is a listing of revocation of CA certificates. It is maintained by the CA infrastructure that the NGLD-M trusts and made available via the same means as a CRL. NGLD-M is required to retain current copies of ARL and allocate storage space of at least 4MB per ARL. The ARL is used to ascertain the validity and revocation status of a CA certificate issued by the CA infrastructure, used on the NGLD-M to check the validity of signed CMS packages by authenticating that the signer's certificate is valid and whenever certificates are used. There are several external interfaces discussed in section 0 - 3.3 (U) System External Interface Requirements and its sub-sections that involve the sharing of ARLs with external systems to support operational requirements.

3.2.4.2.5 (U) Receive Device Configuration Settings

(U//FOUO) The Device Configuration Settings are information used to configure networking devices. The NGLD-M receive, stores and manages device configuration setting for Routers, switches, and end cryptographic units. There are several external interfaces discussed in section 0 - 3.3 (U) System External Interface Requirements and its sub-sections that involve the sharing of this Device Configuration Settings with external systems to support operational requirements.

3.2.4.2.6 (U) Receive Software/Firmware

(U//FOUO) The NGLD-M is required to support the ability to perform field upgrade and programming/reprogramming of the cryptographic software/firmware without needing to be returned to the factory, depot, or a trusted facility. NGLD-M software/firmware packages are signed by NSA and require PKI validation prior to use by an authorized user. Software/Firmware may also include Information Assurance Vulnerability Alerts (IAVA) patches. There are several external interfaces discussed in section 0 - 3.3 (U) System External Interface Requirements and its sub-sections that involve the sharing of this Software/Firmware with external systems to support operational requirements.

3.2.4.2.7 (U) Receive Health and Monitoring Data

(U//FOUO) The NGLD-M generates its own health and monitoring data that is used to ascertain the health of the device. This is covered in sections 0 3.2.9.1 (U) Health and Monitoring Data and the sharing of this data with external sources is covered under section 0 3.3.3 (U) Logical (Networked) External Interfaces. On the receiving-end, the NGLD-M also receives health and monitoring from other devices via the NGLD-M Last Mile API. This interface is covered in section 0 3.3.3.5 (U) NGLD-M Last Mile API (PUI:NLMA).

(U//FOUO) Health and Monitoring data is shared with the ACES/iApp workstation and other NGLD-M devices using the Last Mile API (LMA) to support near real-time analysis of the health of the NGLD-M device. The NGLD-M is able to share selected metrics / data through the iApp standard APIs to allow for analysis, visualization and informed decision making on the receiving end. This capability supports networked devices to allow in-band key management and health and status monitoring. With useful information from the NGLD-M, authorized users receive situational awareness for information including, but not limited to, battery life reading, Central Processing Unit (CPU)/Memory/Storage utilization, and Compromise Management of Cryptographic Products. The ”Receive” capability here allows health and monitoring data that is shared with the NGLD-M LMA services (as an intermediary) to be accepted / persisted for further eventual distribution to the destination.

3.2.4.3 (U) Receive Cryptographic Products and CMS Packages

(U//FOUO) The NGLD-M receives, stores and manages Cryptographic Products from a variety of sources (e.g., OTNK-Compliant storefronts, imports, etc.). These are often in the form of CMS Packages if received from KMI or an OTNK-Compliant Storefront as the source. A variety of Cryptographic Products supported by the NGLD-M can be retrieved from various sources. Cryptographic Products may include:

- Symmetric Products
- Asymmetric Products
- Certificate Products
- CRLs
- ARLs
- Software/Firmware
- Trust Anchor, etc.

3.2.5 (U) Storage

(U//FOUO) This section addresses any specific storage requirements for the NGLD-M. The NGLD-M provides memory for the storage and retrieval from storage of secure and non-secure data. Data includes cryptographic keys, non-key, and mission data. Secure data storage/retrieval involves the encryption/decryption of data. The NGLD-M provides RED/BLACK separation of stored data.

3.2.6 (U) Distributing

(U//FOUO) The NGLD-M Distributing capability provides the methods to distribute cryptographic key, non-cryptographic key content, and mission plan data to other systems.

(U//FOUO) Mission Plans data includes:

- Platform Groups, Platforms, Devices, Cryptographic Keys/Key Tags, HAVEQUCK (WOD, MWOD), frequency hopping data such as EP Data, Message data, benign fill messages, SOI data, Radio Configuration Files (RCFs), and SINCGARS Loadset may be received over a variety of interfaces (e.g., 87-27, Ethernet, DS-101, DS-102, RS-232, USB, etc.).

(U//FOUO) Cryptographic keys include:

- Encrypted and unencrypted symmetric and asymmetric keys in varied formats (e.g., 87-27, Tier 2 XML, Tier 3 XML, CMS package) may be obtained over varied interfaces (e.g. Ethernet, DS-101, DS-102, RS-232, USB, etc.).

(U//FOUO) Other non-key data includes:

- Certificates, CRLs, ARLs, ECU Commands, Health and Monitoring Data, Device Configuration Settings, Software/Firmware, Information Assurance Vulnerability Alert (IAVA) Patches received over various interfaces (e.g. Ethernet, USB interfaces, DS-101, etc.).

(U//FOUO) Distribution includes:

- Distributing cryptographic keys, mission plan data and non-key data to other systems.
- Issue keys to other systems.
- Fill keys into ECUs.

(U//FOUO) The NGLD-M provides the capability to distribute cryptographic keys and data, using the defined protocols and formats identified in Table 7 – (U) NGLD-M Distribution Data Types and Interfaces.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Type of Data	Interfaces	Data Format	Specification
Platform Group, Platform, Device Sets (i.e., non-key payload data)	DS-101/RS-232	87-27	CT3 ICD
Platform, Device Sets (i.e. non-key payload data)	DS-101/RS-232	87-27	CT3 ICD
Key Tag/Key Material	DS-101/RS-232, DS-102	87-27	CT3 ICD, EKMS-308
Key Material	CFDI (KYK-13)	CFDI	EKMS-308
Key Material	CFDI (KOI-18)	CFDI	EKMS-308
Key Material	CFDI (KYX-15), OTAT	CFDI	EKMS-308
Key Material (Benign Fill)	DS-101/RS-232	87-27	EKMS-217
Benign Fill Messages (non-key material)	DS-101/RS-232	87-27	EKMS-217
EP Data	DS-101/RS-232	87-27	CT3 ICD
Message Data	DS-101/RS-232	87-27	CT3 ICD
HAVEQUICK	DS-101/RS-232	87-27	CT3 ICD
SOI	DS-101/RS-232	87-27	CT3 ICD
Fill Device Audit Data	DS-101/RS-232, Ethernet, USB	87-27	EKMS-603B
ECU Commands	DS-101/RS-232	87-27	EKMS-308
CMS Package	Ethernet, USB, Wireless	CMS, Signed Data	OTNK
Certificates	Ethernet, USB, Wireless	X.509	OTNK
Certificate Revocation Lists (CRL)	Ethernet, USB, Wireless	X.509	OTNK
Authority Revocation Lists (ARL)	Ethernet, USB, Wireless	X.509	OTNK

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Type of Data	Interfaces	Data Format	Specification
Health and Monitoring Data	Ethernet	SNMP	SNMP, LMA API
Radio Configuration File (RCF)	USB, Ethernet, Wireless	Tier 3 XML	Tier 3 XML Schema
Device Configuration Settings	Ethernet, USB, Wireless	SNMP	SNMP, LMA API
Software/Firmware	Ethernet, USB, Wireless	CMS, Signed Data	OTNK

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Table 7 – (U) NGLD-M Distribution Data Types and Interfaces

3.2.6.1 (U) Cryptographic Key Issue

(U//FOUO) The NGLD-M Cryptographic Key Issue capability provides the methods to output cryptographic products to other systems where the recipient system is not the consumer. When Issuing products from the NGLD-M, the DS-100 tag, cryptographic content, and optional Text ID are included. Cryptographic Key are distributed from the NGLD-M via the 87-27 format to CT3 compatible systems. There are several external interfaces discussed in section 0 - 3.3(U) System External Interface Requirements and its sub-sections that involve the distribution of Cryptographic Key with external systems to support operational requirements.

(U//FOUO) Cryptographic keys are issued to other systems in two ways, via the Data Sharing capabilities where the products are assigned to a device as part of the mission planning data or unassigned.

3.2.6.2 (U) Cryptographic Key Fill

(U//FOUO) The NGLD-M Cryptographic Key Fill capability outputs cryptographic key material into the ECU where the recipient system is the consumer of the products. When filling products from the NGLD-M into the ECU, typically only the cryptographic key material is included in the key fill process. Although some ECUs require the key tag to go along with the key material also.

(U//FOUO) Table 8 – (U) NGLD-M Supported Equipment Profiles provides a listing of devices that are supported by the NGLD-M. The NGLD-M stores the profile information for supported devices and use the profile information when performing the key fill operations.

Table 8 – (U) NGLD-M Supported Equipment Profiles

ID	Device Type	Protocol
0	ARC-164	DS-102
1	ARC-190	DS-102
2	ARC-201	DS-102
3	ARC-201A	DS-102
4	ARC-210	DS-101
5	ARC-220	DS-101
6	ARC-222	DS-102
7	C-11561	DS-102
8	CSZ-1A	DS-102
9	GOE-2	DS-102
10	NOT USED	
11	GPS-PLGR	DS-102
12	GRC-171	DS-102
13	HGX-82	DS-102
14	NTDR	DS-101
15	KG-194A	DS-102
16	KGV-23	DS-101
17	NOT USED	

ID	Device Type	Protocol
18	KG-40A	DS-102
19	KG-45	DS-102
20	NOT USED	
21	KG66-A	DS-102
22	KG-81	DS-102
23	NOT USED	
24	NOT USED	
25	KG94-A	DS-102
26	KG-95	DS-102
27	KGR-66	DS-102
28	KGV-11A	DS-102
29	KGV-13	DS-102
30	NOT USED	
31	KGV-68	DS-102
32	KGV-8	DS-102
33	KGV-8B	DS-101
34	KGV-9	DS-102
35	KI-36	DS-102
36	KIR-1C	DS-102
37	KIT-1C	DS-102
38	NOT USED	
39	NOT USED	
40	KIV-7	DS-101/DS-102
41	NOT USED	
42	KY-68	DS-102
43	KY-90	DS-102
44	KYV-5	DS-102
45	NOT USED	
46	KG-84A	DS-102
47	KG-84C	DS-102
48	MO-3	DS-102
49	NOT USED	
50	NOT USED	
51	KYK-13	DS-102

ID	Device Type	Protocol
52	KYX-15	DS-102
53	NOT USED	
54	KY-57	DS-102
55	KY-58	DS-102
56	KY-67	DS-102
57	KG-83	DS-102
58	HGX-83	DS-102
59	KGX-93	DS-102
60	KGX-93A	DS-102
61	KW46-OT	DS-102
62	KY-100	DS-102
63	RT-1523	DS-102
64	RT-1523B	DS-102
65	NOT USED	
66	NOT USED	
67	KW-46	DS-102
68	KOK-22 (KP)	DS-101
69	KOK-13	DS-102
70	MX-18290	DS-102
71	DTD/SDS/NGLD-M	DS-101
72	UNKNOWN	DS-101/DS-102/RS-232
73	PSC-11	DS-102/RS-232
74	PSC-5	DS-102
75	WORKSTATIONS	
76	RT-1794	DS-101
77	KY-99A	DS-101
78	TSC-154	DS-101/DS-102
79	ARC-234	DS-101/DS-102
80	PSC-5D	DS-101
81	KS-10	DS-102
82	ARC-231	DS-101
83	PSC-5C	DS-101
84	NOT USED	

ID	Device Type	Protocol
85	GPS MAGR	DS-102
86	KG-75	DS-101
87	KG-175	DS-101
88	NOT USED	
89	ARC-201D	DS-102
90	RCUT	RS-232
91	KOV-17	DS-101
92	APX-123/UPX-41	DS-101
93	KIV-77	DS-101
94	KIV-78	DS-101
95	KIV-7M	DS-101/DS-102
96	KIV-19M	DS-101/DS-102
97	KG-235	DS-101
98	KG-240	DS-101
99	KG-250/250X/255	DS-101
100	CSEL HHR	RS-232
101	KIV-6	DS-102
102	APX-118	DS-102
103	NOT USED	
104	KIV-114	DS-102
105	KIV-119	DS-102
106	NOT USED	
107	NOT USED	
108	KGV-72	DS-101
109	MIDS JTRS	DS-101
110	KOV-20	DS-101
111	NOT USED	
112	NOT USED	
113	MATT BLOCK 0/1	DS-102
114	MATT BLOCK 2/3	DS-102
115	B-MATT	DS-102
116	AN/CYZ-24	DS-102
117	KGR-96	DS-102
118	ENTR EDM Block1	DS-102
119	JTT-B	DS-102
120	CTT	DS-102
121	JTT SR	DS-102
122	NOT USED	
123	NOT USED	
124	NOT USED	
125	IMS CSCU	RS-232
126	IMS CST	RS-232
127	IMS DM	RS-232
128	GPS-DAGR	DS-101/RS-232
129	PRC-148	DS-102
130	PIK	RS-232
131	FAB-T DSM	RS-232
132	FAB-T FCS	RS-232
133	KG-333/KGV-361	DS-101
134	NOT USED	
135	KOK-23	DS-101/RS-232
136	AFCPT	DS-102
137	NOT USED	
138	KOV-222	DS-101
139	SSNT-SDB2	RS-232
140	SCWDL-SDB2	RS-232
141	SCWDL	RS-232
142	NOT USED	
143	ENTR USB	DS-101
144	NOT USED	
145	NOT USED	
146	JIPM	DS-101
147	MYK-16(17)B	DS-101
148	NOT USED	
149	KI-17	DS-101
150	MYK-7	DS-102
151	KG-144	DS-102
152	NOT USED	

ID	Device Type	Protocol
153	AN/PRC-154	DS-101
154	KGV-136	DS-101
155	NOT USED	
156	TWCS	RS-232
157	NOT USED	
158	APX-124	DS-101
159	TDSPP	RS-232
160	AN/PRC-155	DS-101
161	NOT USED	
162	LINK16CM	DS-101
163	VGI	RS-232
164	DGNS	DS-102
165	EGI	DS-102
166	RT-1799	DS-101/DS-102
167	EPLRS Modern	DS-101
168	L16SYS	DS-101
169	ARC-234M	DS-101
170	KY-57M	DS-101
171	KY-58M	DS-101
172	KY-99M	DS-101
173	KY-100M	DS-101
174	KYV-5M	DS-101
175	NOT USED	
176	ARC-210M	DS-101
177	NOT USED	
178	PRC-117G	DS-101/DS-102
179	PRC-152A	DS-101/DS-102
180	SideHat	DS-101
181	NOT USED	
182	SRW Applique	DS-101/DS-102
183	IFDL	DS-101
184	TTNT	DS-101
185	ARC-231M	
186	SMC	DS-101
187	PRC-118	
188	MDL-LRASM	RS-232
189	NOT USED	
190	GASNT	
191	ADTS/DAR-400ES	
192	R-2674(C)/A	
193	JMPS-GPS	
194	AN/VRC-118	
TBD	AN/VRC-118 MNVR	
196	GPS-MCODE	
TBD	AN/PRC-117 MUOS	
198	SDB-II	
TBD	FAB-T/KOV-442/443	
TBD	JMPS-GPS	

3.2.6.2.1 (U) Unassigned Cryptographic Key Fill

(U//FOUO) The NGLD-M Unassigned Cryptographic Key Fill capability provides the method to fill keys into an ECU. Since the keys are not first assigned to an ECU, the target ECU is selected from a list of supported ECUs by the user during the fill operation.

3.2.6.2.2 (U) Platform-Based Cryptographic Key Fill

(U//FOUO) The NGLD-M Platform-based Cryptographic Key Fill capability provides the method to fill keys into one or more ECUs that are assigned to a Platform. The cryptographic key fill process is initiated by selecting a Platform and process through the key fill process for each ECU assigned under that Platform. In the case where the ECUs are on a specified computer bus, a single cryptographic key fill operation from the Platform level will fill all cryptographic keys to the ECUs automatically. If the ECUs that are assigned to the selected Platform are not connected on a computer bus, the user will connect and fill one ECU at a time. Each ECU may have one or more Keys/Key Tags/EP Data/Message Data/RCFs assigned to it.

3.2.6.2.3 (U) Equipment-Based Cryptographic Key Fill

(U//FOUO) The NGLD-M Equipment-Based Cryptographic Key Fill capability provides the method to fill keys into a selected ECU. The cryptographic key fill process is initiated by selecting an ECU and all ECU fill locations that have keys assigned will be filled one by one automatically. Each ECU may have one or more Keys/Key Tags/EP Data/Message Data/RCFs assigned to it.

3.2.6.3 (U) Distribute Mission Plan Data

(U//FOUO) The NGLD-M Transmit Mission Plan Data capability provides the method to distribute cryptographic key, mission data, and non-key data from the NGLD-M persistence store to other systems. For cryptographic keys, the DS-100 tag as well as related information unique to the CT3 such as effective date, expiration date, data type, and decryptor location are also included. There are several external interfaces discussed in section 0 - 3.3 (U) System External Interface Requirements and its sub-sections that involve the sharing of data with external systems to support operational requirements.

3.2.6.3.1 (U) Distribute Platform Group

(U//FOUO) A Platform Group is a user-defined item that represents a grouping of Platforms. The NGLD-M Distribute Platform Group capability provides the method to distribute Platform Groups to other CT3 compatible systems that support Platform Group. Platform Groups are distributed from the NGLD-M via the 87-27 format from iApp. Platform Group may have one or more Platforms assigned to it.

3.2.6.3.2 (U) Distribute Platform

(U//FOUO) A Platform is a user-defined item that represents a grouping of Devices. The NGLD-M Distribute Platform capability provides the method to distribute Platforms to other systems. Platforms are distributed from the NGLD-M via the 87-27 format to CT3 compatible systems. Platform may have one or more Devices assigned to it.

3.2.6.3.3 (U) Distribute Device

(U//FOUO) A Device is a user-defined instance of a particular device type supported by the NGLD-M. The NGLD-M Distribute Device capability provides the method to distribute Devices to other systems. Devices are distributed from the NGLD-M via the 87-27 format to CT3 compatible systems. A Device may have one or more Keys/Key Tags/EP Data/Message Data/RCFs assigned to it.

3.2.6.3.4 (U) Distribute Cryptographic Key/Key Tag

(U//FOUO) Distribution of Cryptographic Key is covered under the Cryptographic Key Issue section of this document. The NGLD-M Distribute Cryptographic Key/Key Tag capability also provides the method to distribute key tags. Key tags are created so that the user can perform last mile mission planning in advance of having the key material. Cryptographic Key Tags are distributed from the NGLD-M via the 87-27 format to CT3 compatible systems.

3.2.6.3.5 (U) Distribute EP Data

(U//FOUO) EP data is considered non-cryptographic key content leverage as support an Electronic Counter Measure (ECM) resistant/frequency-hopping system used for jam resistance and to protect military radio traffic. EP Data includes Integrated COMSEC (ICOM) Hopsets, Non-ICOM Hopsets, Lockouts, Single Channel Frequency, Cue Frequency. EP Data are distribute from the NGLD-M via 87-27 format from various systems. EP Data are distributed from the NGLD-M via the 87-27 format to CT3 compatible systems. EP Data can also be filled into ECUs that support EP Data.

3.2.6.3.6 (U) Distribute Message Data

(U//FOUO) Message Data type is non-cryptographic key used with HAVEQUICK, Time of Day (TOD) from the Global Positioning System (GPS) system, Word of the Day (WOD) which serves as a key, and Network Identification (Net ID) on airborne devices for anti-jamming. Message Data are transmit from the NGLD-M via 87-27 format to CT3 compatible systems. Message Data can also be filled into ECUs that support Message Data.

3.2.6.3.7 (U) Distribute Benign Fill (BF) Message

(U//FOUO) BF Messages are mainly used to support the F-22 and Advanced Extremely High Frequency (AEHF) benign keying, benign rekeying, and BF operations. These BF Messages include Credential Request (CREDRQ), ECU Response (ECURS), Application Key Material Delivery (AKDELIV), Key Replacement Delivery (KRDELIV). The NGLD-M Distribute Benign Fill Message capability provides the method to distribute Benign Fill Messages from the NGLD-M via the 87-27 format to CT3 compatible systems. BF Messages can also be filled into ECUs that support BF Messages.

3.2.6.3.8 (U) Distribute SOI Data

(U//FOUO) SOI Data includes network groups, networks, time period, call signs, call words, cue and manual frequencies, suffixes, expanders, signs, countersigns, pyrotechnic and smoke signals, and quick references. The NGLD-M Distribute SOI Data capability provides the method to distribute SOI Data from the NGLD-M via the 87-27 format from CT3 compatible systems.

3.2.6.3.9 (U) Distribute RCF

(U//FOUO) RCFs are created for specific networks for IP-based software defined radios. These RCFs are generated to configure a radio, and the NGLD-M provides the capability to download the correct RCFs to the radio. The NGLD-M Distribute RCF capability provides the method to distribute RCFs from the NGLD-M via the 87-27 format to CT3 compatible systems. RCFs can also be filled into ECUs that support RCFs.

3.2.6.3.410 (U) Distribute Device Configuration Settings

(U) This section covers the requirements for the distribution of device configuration settings. Device Configuration Settings contain information used to configure networking devices. The NGLD-M receives, stores and manages device configuration setting for routers, switches, and ECUs.

3.2.6.4 (U) Distribute CRLs

(U//FOUO) CRLs are a focal part of the PKI system. The NGLD-M possesses several certificates from KMI. The NGLD-M performs signature verification on products received from KMI or other trusted sources. The NGLD-M also allows connections and establishes connections with external interfaces. These activities involve certificate revocation list checks to ensure the certificate utilized externally is not on the revoked list. NGLD-M has the ability to distribute/share these certificates in its role as an intermediary. There are several external interfaces discussed in section 0 - 3.3 (U) System External Interface Requirements and its sub-sections that involve the sharing of CRLs with external systems to support operational requirements.

3.2.6.5 (U) Distribute Audit Data

(U//FOUO) NGLD-M manages its internal (fill) device audit data. There are several external interfaces discussed in section 0 - 3.3 (U) System External Interface Requirements and its sub-sections that involve the sharing of this audit data with external systems to support operational requirements. There are several external interfaces discussed in section 0 - 3.3 (U) System External Interface Requirements and its sub-sections that involve the sharing of this audit data over network with external systems to support operational requirements.

3.2.6.6 (U) Distribute CMS Packages

(U//FOUO) The majority of products are packaged by KMI in CMS format in accordance with KMI's OTNK specifications. The NGLD-M can manage CMS packages wrapped for the NGLD-M itself (High Assurance or Medium Assurance PKI), or CMS packages that are wrapped for externally supported KMI-Aware Devices. There are several external interfaces discussed in section 0 - 3.3 (U) System External Interface Requirements and its sub-sections that involve the sharing of this CMS Packages with external systems to support operational requirements.

3.2.6.7 (U) Distribute Certificate Products

(U//FOUO) NGLD-M manages various certificate products in support of the KMI PKI implementation, both High Assurance and Medium Assurance. This involves managing certificates and trust anchors from KMI for the NGLD-M device as well as distributing to other ECUs. The NGLD-M manages Certificate Signing Requests (CSRs) for the NGLD-M as well as external KMI-Aware devices it supports in the role of an intermediary. There are several external interfaces discussed in section 0 - 3.3 (U) System External Interface Requirements and its sub-sections that involve the sharing of Certificate Products with external systems to support operational requirements.

3.2.6.8 (U) Distribute Health and Monitoring Data

(U//FOUO) The NGLD-M generates health and monitoring data that is then distributed externally for assistance with analysis, management and decision making. The requirements for the externally-supported sources this data is sent to can be found in section 0 3.3.3.4 (U) ACES/iApp Last Mile API (PUI:ILMA). This section captures the requirement establishing the need to send this data.

(U//FOUO) NGLD-M Health Status operations allow the NGLD-M to monitor the health and security of the hardware, software, and sensitive data. Health Status operations provide assurance that security services are operating as intended and address hardware, software, sensitive data, security critical functions, power states, power supply availability, configuration change, malfunction detection, and maintain cognizance of data transmission over external interfaces in support of power off timing. The collection of pertinent metrics allow the health and status of the NGLD-M to be assessed.

(U//FOUO) Health and Monitoring data is shared with the iApp workstation to support near real-time analysis of the health of the NGLD-M device. When network-monitoring technologies gather information from the NGLD-M, the NGLD-M is required to ensure the integrity of the exchange of health status data. The NGLD-M is able to share selected metrics / data through the iApp standard APIs to allow for analysis, visualization and informed decision making on the receiving end. This capability supports networked devices to allow in-band key management and health and status monitoring. With useful information from the NGLD-M, authorized users receive situational awareness for information including, but not limited to, battery life reading, CPU/Memory/Storage utilization, and Compromise Management of Cryptographic Products.

3.2.6.9 (U) Distribute ARLs

(U//FOUO) An ARL is a listing of revocation of CA certificates. It is maintained by the CA infrastructure that the NGLD-M trusts and made available via the same means as a CRL. NGLD-M retains current copies of ARLs and allocates adequate storage space. The ARL is used to ascertain the validity and revocation status of a CA certificate issued by the CA infrastructure and to check the validity of signed CMS packages by authenticating that the signer's certificate is valid. The NGLD-M can distribute ARL data to support operations.

3.2.7 (U) Cryptography

(U//FOUO) The NGLD-M supports High Assurance and Medium Assurance cryptographic operation modes. After Power-Up succeeds, the NGLD-M can enter Medium Assurance mode for an authorized user. An authorized NGLD-M user can utilize High Assurance cryptographic operations after a CIK is inserted and passes validation checks. After the cryptographic subsystem is ignited then High Assurance algorithms may be usable along with Medium Assurance algorithms so long as security validation rules are met.

(U//FOUO) All NGLD-M cryptographic operations include the use of Algorithms for encryption, decryption, and validation operations, key pair management for the NGLD-M Medium and High Assurance identities within the NSA KMI PKI, IPSEC channel operations for communication with peer NGLD-M, digital signature services, data at rest requirements, decrypting software distribution, key management support, programmability, Cryptographic Software/Firmware loading and storage, level of security and classification behaviors, and Audit behavior and maintenance.

3.2.7.1 (U) Algorithms

(U//FOUO) The NGLD-M supports algorithms that are used for encryption, decryption, and validation operations across multiple cryptographic scenarios and in support of High Assurance or Medium Assurance operations. Table 9 provides a list of algorithms required as well as amplifying information about relevant functionality tied to algorithm uses in the NGLD-M. The handling of these algorithms within the NGLD-M is sensitive and is subject to routines for their validation and activation prior to use to ensure correct function prior to being considered for use.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Function/Use Case	Requirement	Required Algorithms	Acceptable	Notes
TrKEK Encrypt/Decrypt	EKMS Compatibility	ACCORDION 1.3		Required for support of legacy key distribution methods. See OTNK20.8
Transport Layer Security (TLS) for KMI	KMI Compatibility	AES-256 (GCM), SHA-256/384		See OTNK 3.1 section 7 requirements: OTK116, OTNK148
KMI Key Agreement	KMI Compatibility	ECDH-384, SPONDULIX-S		Both ECDH and SPONDULIX-S are supported in KMI CI-2 Spin 3 (see OTNK specification for additional detail)
KMI Key Derivation/Message Digest	KMI Compatibility	SHA-384		Requirement: OTNK20.1, OTNK20.6
KMI Black Key Wrap	KMI Compatibility	AES Key Wrap	ACCORDION 3.0 (for future growth)	Requirement: OTNK20.5, OTNK20.7
KMI Signatures	KMI Compatibility	ECDSA-384		Requirement: OTNK20.2
Internal Key Wrap	Vendor Implementation	See column D (Acceptable)	AES Key Wrap, ACCORDION 1.3, ACCORDION 3.0	All are NSA-approved algorithms for internal key wrap (see OTNK specification for additional detail)
Symmetric Encryption for Data at Rest (DAR)	Vendor Implementation; TS Data at Rest		AES-256 or MEDLEY	
Security Software Confidentiality	Vendor Implementation	WATARI	WATARI	
Security Software Signature (When software is updated, NSA signs it with the listed algorithm. NGLD-M receives the update and validates the signature)	Vendor Implementation		KM-TG-0002-96 or KM-TG-0003-03 upgradeable to SILVER LINING	KM-TG* is the only algorithm NSA currently supports for software signature. NSA CACMB prefers to see a path to SILVER LINING because the useful life of KM-TG* is limited.
Non-Security Software Confidentiality (This is encryption of non-crypto software)	Vendor Implementation		AES, WATARI, MEDLEY	WATARI may be preferred in order to be compatible with future KMI software distribution approach in KMI CI-3.
Non-Security Software Signature (This is signature for non-crypto software)	Vendor Implementation		ECDSA, RSA, key based hashes	The combination of SHA-384/ECDSA-384 is recommended to be compatible with future KMI software distribution approach.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Table 9 – (U) List of Algorithms

3.2.7.2 (U) Key Pair Management

(U//FOUO) The cryptographic NGLD-M supports the use of High Assurance and Medium Assurance certificates. After a valid and approved external security stimulus that authorizes High Assurance cryptographic processing is recognized and validated an authorized user may use High Assurance and Medium Assurance certificates known activated cryptographic subsystem. In the absence of an activated High Assurance cryptographic subsystem, the NGLD-M may use Medium Assurance certificates for all available system operations.

(U//FOUO) Key Pair Management provides requirements for activating public/private key pairs, certificate signing requests, trust anchor and certificate authority certificates, CRLs, and ARLs.

3.2.7.3 (U) Internet Protocol Security (IPSEC)

(U//FOUO) The NGLD-M supports IPSEC communications in order to provide a guaranteed secure channel between instances of NGLD-M. KMI High Assurance IA(M) certificates are used for security association establishment of IPSEC tunnels. During the use of IPSEC channel usage, KMI certificate authority materials (e.g., trust anchors, certificate authority certificates, CRLs, ARLs) are used in validation routines. After valid IPSEC tunnels are established TLS mutually authenticated communications are used between the authorized systems to provide an additional layer of authenticated and encrypted protection; enabling OTNK and LMA. For 4etails on IPSEC algorithms please see section 0 - 3.2.7.1 (U) Algorithms.

3.2.7.4 (U) Digital Signature Services

(U//FOUO) NGLD-M performs digital signature verification of signed products that include, but are not limited to, CMS packages, software and firmware, certificates, CRL/ARL using authorized algorithms (see section 0 - 3.2.7.1 (U) Algorithms). In the event of re-wrapping products, the NGLD-M applies a digital signature.

3.2.7.5 (U) Data at Rest Security

(U//FOUO) The NGLD-M provides built-in data at rest encryption, decryption, and integrity validation mechanisms for data protection up to a level of Top Secret; in accordance with NSA IASRD tailored for NGLD-M and RMF.

3.2.7.6 (U) Decrypting Software Distribution

(U//FOUO) The NGLD-M provides built-in High Assurance software distribution validation and decryption features. This feature is used when NGLD-M undergoes maintenance and receives authentic and encrypted update package(s).

3.2.7.7 (U) Cryptographic Key Storage

(U//FOUO) The NGLD-M provides storage for its High Assurance and Medium Assurance key materials as well as the key material that is destined for ECUs. Key material that is stored will contain identifying and amplifying information and this information is required to be bound and stored with the key material.

3.2.7.8 (U) Rollover

(U//FOUO) The NGLD-M provides capability for detecting when rollover events should occur, in the case where key effective dates are set to expire and the next key (known by its effective date) can be logically chosen. The NGLD-M can be commanded by the user to perform a rollover from one TrKEK key to another and it may be configurable to allow for limited automated behavior to perform simple rollover operations where agreement on effective dates are reached by the key provider and the NGLD-M authorized user. The simple automated rollover routine allows for rollover to the next key when the predecessor key reaches the end of the effective date (i.e., expires). Expired keys are not automatically deleted and require intervention by an authorized user to adjudicate deletion.

3.2.7.9 (U) Software/Firmware Programmability

(U//FOUO) The NGLD-M is software/firmware programmable and re-programmable when directed by authorized users. NGLD-M classified configuration/programming data is required to be saved in encrypted form when the NGLD-M enters an operational state and will decrypt and load valid configuration/programming data for operational use when directed.

3.2.7.10 (U) Cryptographic Software/Firmware Loading

(U//FOUO) The NGLD-M supports the ability to perform field upgrade and programming/reprogramming of the cryptographic software/firmware without needing to be returned to the factory, depot, or a trusted facility. NGLD-M software/firmware packages are signed by NSA and require PKI validation prior to use by an authorized user. Any invalid packages are not to be used and reports of the failure are to be captured. Information about versioning of software/firmware is retained for viewing. NGLD-M also includes privileging for the ability to rollback to a previously valid loaded version of the Software/Firmware. The NGLD-M is also required to provide a valid user with the ability to overwrite a previous version of stored cryptographic software/firmware.

3.2.7.11 (U) Cryptographic Software/Firmware Storage

(U//FOUO) The NGLD-M provides functionality to encrypt, decrypt, and validate cryptographic software/firmware for storage. In addition, retention of multiple boot images of the encrypted cryptographic software/firmware is required.

3.2.7.12 (U) Level of Security and Classification

(U//FOUO) The NGLD-M performs cryptographic operations using cryptographic key material that is classified as Unclassified, Confidential, Secret, or Top Secret. NGLD-M is required to prevent a cryptographic service from running if the cryptographic service is of a higher classification than the current cryptographic classification level of the NGLD-M.

3.2.7.13 (U) Unclassified Handling

(U//FOUO) The NGLD-M provides the capability to be rendered Unclassified or Unclassified Controlled Cryptographic Item (CCI) when in the Powered Off state. In addition, NGLD-M processing from an Unclassified CCI state to a classified operational state is also required.

3.2.7.14 (U) Audit

(U//FOUO) The NGLD-M is required to support Audit capabilities in accordance with NSA NGLD-M Tailored IASRD and RMF. Audit information reporting will be available to the user upon request, and the device is required to maintain a minimum of 8 MB of internal storage for the use of Audit Event storage. In the event the audit storage space reaches maximum capacity, overwrite of the oldest Audit Events is required, but any overwrite occurrences are required to be reported as an audit event.

3.2.8 (U) Discrete Operation

(U//FOUO) The NGLD-M will provide a Discrete Operation mode. This mode allows for the device to perform a limited set of extended processes while being locked (e.g., software/firmware downloads, large data downloads, transfers between NGLD-Ms, provide PDE and LMA services) without a human user required to be interactively logged in during the operation. The device does not allow any additional operations to be performed while in

Discrete Operation mode and will display limited informational status of the operations that are taking place.

3.2.9 (U) Built-In Test and Health Status

(U//FOUO) The NGLD-M is required to execute Built-In-Test (BIT) in accordance with NSA NGLD-M tailored IASRD. BIT is executed during power-on and restart, periodically while powered on, after malfunction, and can be initiated by an authenticated user on demand. BIT is used to validate the correctness of functionality of hardware, firmware, and software components. These components include processors, volatile memory, non-volatile memory, internal control buses, internal data busses, interfaces, firmware, software, cryptographic algorithms. When BIT is in process, the user can discern that BIT is in process and is able to determine the success of failure of BIT results. Components that fail BIT must be isolated and BIT failure information is made available to authenticated users. BIT failures are also persisted as non-editable log data. The user can discern the criticality of the failed component and practical steps to remedy the issue, caused by failures, are displayed to the user.

3.2.9.1 (U) Health and Monitoring Data

(U//FOUO) NGLD-M Health Status operations are also required to monitor the health and security of the hardware, software, and sensitive data. Health Status operations are required to provide assurance that security services are operating as intended and address hardware, software, sensitive data, security critical functions, power states, power supply availability, configuration change, malfunction detection, and maintain cognizance of data transmission over external interfaces in support of power off timing. When network-monitoring technologies gather information from the NGLD-M, the NGLD-M is required to ensure the integrity of the exchange of health status data.

(U//FOUO) Health and Monitoring data is shared with the iApp workstation to support near real-time analysis of the health of the NGLD-M device. The NGLD-M is able to share selected metrics / data through the iApp standard APIs to allow for analysis, visualization and informed decision making on the receiving end. This capability supports networked devices to allow in-band key management and health and status monitoring. With useful information from the NGLD-M, authorized users receive situational awareness for information including, but not limited to, battery life reading, CPU/Memory/Storage utilization, and Compromise Management of Cryptographic Products.

3.2.10 (U) Alarm

(U//FOUO) The NGLD-M provides Alarm determination and issuance in accordance with NSA tailored IASRD requirements. When Alarm states are detected associated data is displayed in accordance with the authorization level of the users of the system as well as in non-editable logs. Source of Alarms may include activities attributable to CIK removal, BIT failures, events described in IASRD or RMF non-functional requirements, and others.

3.2.11 (U) Configuration Management

(U//FOUO) The NGLD-M utilizes network interfaces to configure or reconfigure other network devices with an initial configuration to allow over-the-network management. This simple configuration activity must be done within five minutes or less. The distant end network devices include routers, switches, and end cryptographic units.

3.2.12 (U) Zeroization

(U//FOUO) Various actions and conditions can initiate and trigger the zeroization process on the NGLD-M during any mode of operation. The NGLD-M supports user initiated zeroization through the manipulation of physical and software buttons as well as via triggered events detected and directed by the system.

(U//FOUO) There are multiple types of zeroization, to include selective zeroization, recoverable zeroization, destructive zeroization, and passive zeroization.

- **Selective Zeroization:** Selective zeroization is a process through which the NGLD-M selectively zeroizes one or more keys within the NGLD-M cryptographic subsystem. Selective zeroization applies to both "working" key material and key material in persistent storage.
- **Recoverable Zeroization:** Recoverable zeroization is a process through which all application key material within the NGLD-M crypto is zeroized, but the NGLD-M crypto-specific key material is left intact. The NGLD-M crypto-specific key material is key material that would be used to fill new application key material into the crypto. The NGLD-M crypto does not have to be reinitialized after a recoverable zeroization has been done. Recoverable zeroization occurs when the Zeroize button is purposefully pressed, with power applied, when the external battery is removed, for a set amount of time, and when an SSO enters the password incorrectly ten (10) times.
- **Destructive Zeroization**: Destructive zeroization is a process through which the NGLD-M is zeroized and all key material within the NGLD-M crypto is rendered unrecoverable. The NGLD-M crypto is required to be reinitialized after a destructive zeroization has been done. Destructive zeroization is triggered when a quadrant event is detected.
- **Passive Zeroization:** During passive zeroization, working Random Access Memory (RAM) memory is cleared by removing power to the memory. The Passive zeroization occurs in the shortest time possible. Passive zeroization occurs during power-down.

3.2.13 (U) Multi-Domain Support

(U//FOUO) The NGLD-M provides multi-domain support, one domain at a time but it is not a cross-domain solution. For information on physical external interfaces that connect to networks of varied classification, please see section 3.3.2 (U) Physical External Interfaces.

3.2.14 (U) ECU-Profile Management

(U//FOUO) New ECUs requiring fill device support are introduced occasionally. In order to avoid a software/firmware update and potentially some level of recertification activity for the device in order to accommodate the new ECU profile, the NGLD-M ECU Profile Management capability is introduced. This capability is intended to support the instantiation of new ECU profiles on the NGLD-M dynamically. The primary path of this operation is to have an external workstation component (e.g. ACES/iApp) capable of generating trusted ECU profile data for ingest into an NGLD-M. Upon receipt, the NGLD-M will then be capable of importing / receiving, persisting and processing this data. The alternate path of the operation is to support a workflow for the generation of a new profile on the NGLD-M device on demand.

3.2.15 (U) Legacy Interfaces/Backward Compatibility

(U//FOUO) One of the most important roles of the NGLD-M is to facilitate the transition of cryptographic key management from the legacy system into the KMI environment. The NGLD-M accomplishes this important role by providing supports for legacy functions, legacy data formats, and legacy external interfaces when receiving/distributing cryptographic key material and mission data from legacy systems, managing legacy ECU profiles and issuing and filling legacy ECUs until all systems and ECUs have transitioned to the KMI environment.

(U//FOUO) Another legacy function and interface is supporting the filling the DTD TrKEK into another fill device so that the fill device can decrypting DTD TrKEK encrypted keys when issuing keys or filling ECUs. The NGLD-M also provides the capability to initiate low level commands to legacy ECUs. The Commands include: Set Station Address, Set Station ID, Zeroize All, Zeroize EEPROM, Zeroize All RAM, and Zeroize RAM to the following ECUs: ADDI, JTIDS, KGV-23, RT-1794, MIDS JTRS, Mode 5 IFF, LINK16CM, IFDL and TTN devices.

3.2.16 (U) Accessory

(U//FOUO) The NGLD-M uses several external accessories to support it operational goals. This set of accessories includes supporting battery recharging, network access, data exchanges, and cryptographic key operations. The NGLD-M performs these operations using a power accessory/cable, Ethernet cable, USB cable, and six pin audio fill cable.

3.2.17 (U) Power-Down

(U//FOUO) The NGLD-M is required to power-down when triggered by a user or automated function. The user can trigger power-down directly via the timed toggling of a physical key press of a determined length of time (e.g., 3 seconds) and/or via interactive software means. When power-down occurs, the working memory of the system must be passively zeroized.

(U//FOUO) Automated functions that trigger power-down include the passive zeroization event, Anti-TAMPER event, critical alarm event (including, but not limited to, low battery availability), and after an inactivity threshold timeout has been met. An inactivity threshold is reached when there is no touch screen input, button presses, USB attached device input (e.g., mouse, keyboard), and any network traffic detected within the threshold time limit. The inactivity threshold timeout event is configurable by an authorized user and must come pre-loaded with a default setting.

3.2.18 (U) Seeking Help

(U//FOUO) The NGLD-M provides the authorized user with help information, to include a quick reference guide (QRG) and a list of helpdesk contact details.

3.2.19 (U) General User Interface

(U//FOUO) The NGLD-M shall strive to provide the best possible user experience (UX) on the device through the strategic design of the user interface that makes the user's job simple and more efficient. The user interface may require an iterative design process where prototypes are developed and presented to the user communities for feedback. The user interface components of the NGLD-M may include icon-based navigation, home page, customization and configuration of the UI and favorites, simple workflows, display of current status, meaningful error messages, etc.

3.3 (U) System External Interface Requirements

(U//FOUO) The NGLD-M system external interface requirements are categorized according to the physical or logical attributes of each.

(U//FOUO) Physical External Interfaces, described in section 0 address the requirements for the physical subcomponents that make up the NGLD-M as a hardware product, which can be directly used by privileged users. The physical subcomponents include: Display, Keypad, Fill Port, CIK and interface, USB, Ethernet (RJ45), Wireless, and Operational Battery.

(U//FOUO) Logical External Interfaces, described in 0 - 3.3.3 (U) Logical (Networked) External Interfaces, address the requirements for the data exchanges that occur with external systems that are not enclosed in the hardware of the NGLD-M and are generally distant to the NGLD-M.

3.3.1 (U) Interface Identification and Diagrams

(U//FOUO) The NGLD-M contains physical external interfaces that are used to interact with external interfacing entities; such as privileged users and/or disparate systems in both Medium Assurance and High Assurance modes. Figure 7 – (U) NGLD-M Physical External Interfaces provides an overview of the NGLD-M physical external interfaces along with entity information known to interface with the NGLD-M. The NGLD-M physical interfaces include: Display (touchscreen), Keypad, Fill Port, CIK, USB, Ethernet (RJ45), Wireless, and Operational Battery. See Table 10 -(U) NGLD-M External Interfaces and Medium and High Assurance mode characteristics by Interface

3.3.2 (U) Physical External Interfaces for additional physical subcomponent details and 0 3.3.3 (U) Logical (Networked) External Interfaces for additional information on external interfaces used by NGLD-M.

(U//FOUO) NGLD-M can operate in Medium Assurance and High Assurance modes and a result of these modes is manifest in the active or not active state of its interfaces and the types of data that can be shared across those interfaces and with whom. Table 10 -(U) NGLD-M External Interfaces and Medium and High Assurance mode characteristics by Interface provides characteristics of the NGLD-Ms physical interfaces, their use in logical external communications, and the known data types that are associated with the interfaces when operating in particular mode.

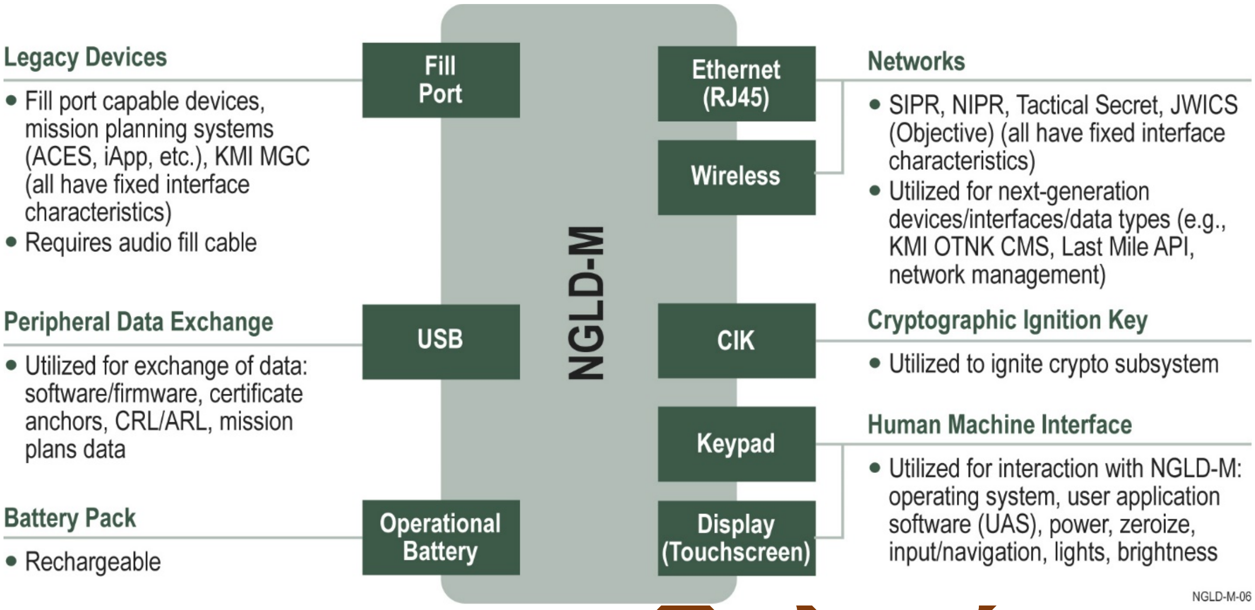

Legacy Devices
• Fill port capable devices, mission planning systems (ACES, iApp, etc.), KMI MGC (all have fixed interface characteristics)
• Requires audio fill cable
Peripheral Data Exchange
• Utilized for exchange of data: software/firmware, certificate anchors, CRL/ARL, mission plans data
Battery Pack
• Rechargeable
Fill Port
USB
Operational Battery
NGLD-M
Ethernet (RJ45)
Wireless
CIK
Keypad
Display (Touchscreen)
Networks
• SIPR, NIPR, Tactical Secret, JWICS (Objective) (all have fixed interface characteristics)
• Utilized for next-generation devices/interfaces/data types (e.g., KMI OTNK CMS, Last Mile API, network management)
Cryptographic Ignition Key
• Utilized to ignite crypto subsystem
Human Machine Interface
• Utilized for interaction with NGLD-M: operating system, user application software (UAS), power, zeroize, input/navigation, lights, brightness
NGLD-M-06

Figure 7 – (U) NGLD-M Physical External Interfaces

UNCLASSIFIED / FOR OFFICIAL USE ONLY

NGLD-M Interfaces and Data Types		Medium Assurance Mode	High Assurance Mode
External Physical Interfaces	Display	Active	Active
	Keypad	Active	Active
	Fill Port	Not Active	Active
	CIK (High Assurance)	Not Active	Active
	Authenticator (Medium Assurance)	Active	Active
	USB	Active	Active
	Ethernet (RJ45)	Active	Active
	Wireless	Active	Active
	Operational Battery	Active	Active
External Logical Interfaces	Display	Local Input/Output only	Local Input/Output only
	Keypad	Local Input/Output only	Local Input/Output only
	Fill Port	Not Used	Connects with MGC, Legacy ECUs, ACES, Fill Devices (e.g., NGLD-M, SKL, etc.).
	CIK (High Assurance)	Not Used	To Be Defined

NGLD-M Interfaces and Data Types		Medium Assurance Mode	High Assurance Mode
	Authenticator (Medium Assurance)	To Be Defined	To Be Defined
	USB	Utilizing mass storage: iApp/MSApp, Approved workstations, approved accessories, Legacy ECUs. Can connect with KMI Medium Assurance credentials if USB is acting as virtual ethernet: NSA Storefront (on several classification domains: NIPR, SIPR, Tactical Secret, JWICS (Objective requirement)), KMI-Aware/PDE enabled devices, iApp/MSApp, MGC (MPMSS), Routers/Switches, Network monitoring systems.	Utilizing mass storage: iApp/MSApp, Approved workstations, approved accessories, Legacy ECUs. Can connect with KMI High Assurance credentials if USB is acting as virtual ethernet: NSA Storefront (on several classification domains: NIPR, SIPR, Tactical Secret, JWICS (Objective requirement)), KMI-Aware/PDE enabled devices, iApp/MSApp, MGC (MPMSS), Routers/Switches, Network monitoring systems.
	Ethernet (RJ45)	Connects using KMI Medium Assurance credentials: NSA Storefront (on several classification domains: NIPR, SIPR, Tactical Secret, JWICS (Objective requirement)), KMI-Aware/PDE enabled devices, iApp/MSApp, MGC (MPMSS). Routers/Switches, Network monitoring systems.	Connects using KMI High or Medium Assurance credentials: NSA Storefront (on several classification domains: NIPR, SIPR, Tactical Secret, JWICS (Objective requirement)), KMI-Aware/PDE enabled devices, iApp/MSApp, MGC (MPMSS). Routers/Switches, Network monitoring systems.
	Wireless	Connects using KMI Medium Assurance credentials: NSA Storefront (on several classification domains: NIPR, SIPR, Tactical Secret, JWICS (Objective requirement)), KMI-Aware/PDE enabled devices, iApp/MSApp, MGC (MPMSS). Routers/Switches, Network monitoring systems.	Connects using KMI High or Medium Assurance credentials: NSA Storefront (on several classification domains: NIPR, SIPR, Tactical Secret, JWICS (Objective requirement)), KMI-Aware/PDE enabled devices, iApp/MSApp, MGC (MPMSS). Routers/Switches, Network monitoring systems.
	Operational Battery	Local only	Local only
Data Types	Display	Video Signals	Video Signals
	Keypad	Keypad Signals	Keypad Signals

NGLD-M Interfaces and Data Types		Medium Assurance Mode	High Assurance Mode
	Fill Port	Not Used	Key material (Red/Black), Benign Fill, Message data, SOI data, EP data, Database items, Software/Firmware, Audit data, Fault data, ECU Commands.
	CIK (High Assurance)	Not Used	Key Split data, To Be Defined
	Authenticator (Medium Assurance)	To Be Defined	To Be Defined
	USB	Certificate data, CRL/ARLs, CMS key packages, Audit data, Fault data, Accounting data, RCF, Router/Switch configuration data, Backup data, File sets, Software/Firmware, Network time, Health Monitoring Data, Tier 2 XML, Tier 3 XML, E-PGF data, Network authentication data, SNMP.	Certificate data, CRL/ARLs, CMS key packages, Audit data, Fault data, Accounting data, RCF, Router/Switch configuration data, Backup data, File sets, Software/Firmware, Network time, Health Monitoring Data, Tier 2 XML, Tier 3 XML, E-PGF data, Network authentication data, SNMP.
	Ethernet (RJ45)	Certificate data, CRL/ARLs, CMS key packages, Audit data, Fault data, Accounting data, RCF, Router/Switch configuration data, Backup data, File sets, Software/Firmware, Network time, Health Monitoring Data, Tier 2 XML, Tier 3 XML, E-PGF data, Network authentication data, SNMP.	Certificate data, CRL/ARLs, CMS key packages, Audit data, Fault data, Accounting data, RCF, Router/Switch configuration data, Backup data, File sets, Software/Firmware, Network time, Health Monitoring Data, Tier 2 XML, Tier 3 XML, E-PGF data, Network authentication data, SNMP.
	Wireless	Certificate data, CRL/ARLs, CMS key packages, Audit data, Fault data, Accounting data, RCF, Router/Switch configuration data, Backup data, File sets, Software/Firmware, Network time, Health Monitoring Data, Tier 2 XML, Tier 3 XML, E-PGF data, Network authentication data, SNMP.	Certificate data, CRL/ARLs, CMS key packages, Audit data, Fault data, Accounting data, RCF, Router/Switch configuration data, Backup data, File sets, Software/Firmware, Network time, Health Monitoring Data, Tier 2 XML, Tier 3 XML, E-PGF data, Network authentication data, SNMP.
	Operational Battery	To Be Defined	To Be Defined

NGLD-M Interfaces and Data Types	Medium Assurance Mode	High Assurance Mode

UNCLASSIFIED//FOR OFFICAL USE ONLY

Table 10 -(U) NGLD-M External Interfaces and Medium and High Assurance mode characteristics by Interface

3.3.2 (U) Physical External Interfaces

(U//FOUO) This section addresses the requirements for the physical subcomponents that make up the NGLD-M as a hardware product that can be directly interacted with by users or attached to local systems in support of communication protocols: DS-101, DS-102, MIL-STD-188-114, RS-232, USB, Ethernet, and wireless. The physical subcomponents include: Display, Keypad, Fill Port, CIK and interface, Universal Serial Bus (USB), Ethernet (RJ45), Wireless, and Operational Battery.

3.3.2.1 (U) Display

(U//FOUO) The NGLD-M is required to provide a touchscreen display for NGLD-M users to direct/interface the internal device User Application Software (UAS). From a physical interface perspective, the display must fit within the size, weight, and power (SWAP) requirements for NGLD-M, and must be impact and scratch resistant. The display also needs to be usable by personnel in hazardous environments that require them to operate up to Mission Oriented Protective Posture (MOPP) Level 4, which includes wearing thick rubber gloves. The display must provide brightness controls that allow the user to operate in low light, sunlight, and with night vision technology as well as be viewable in greyscale/monochrome. The system will support the maximum resolution possible by the hardware, with contrast ratio being sufficiently high in all the needed lighting modes, and with a minimum of 262K colors. The NGLD-M will also provide the user with the ability to switch between portrait and landscape configuration and the ability to set one as a default.

3.3.2.2 (U) Keypad

(U//FOUO) The NGLD-M is required to provide a keypad interface that allows the user to navigate the NGLD-M in lieu of touch navigation capabilities via the combined display and UAS. Other physically manipulated components of the keypad include support for power-up, power-down, brightness control, and zeroization.

3.3.2.3 (U) Fill Port

(U//FOUO) The NGLD-M is required to interface with other devices via a 6-pin fill port interface, supporting DS-101, DS-102, and RS-232 at minimum defined rates. The fill port interface may be an extraneous part and will not be counted toward calculating the SWAP of NGLD-M. The fill port supports communication and data sharing with other devices and is also used to support updating the software/firmware of the NGLD-M.

3.3.2.4 (U) Cryptographic Ignition Key (CIK)

(U//FOUO) In accordance with security requirements, the NGLD-M is required to incorporate a valid methodology by which the cryptographic subcomponent and Fill Port interface of the NGLD-M will be activated. The cryptographic subcomponent of NGLD-M provides appropriately privileged users with access to High Assurance and Medium Assurance cryptographic services. The NGLD-M cryptographic subcomponent and Fill Port interface are not to be operable without a valid, security approved activation implementation.

3.3.2.5 (U) Universal Serial Bus (USB)

(U//FOUO) The NGLD-M provides a USB interface. Extraneous parts connected via USB are *not* counted toward calculation of SWAP. The USB interface is used for supporting data movement with valid and approved systems and for charging of NGLD-M batteries. Data to be moved includes, but is not limited to, software/firmware updates, Certificate data (e.g., KMI IA(I), KE(I), IA(M), certificate authority certificates, CRL/ARLs, web server certificates, etc.), mission plans, ECU profile data, CMS packages, and the like.

3.3.2.6 (U) Ethernet (RJ45)

(U//FOUO) The NGLD-M provides an Ethernet (RJ45) interface to authorized users. This interface supports the operation of the NGLD-M to connect with multiple security domains, one at a time, such as SIPRNet, NIPRNet, Tactical Secret, or JWICS (objective). The Ethernet (RJ45) interface operates at Gigabit Ethernet speed and provides capability for network protocol usage compliant with fixed logical interface specification; including, but not limited to, OTNK, TLS, SNMP, TFTP, FTPS. Extraneous parts connected via Ethernet (RJ45) are not counted toward calculation of SWAP.

(U//FOUO) The NGLD-M supports transmit and receive of general data and files, PKI certificate data (e.g., IA(I), IA(M), KE(I)), mission plan data, profile data, Certificate Revocation List (CRL) data, Authority Revocation List (ARL) data, and Cryptographic Message Syntax (CMS) via the wired network. NGLD-M will require periodic software and firmware updates and the wired Ethernet (RJ45) must support download of software and firmware. The NGLD-M is also required to occasionally support the loading and configuration of ECUs as well as be managed by the NetOps toolset; all via the wired Ethernet (RJ45) interface. Protocols that are required for wired Ethernet (RJ45) support include TLS 1.2 (or later, as well as have backward compatibility), Simple Network Management Protocol (SNMP), File Transfer Protocol Secure (FTPS), and Trivial File Transport Protocol (TFTP).

3.3.2.7 (U) Wireless

(U//FOUO) The NGLD-M provides cryptographically secured wireless interface to authorized users. The wireless interface will be disabled by default and allow the user to enable or disable it on demand. The NGLD-M will support transmit and receive of data to include but not limited to, software/firmware packages, mission plans, profiles, PKI certificates, CRLs, ARLs, CMS content, KEK and other approved content via this interface. Protocols that are required for wireless support include TLS 1.2 (or later, as well as have backward compatibility to TLS 1.0 at a minimum), SNMP, FTPS, and TFTP.

3.3.2.8 (U) Operational Battery

(U//FOUO) The NGLD-M is required to provide an operational battery pack that is rechargeable within 48 hours, has no memory, and is low maintenance, non-spill, and thermal safe. In addition, this battery pack must be rechargeable via worldwide alternating current (AC) power.

3.3.3 (U) Logical (Networked) External Interfaces

(U//FOUO) There are several externally networked systems, APIs and endpoints the NGLD-M and its privileged users communicate with to fulfill the mission. This section covers the logical external interfaces (beyond the physical) that the NGLD-M must interact with via the network to meet operational requirements. The interfaces in Figure 8 - (U) Logical External Interfaces are described in the following subsections.

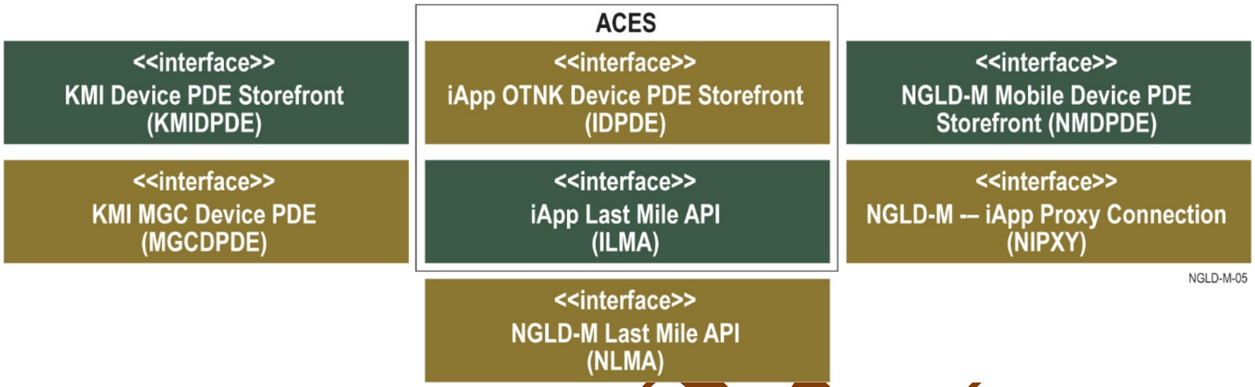


Figure 8 - (U) Logical External Interfaces

(U//FOUO) The interconnectivity of these interfaces as they relate to the NGLD-M can be seen in Figure 9 - (U) Logical External Interfaces Context Diagram. Functional requirements pertaining to the use of the various Device PDEs and the information / products retrieved from these interfaces are described throughout section 0-3.2 (U) System or Subsystem Functional Requirements. These Storefronts reside at various endpoints (Uniform Resource Identifiers - URIs), but follow the same protocols and standards set forth in KMI 3300 for how a device communicates with each. They are also referred to as 'OTNK-Compliant Storefronts' throughout this document where helpful to generalize interface requirement and products retrieved from any of these interfaces.

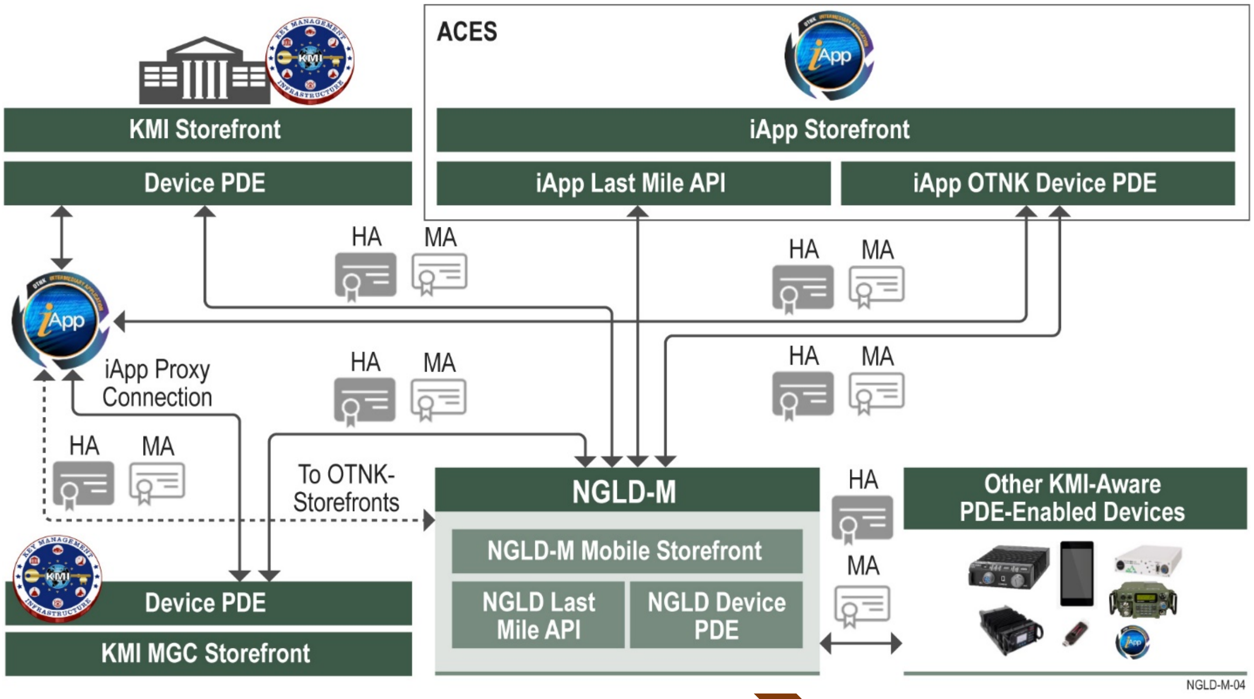


Figure 9 - (U) Logical External Interfaces Context Diagram

3.3.3.1 (U) KMI Device PDE Storefront (PUI:KMIDPDE)

(U//FOUO) The KMI Storefront's KMI Device PDE Storefront is one of several distribution services offered by KMI in support of the OTNK features of the system. The NGLD-M authenticates to this interface as a KMI-Aware Device using both Medium and High Assurance PKI (credentials) to retrieve PALs and download applicable products. This is one of several OTNK-Compliant storefronts accessed by the NGLD-M.

3.3.3.2 (U) KMI Management Client (MGC) Device PDE Storefront (PUI:MGCDPDE)

(U//FOUO) The KMI MGC Device PDE Storefront is similar to the KMI Device PDE Storefront offered at the PRSN, but is accessed via the KMI MGC. This is one of several distribution services offered by KMI in support of OTNK. The NGLD-M authenticates as a KMI-Aware device using both Medium and High Assurance PKI (credentials) to retrieve PALs and download applicable products. This is one of the several OTNK-Compliant storefronts accessed by the NGLD-M.

3.3.3.3 (U) ACES/iApp OTNK Device PDE Storefront (PUI:IDPDE)

(U//FOUO) The NGLD-M communicates with ACES/iApp's OTNK-Compliant Device PDE Storefront in a similar fashion to its communications with the KMI Device PDE Storefronts. This is another of the several OTNK-Compliant storefronts accessed by the NGLD-M. The iApp OTNK Device PDE Storefront interface is compliant with the KMI 3300 specification providing an alternate endpoint for the NGLD-M performing as a KMI-Aware device. iApp provides Intermediary services including distribution and ordering for iApp and NGLD-M users. The NGLD-M authenticates as a KMI-Aware device to the iApp Storefront using both Medium and High Assurance PKI (credentials) to retrieve PALs and download applicable products.

3.3.3.4 (U) ACES/iApp Last Mile API (PUI:ILMA)

(U//FOUO) The ACES/iApp Last Mile API (LMA) is a CCB-supported API that supports the communication of pertinent content such as audit data, cryptographic, products and health and status monitoring data. NGLD-M devices and users can share data, information, and reports to allow Local Elements and COMSEC Managers to perform required operations and satisfy local service and agency-specific policies, which supports operational NGLD-M use cases and workflow. Users can configure NGLD-M devices to authenticate using both Medium and High Assurance PKI (credentials) and exchange data with a networked (or connected) iApp using the iApp LMA standardized services.

3.3.3.5 (U) NGLD-M Last Mile API (PUI:NLMA)

(U//FOUO) The NGLD-M LMA provides services to allow external clients to communicate and share data with another device implementing the API. The external client authenticates as a KMI-Aware device using both Medium and High Assurance PKI (credentials) to share data.

3.3.3.6 (U) NGLD-M Mobile Device PDE Storefront (PUI:NMDPDE)

(U//FOUO) The NGLD-M has an OTNK-Compliant Device PDE Storefront interface. This allows the NGLD-M to serve as a Storefront for its locally supported PDE-Enabled KMI-Aware Devices. This interface is compliant with the KMI 3300 specification allowing the NGLD-M to perform as a service in alignment with KMI to support an alternate endpoint for KMI-Aware devices. Supported PDE-Enabled KMI-Aware Devices authenticate as KMI-Aware devices using Medium and High Assurance PKI (credentials) to exchange data. Supported data on this PDE storefront would be primarily data received from KMI (formatted in accordance with KMI 3300 standards). It could also be supported cryptographic products that were re-wrapped (objective) in accordance with the same standards.

3.3.3.7 (U) NGLD-M iApp Proxy Connection (PUI:NIPXY)

(U//FOUO) The NGLD-M iApp Proxy connection allows for the NGLD-M connected to an iApp workstation to connect to an OTNK-Compliant Device PDE endpoint using its KMI Medium or High Assurance credentials. The iApp Proxy supports the NGLD-M with its goal of communicating with an established OTNK-Compliant endpoint without being directly connected to a network port, but rather docked with an iApp Manager Workstation.

3.4 (U) System Internal Interface Requirements

(U//FOUO) The NGLD-M Internal Interfaces support the device's operational goals by moving internal data through the system in a secure fashion. The NGLD-M's internal interfaces include an Operating System (OS), UAS, High Assurance Cryptographic Module, and a testing framework. The OS runs on the device and hosts the UAS, which in turn directs access to the physical interfaces. The UAS provides the user interface to the device that interacts with the OS and drivers to complete user directed operations. The High Assurance cryptographic module performs all secure operations of the device. The testing framework performs system checks to ensure that the device is not compromised.

(U//FOUO) Figure 10- (U) Logical Internal Interface Components provides a logical view of the internal interface components. The specific sub-components of the internal interfaces purposely excluded and left to the design.

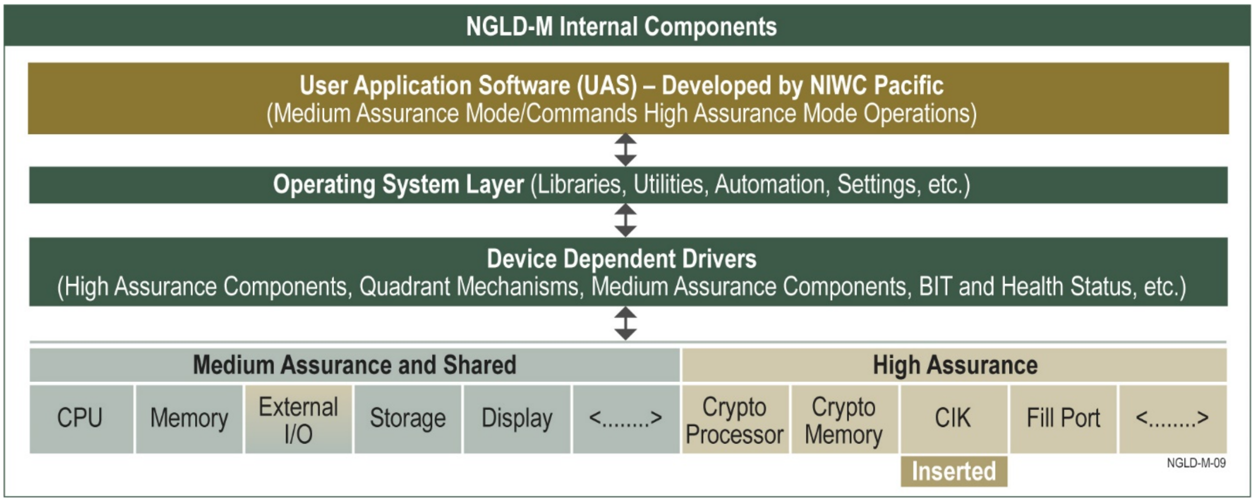

NGLD-M Internal Components
User Application Software (UAS) – Developed by NIWC Pacific
(Medium Assurance Mode/Commands High Assurance Mode Operations)
Operating System Layer (Libraries, Utilities, Automation, Settings, etc.)
Device Dependent Drivers
(High Assurance Components, Quadrant Mechanisms, Medium Assurance Components, BIT and Health Status, etc.)
Medium Assurance and Shared
High Assurance
CPU
Memory
External I/O
Storage
Display
<........>
Crypto Processor
Crypto Memory
CIK
Fill Port
<........>
Inserted
NGLD-M-09

Figure 10- (U) Logical Internal Interface Components

3.5 (U) System Internal Data Requirements

(U) Not supplied with this SRD at this time.

3.6 (U) Adaptation Requirements

(U) Not supplied with this SRD at this time.

3.7 (U) Environmental, Safety, and Operational Health (ESOH) Requirements

(U//FOUO) The NGLD-M is operated by a user and as such all safety and health hazards are eliminated or reduced to the lowest risk levels practical with residual hazards accepted by appropriate risk decision authorities. The device is free from conditions that can cause death, injury, or illness to users.

3.7.1 (U) Chemical, Biological, Radiological, and Nuclear (CBRNE)

(U//FOUO) The NGLD-M operational mission may require the device to operate in CBRNE areas. The device meets all documented US Army requirements for having to operate in the aforementioned environments, as well as all decontamination requirements. **Note: NGLD-M is not required to meet the explosive requirements.**

3.8 (U) Security and Privacy Requirements

(U//FOUO) The NGLD-M is a High Assurance load device that is network enabled and is required to meet security requirements found within the NSA NGLD-M Tailored IASRD. This includes, and is not limited to, requirements for providing physical safeguards, assured completion of processing, physical external interface controls, TAMPER, Zeroization without external power required, TEMPEST, Fail Safe Design Analysis (FSDA), inclusion of security mechanisms, and cleared personnel and facilities for development.

(U//FOUO) NGLD-M Tailored Operational Security Doctrine (OSD) Requirements apply.

(U//FOUO) The NGLD-M is operated on DoD networks and must meet security requirements that align with RMF security controls. The RMF security controls are guided by the security classifications of Confidentiality (High), Integrity (High), and Availability (High), along with classified and tactical overlays. RMF security controls have traceability to detailed requirements sourced from applicable Security Technical Implementation Guide (STIG) and Security Requirements Guide (SRG) sources. Applicability of exact STIG and SRG requirement source documents are identified based on the proposed technical implementation of the solution.

3.8.1 (U) General Security and Privacy

(U//FOUO) The NGLD-M provides general security and privacy protection mechanisms that include physical access control, processing execution guarantees, command of external interfaces, and controlled access to high assurance capable cryptographic subsystems. Physical access control includes preventing physical access to all internal software, firmware, and hardware elements. Processing execution guarantees requires NGLD-M to contain mechanism(s) that guarantee the completion of actions once they are initiated. The external interfaces of the NGLD-M will be able to be enabled and disabled on command. Controlled access to high assurance capable cryptographic subsystems requires an explicit user login onto the crypto subsystem, after a hardware reset, if a recognized and valid high assurance CIK is inserted.

3.8.2 (U) Tamper

(U//FOUO) The NGLD-M provides Tamper protection in accordance with the NSA NGLD-M Tailored IASRD. NGLD-M will support Field Tamper recovery, Anti-Tamper capabilities during the absence of external power, and will protect software and firmware within the Information Security (INFOSEC) boundary.

3.8.3 (U) TEMPEST

(U//FOUO) The NGLD-M meets TEMPEST Level I requirements found within the NSA NGLD-M Tailored IASRD.

3.8.4 (U) Information Assurance Standards and Certification

(U//FOUO) The NGLD-M includes security mechanisms to meet the FSDA requirements found within the NSA NGLD-M Tailored IASRD. In support of IASRD requirements, product development will be done by US citizens cleared at the Secret or higher level and within facilities cleared at the Secret or higher level.

3.8.5 (U) NGLD-M Operational Security Doctrine (OSD)

(U//FOUO) The NGLD-M implements the NGLD-M Tailored OSD requirements. The NGLD-M OSD is the Security Doctrine for how the data and device are handled. How the device is handled depends on several factors including data in the device, what operational state it is in, the location the device is being used, etc. The device allows users to follow the requirements in the document and operate in a secure fashion.

3.8.6 (U) Risk Management Framework (RMF)

(U//FOUO) The RMF is a multistep process used by the NGLD-M program to build security into the product and allow the product to be fielded and maintain an authority to operate (ATO) on DoD Networks. The technical details of the RMF requirements are found within applicable STIGs and SRGs. STIG documents are aligned with specific technologies such as Application Security, Cloud Security, Cross Domain Solutions, Host Based Security System (HBSS), and Mobility, Network / Perimeter / Wireless, and Operating Systems. Within these technology areas, there are multiple security requirement documents that focus on specific makes and models of produced technologies, as well as a baseline of specific security requirements and information on how to implement and test. NGLD-M UAS developers will develop to the Application Security and Development STIG and will assess the inclusion of other STIGs as required. SRG documents, like STIGs, provide security requirements that are aligned with less specific technologies that have not yet been fully supported with STIG specific technology requirements management. Until the hardware and operating system specifics for NGLD-M are known, the NGLD-M UAS developers will target less specific Database SRG and Web Server SRG sources of the RMF technical security requirements.

3.9 (U) System Environment Requirements

(U//FOUO) The NGLD-M is exposed to many different operational environments when it is being used. Due to this, the NGLD-M is required to meet the US Army's environmental requirements for devices that operate in these environments.

3.9.1 (U) Environment

(U//FOUO) The NGLD-M is transported, stored, and operates in a myriad of environments depending on the operational theatre. Everything from warehouse storage to the battlefield in every environment across the globe. As a result, the NGLD-M meets a very strict set of environmental requirements so it is able to stand up to many environmental hazards while it is being used. These hazards consist of temperature, exposure, shock, vibration, water, electricity and other hazards that are captured in the documents that govern the environmental requirements for the device.

3.9.2 (U) High-Altitude Electromagnetic Pulse (HEMP)

(U//FOUO) Due to the use of the NGLD-M in varied austere environments such as high altitude, the device may be exposed to a HEMP and as a result must meet the required HEMP requirements and testing defined in MIL-STD 2169B when it is not turned on and no external cables are connected.

3.10 (U) Computer Resource Requirements

3.10.1 (U) Computer Hardware Requirements

(U) This is not supplied at this time but will be generated as a part of the System hardware software requirements

3.10.2 (U) Computer Hardware Resource Utilization Requirements

(U) Not supplied with this SRD at this time but will be generated as a part of the System hardware software requirements

3.10.3 (U) Computer Software Requirements

3.10.3.1 (U) Operating System

(U//FOUO) The NGLD-M Operating system meets security requirements and is integrated to be maintained in an efficient manner.

3.10.4 (U) Computer Communications Requirements

(U) Not supplied with this SRD at this time but will be generated as a part of the System hardware software requirements

3.11 (U) System Quality Factors

3.11.1 (U) Reliability, Availability, Maintainability (RAM)

(U) Reliability, Availability, and Maintainability are independent system attributes that collectively affect the logistical management and support of a given system. Specifically, Reliability is a probability value identifying the system's ability to perform without as defined by functional requirements under defined conditions without entering a failure state. Maintainability represents the probability that a given system is repairable given a defined toolset with a specified timeframe. Availability is the probability that, given the Reliability and Maintainability estimated values, a system is operational and accessible to the user. The following requirements outline the RAM requirements for the NGLD-M.

3.11.2 (U) Expandability

(U) The NGLD-M is intended to support the DoD military services and US Government Civil Agencies for a number of years into the future. To ensure the NGLD-M is able to manage the evolution of these diverse organizations and the expected growth in both the operational software and data retention requirements during this extended timeframe, the NGLD-M must accommodate memory expansion in both volatile and non-volatile memory.

3.11.3 (U) Performance

(U) Performance covers the extent to which the functions supporting the NGLD-M mission are executed. Performance characteristics are measured in terms of quantity and quality. The NGLD-M must perform within tolerable limits for core functions.

3.12 (U) Design and Construction Constraints

(U) Not supplied with this SRD at this time but will be derived upon the vendor selection.

3.13 (U) Personnel Related Requirements

(U) Not supplied with this SRD at this time. This are defined in PWS rather than SRD.

3.14 (U) Training Related Requirements

(U) Not supplied with this SRD at this time. This are defined in PWS but not with SRD.

3.15 (U) Logistics Related Requirements

(U//FOUO) Logistics is a multi-functional domain associated with ensuring support considerations are a fundamental aspect of a system’s requirements, design, development, to ensure throughout the development lifecycle that the fielding, sustainment, and improvement modifications of systems are understood and taking into consideration. When this approach is taken throughout development, an increased probability that the system can be efficiently supported through its product lifespan and that the required infrastructure necessary to provide operational support of the system are identified and acquired is realized.

3.16 (U) Other Requirements

3.16.1 (U) User Application Software (UAS) Integration

(U//FOUO) The NGLD-M User Application Software (UAS) is the user-facing cryptographic key management application / software on the NGLD-M. It provides the main user-interface the user leverages in order to perform cryptographic key management functions with the NGLD-M device. The NGLD-M UAS software provides the capability for the user to perform overall cryptographic key management actions. Naval Information Warfare Center Pacific (NIWC-PAC) is the developer of the NGLD-M UAS. The Vendor will integrate the User Application Software (UAS) developed by NIWC-PAC and provided as Government Furnished Software (GFS).

3.16.2 (U) Supporting Tools

(U//FOUO) There are a number of tools developed that support the NGLD-M operationally. This includes a tool to help support the software update process covering both software and firmware. Additionally, there is a tool to support dynamic ECU profile generation.

3.16.3 (U) Test Asset

(U//FOUO) Test assets are provided to support a variety of test events as well as troubleshooting. Assets are provided using developmental software, debugging tools and hardware.

3.17 (U) Packaging Requirements

(U) Not supplied with this SRD at this time but defined in PWS.

3.18 (U) Statutory, Regulatory, and Certification Requirements

3.18.1 (U) Statutory Requirements

(U) Not supplied with this SRD at this time but defined in PWS.

3.18.2 (U) Regulatory Requirements

(U) Not supplied with this SRD at this time but defined in PWS.

3.18.3 (U) Certification Requirements

(U) Not supplied with this SRD at this time but defined in PWS.

3.19 (U) Precedence and Criticality of Requirements

(U) Not supplied with this SRD at this time but defined in PWS.

3.20 (U) Demilitarization and Disposal

(U) The demilitarization and disposition of the system has to be in accordance with AR 710-02 (Supply Policy below the National Level).

(U/FOUO) Demilitarization/Destruction: - All demilitarization/destruction of the system shall be performed at authorized Depot facilities. Classified COMSEC equipment and CCI, including components, scrap or residue are specifically prohibited from turn-in to Defense Reutilization and Marketing Office (DRMO).

(U//FOUO) Departments and agencies that do not have NSA-approved COMSEC destruction facilities will send the system to NSA for destruction.

(U) Dispose of equipment hulk. NOTE: (U) While not required, it is recommended that the remaining hulk be smashed prior to disposal.

(U) NGLD-M shall be designed to allow sensitive sub components to be disposed of in a cost effective manner.

(U) NGLD-M shall be designed to comply with National Environmental Protection Act.

4. (U) VERIFICATION PROVISIONS

(U) The four fundamental methods of verification for the NGLD-M SRD requirements are Demonstration, Test, Analysis, and Inspection. The requirements traceability table provided in Appendix C includes all NGLD-M requirement stated in section 3 with an associated verification method.

4.1 (U) Verification Methods

4.1.1 (U) Demonstration

(U) Demonstration is the manipulation or operation of the NGLD-M to verify observable functional operation not requiring use of instrumentation, special test equipment, or subsequent analysis that the results are as planned or expected.

4.1.2 (U) Test

(U) Test is the verification of the NGLD-M operation using instrumentation or other special test equipment to collect data for later analysis.

4.1.3 (U) Analysis

(U) Analysis is the verification of NGLD-M operation through processing of accumulated data obtained from other qualification methods. Analysis allows for predictive statements about the typical performance of the NGLD-M based on the confirmed test results of a sample set or by combining the outcome of individual tests to make conclusions. This method is often used to predict the breaking point or failure by using nondestructive tests to extrapolate the failure point.

4.1.4 (U) Inspection

(U) The Inspection verification method is the nondestructive examination of the NGLD-M through examination of components, documents, drawings, etc.

4.1.5 (U) Special Verification Methods

(U) Although not planned for, the NGLD-M may require special verification methods, e.g., use special tools, techniques, procedures, facilities, acceptance limits, use of standard samples, etc. in order to successfully verify requirements implementation.

5. (U) REQUIREMENTS TRACEABILITY

(U//FOUO) Refer to the following appendix for the NGLD-M Requirements Traceability matrix:

0 - 7.1 (U) Appendix A – Requirement Verifications and Traceability Matrix.

6. (U) Notes

6.1 (U) Definitions and Acronyms

(U) The following table lists all definitions and acronyms used in the document.

Acronym/Abbreviation	Description
AAA	Authentication-Authorization-Accounting
ACES	Automated Communication Engineering Software
AEHF	Advanced Extremely High Frequency
AES	Advanced Encryption Standard
AKDELIV	Application Key Material Delivery
API	Application Programming Interface
ARL	Authority Revocation List
ATO	Authority to Operate
AXID	Association and Exchange Identifier
BF	Benign Fill
BIT	Built-in Test
CAC	Common Access Card
CBRN	Chemical, Biological, Radiological, and Nuclear
CCI	Controlled Cryptographic Item
CFDI	Common Fill Device Interface
CIK	Cryptographic Ignition Key
CMS	Cryptographic Message Syntax
COMSEC	Communications Security
CPD	Capability Production Document
CPU	Central Processing Unit
CREDRQ	Credential Request
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CSfC	Commercial Solutions for Classified
CT3	Common Tier 3
DoD	Department of Defense
DoDIN	DoD Information Network
DoDIN-A	DoDIN-Alternate
DSS	Digital Signature Standard
DTD	Data Transfer Device
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECM	Electronic Counter Measure
ECU	End Cryptographic Unit
ECURS	ECU Response

Acronym/Abbreviation	Description
EKMS	Electronic Key Management System
EP	Electronic Protection
ESN	Electronic Serial Number
ESOH	Environmental, Safety, and Operational Health
ESP	Encapsulating Security Payload
FH	Frequency Hopping
FM	Frequency Modulation
FOUO	For Official Use Only
FSDA	Fail Safe Design Analysis
FTPS	File Transport Secure Protocol
Gbps	Giga bits per second
GCM	Galois/Counter Measure
GFS	Government Furnished Software
GICv4	Generic Interrupt Controller version 4
GPS	Global Positioning System
HA	High Assurance
HAIPE	High Assurance Internet Protocol Encryptor
HBSS	Host Based Security System
HEMP	High-Altitude Electromagnetic Pulse
IA	Identity certificate
iApp	Intermediary Application
IAVA	Information Assurance Vulnerability Alert
IASRD	Information Assurance Security Requirements Document
IDPDE	iApp OTNK Device PDE Storefront
ILMA	iApp Last Mile API
IP	Internet Protocol
JENM	Joint Enterprise Network Manager
JMPS	Joint Mission Planning System
K	Thousand
Kbps	Kilobits per second
KE	Key Encryption certificate
KLS	Key Load Status
KMI	Key Management Infrastructure
KMIDPDE	KMI Device PDE Storefront
KRDELIV	Key Replacement Delivery
LMA	Last Mile API
LPDDR4	Low Power Double Data Rate generation 4
MA	Medium Assurance
Mbps	Megabits per second
MGC	Management Client
MGCDPDE	KMI MGC Device PDE
MOPP	Mission Oriented Protective Posture
MPMSS	Mission Planning Mission Support System
NET ID	Network Identification
NGLD-M	Next Generation Load Device-Medium
NIC	Network Interface Card

Acronym/Abbreviation	Description
NIPRNet	Non-classified Internet Protocol Router Network
NIPXY	NGLD-M – iApp Proxy Connection
NLMA	MGLD-M Last Mile API (NLMA)
NMDPDE	NGLD-M Device PDE Storefront
NSA	National Security Agency
OS	Operating System
OSD	Operational Security Doctrine
OTAD	Over-The-Air-Distribution
OTNK	Over-The-Network-Keying
PAL	Product Availability List
PDE	Product Delivery Enclave
PKCS	Public-Key Cryptography Standards
QRG	Quick Reference Guide
RAM	Random Access Memory
RAM	Reliability, Availability, Maintainability
RCF	Radio Configuration Files
RFC	Request For Comments
RJ45	Ethernet
RMF	Risk Management Framework
RoBAC	Role Based Access Control
RSA	Rivest, Shamir, and Adelman
RV	Receive Variable
S2	Software Signature
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SINCGARS	Single Channel Ground Air Radio System
SIPRNet	Secret Internet Protocol Router Network
SKL	Simple Key Loader
SNMP	Simple Network Management Protocol
SOI	Signal Operating Instruction
SRD	System Requirements Document
SRG	Security Requirements Guide
SSO	System Security Officer
SSP	Spoof Protection
STE	Secure Telephone Equipment
STIG	Security Technical Implementation Guide
STU-III	Secure Telephone Unit, Third Generation
SWAP	Size, Weight, and Power
TAMP	Trust Anchor Management Protocol
TBD	To Be Determined
TEMPEST	Transient Electromagnetic Pulse Emanation Standard
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOD	Time of Day
TSK	Transmission Security Key
UAG	User Authentication General

Acronym/Abbreviation	Description
UAS	User Application Software
UI	User Interface
URI	Uniform Resource Identifiers
US	United States
USB	Universal Serial Bus
UTIL	Utility
UX	User eXperience
VESN	Virtual ESN
VG	Variable Generate
VHF	Very High Frequency
VU	Variable Update
WOD	Word of the Day
XML	eXtensbile Markup Language

Table 11 - (U) Definitions and Acronyms

INFOSEC Boundary - The INFOSEC Boundary encompasses those portions of the product/system which perform or implement the security-related functions specified in this document and NSA NGLD-M tailored IASRD.

Cryptographic Boundary - The Cryptographic Boundary, which explicitly defines a continuous perimeter that establishes the physical bounds containing all the hardware, software, and/or programmable logic components that implement the cryptographic services. The Cryptographic Boundary is a subset of the INFOSEC Boundary.

Cryptographic Processing Service - A cryptographic service provided to the system that is associated with a particular key.

Plaintext – Unencrypted information.

Cipher text – Encrypted information.

Encryption – The process of converting Plaintext into Cipher text by means of a code or cryptographic system.

Decryption – The process of converting Cipher text into Plaintext by means of a code or cryptographic system.

Cryptographic Algorithm – Well-defined procedure or sequence of rules or steps, or a series of mathematical equations used to describe cryptographic processes such as encryption/decryption, key generation, authentication, signatures, etc.

RED – Pertaining to plaintext.

BLACK – Pertaining to unclassified and/or cipher text.

COMSEC – Communications Security; generally includes security mechanisms that provide high assurance that information is protected while in transit or at rest.

Critical Security/Security Critical - Descriptive used in association with a security related function to describe a function that if absent, faulty, or improperly configured can/will cause loss or significant degradation of an IA Security Service (Integrity, Confidentiality, Availability, Non-repudiation and Authentication).

KMI-Aware Device – A User Device that can receive and use products that are packaged for it by KMI and for which a Global Device Identifier has been registered so that a product can be generated and packaged for distribution to that specific User Device in that Identifier.

Product Delivery Enclave (PDE)-Enabled KMI-Aware Device – A KMI-Aware device that is able to establish a network connection (e.g., SIPRnet, NIPRnet, or the public internet) to a Primary Services Node PDE to obtain KMI products and services.

Selective Zeroization: Selective zeroization is a process through which the NGLD-M selectively zeroize one or more keys within the NGLD-M crypto. Selective zeroization applies to both "working" key material and key material in persistent storage.

Recoverable Zeroization: Recoverable zeroization is a process through which all application key material within the NGLD-M crypto is zeroized, but the NGLD-M crypto-specific key material is left intact. The NGLD-M crypto-specific key material is key material that would be used to fill new application key material into the crypto. The NGLD-M crypto does not have to be reinitialized after a recoverable zeroization has been done.

Destructive Zeroization: Destructive zeroization is a process through which the NGLD-M is zeroized and all key material within the NGLD-M crypto is rendered unrecoverable. The NGLD-M crypto is required to be reinitialized after a destructive zeroization has been done.

Passive Zeroization: During passive zeroization working RAM memory is cleared by removing power to the memory. The Passive zeroization shall occur in the shortest time possible.

Types of Data:

- Cryptographic Keys (key lengths currently approved by NSA: 128, 192, 256, 384, and 512)

- CMS wrapped packages
- Mission Plans
- Radio Configuration Files
- 87-27 files
- Certificates
- Audit Data
- Various KMI Materials
- Database
- Configuration files.
- RCF files
- eXtensible Markup Language (XML) files.
- HAVEQUICK
- SINCGARS
- Credentials
- device configuration settings

Key Management: The NGLD-M crypto is required to support key management functionality for both Type 1 (Suite A and Suite B) and non-Type 1 cryptographic algorithms. Key management functions include key agreement and key exchange, key update, key fill, key identification, key accounting, key storage and retention, and zeroization. The NGLD-M crypto is required to provide KMI-related cryptographic algorithms.

Black Key vs Benign Key: BLACK fill is distinguished from Benign fill in that BLACK fill implies that a key is encrypted by another existing key and Benign fill implies that a key is encrypted by a key that was negotiated via a Benign key agreement algorithm. All the keys filled to an operational platform in the field are expected to be in Benign or BLACK form. However, to support Benign/BLACK key fill, some unencrypted key material (trust anchor certificates, KEK, FF or EFF seed key material, etc.) must first be loaded.

Simplex: The main **difference between simplex**, **half duplex**, and **full duplex** is that **in a simplex** mode of transmission the communication is unidirectional whereas, **in the half-duplex** mode of transmission the communication is two directional but the channel is alternately used by the both the connected device

NGLD-M Inactivity: NGLD-M inactivity is defined as no user initiated function calls or user initiated operations occurring over a time.

Network Inactivity: The network inactivity is defined as no user initiated network operation.

Cryptographic functions: Access to any functions that are included within Cryptographic boundary.

Last Mile API: This is a method to move cryptographic products from NGLD-M to ECUs using this interface.

7. (U) APPENDICES

7.1 (U) Appendix A – Requirement Verifications and Traceability Matrix

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0001	The NGLD-M shall perform system Power Up upon the detection of the power function.	3.1.1 - High-Level Modes	6.1.3 Net-Ready 6.2.9 (U) Operational Availability (Ao) KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0002	The NGLD-M shall boot up to user login display within 30 seconds.	3.1.1 - High-Level Modes	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0003	The NGLD-M shall transition to normal operation after a valid user is authenticated.	3.1.1 - High-Level Modes	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0004	The NGLD-M shall support transition from interactive mode to discrete mode.	3.1.1 - High-Level Modes	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0005	The NGLD-M shall support transition to a locked state on-demand and when security conditions are met.	3.1.1 - High-Level Modes	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0006	The NGLD-M shall lock the screen when the authorized user initiates discrete mode.	3.1.1 - High-Level Modes	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0007	The NGLD-M shall require re-authentication to resume normal operations.	3.1.1 - High-Level Modes	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0008	The NGLD-M shall support transition to a logged out state.	3.1.1 - High-Level Modes	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0009	The NGLD-M shall run BIT when the system is powered on or restarted, periodically during operation, and after occurrence of system/component malfunction.	3.1.1 - High-Level Modes	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0010	The NGLD-M shall provide the ability for an authorized user to run BIT on-demand.	3.1.1 - High-Level Modes	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0011	The NGLD-M shall visually indicate to the authenticated user that a BIT is in process.	3.1.1 - High-Level Modes	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0012	The NGLD-M shall visually indicate success or failure of BIT to authenticated users.	3.1.1 - High-Level Modes	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0013	The NGLD-M BIT shall visually display the detected failures to authenticated users.	3.1.1 - High-Level Modes	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0014	The NGLD-M BIT shall visually indicate to the authenticated user the criticality of the failed component and provide suggested steps to address the issue.	3.1.1 - High-Level Modes	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0015	The NGLD-M shall generate a 'CIK removed' alarm when the authenticated user is logged in and the CIK is removed.	3.1.1 - High-Level Modes	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Demonstration	T	No	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0016	The NGLD-M shall generate a 'CIK removed' alarm during power-on when the CIK is removed.	3.1.1 - High-Level Modes	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0017	The NGLD-M shall generate an alarm if any BIT failure is encountered at any stage of execution.	3.1.1 - High-Level Modes	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Test	T	No	Yes
NGLD-M_SRD_0018	The NGLD-M shall perform power down at the completion of a passive zeroize event.	3.1.1 - High-Level Modes	6.1.3 Net- Ready 6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0019	The NGLD-M shall perform power down at the detection of an Anti-TAMPER event and shall perform destructive zeroization.	3.1.1 - High-Level Modes	6.1.3 Net- Ready 6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0020	The NGLD-M shall perform power down upon detection of a critical alarm event and shall perform recoverable zeroization.	3.1.1 - High-Level Modes	6.1.3 Net- Ready 6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0021	The NGLD-M shall perform power down activities when an inactive power off timer reaches its configured Threshold.	3.1.1 - High-Level Modes	6.1.3 Net- Ready	Demonstration	T	No	Yes
NGLD-M_SRD_0022	The NGLD-M shall passively zeroize working memory during power-down.	3.1.1 - High-Level Modes	6.1.3 Net- Ready 6.2.8 Security KSA	Test	T	No	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0023	The NGLD-M shall offer a Medium Assurance Mode that does not require the High Assurance Cryptographic Module to be activated.	3.1.2 - NGLD-M and Medium Assurance Mode	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0024	The NGLD-M shall provide a user directed power-up sequence into a Medium Assurance Mode that does not require the High Assurance Cryptographic Module to be active.	3.1.2 - NGLD-M and Medium Assurance Mode	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0025	The NGLD-M shall enforce two-factor authentication when started in Medium Assurance Mode.	3.1.2 - NGLD-M and Medium Assurance Mode	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0026	The NGLD-M shall make all NGLD-M features available that do not require the use or availability of the High Assurance Cryptographic Module when in Medium Assurance Mode.	3.1.2 - NGLD-M and Medium Assurance Mode	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0027	The NGLD-M shall be able to connect to all available networks via external ports allowing IP-based interfaces when in Medium Assurance Mode.	3.1.2 - NGLD-M and Medium Assurance Mode	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0028	The NGLD-M shall be able to use the USB interface when in Medium Assurance Mode.	3.1.2 - NGLD-M and Medium Assurance Mode	6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0029	The NGLD-M shall be able to use the Wireless interface when in Medium Assurance Mode.	3.1.2 - NGLD-M and Medium Assurance Mode	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0030	The NGLD-M shall be able to communicate with KMI and all other OTNK compliant storefronts leveraging its KMI issued Medium Assurance certificate for authentication when in Medium Assurance Mode.	3.1.2 - NGLD-M and Medium Assurance Mode	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0031-1	The NGLD-M shall support the ability to transition between Medium Assurance mode to High Assurance mode without powering down the device.	3.1.3 - NGLD-M and High Assurance Mode	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0031	The NGLD-M shall support the ability to transition between Medium Assurance mode to High Assurance mode without powering down the device.	3.1.3 - NGLD-M and High Assurance Mode	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0032	The NGLD-M shall provide a user directed power-up sequence into a High Assurance Mode in which all features of the NGLD-M including the High Assurance Cryptographic Module are available	3.1.3 - NGLD-M and High Assurance Mode	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0033	The NGLD-M shall require an authorized user and High Assurance capable CIK to transition to High Assurance mode.	3.1.3 - NGLD-M and High Assurance Mode	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0034	The NGLD-M shall be able to connect to all available networks via external ports allowing IP-based interfaces when in High Assurance Mode.	3.1.3 - NGLD-M and High Assurance Mode	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0035	The NGLD-M shall be able to mutually authenticate with its KMI Medium Assurance or High Assurance certificates when communicating with KMI authorized endpoints while in High Assurance mode.	3.1.3 - NGLD-M and High Assurance Mode	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0036	The NGLD-M shall disable all external data transfer interfaces during power up.	3.2.1 - Power-Up	6.1.3 Net-Ready	Demonstration	T	No	Yes
NGLD-M_SRD_0037	The NGLD-M shall visually display status of power up to the user.	3.2.1 - Power-Up	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0038	The NGLD-M shall visually display software and hardware versions to the user.	3.2.1 - Power-Up	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0039	The NGLD-M shall automatically adjust display brightness to the last saved brightness level adjustment provided by the user.	3.2.1 - Power-Up	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0040	The NGLD-M shall be designed to manage user inactivity.	3.2.2 - User (Human User and Device User) Management	6.1.3 Net- Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0041	The NGLD-M shall transition to normal operation when user activities are detected.	3.2.2 - User (Human User and Device User) Management	6.1.3 Net- Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0042	The NGLD-M shall return to the screen the user was on after re-authentication.	3.2.2 - User (Human User and Device User) Management	6.1.3 Net- Ready 6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0043	During normal operation, the NGLD-M shall support user inactivity decision. Note: NGLD-M inactivity is defined as no touch screen inputs, button pushes, and USB attached mouse movement detections, and any network traffic over a time period specified by inactive Power off timer. Inactive power off timer is the time lapse from NGLD-M inactivity until configured value.	3.2.2 - User (Human User and Device User) Management	6.1.3 Net- Ready	Demonstration	T	No	Yes
NGLD-M_SRD_0044	The NGLD-M shall support and manage touch screen lock.	3.2.2 - User (Human User and Device User) Management	6.1.3 Net- Ready 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0045	The NGLD-M shall require to re-authenticate after continuous operation without network operations.	3.2.2 - User (Human User and Device User) Management	6.1.3 Net- Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0046	The NGLD-M re-authentication shall occur after the completion of an operation that is in the process.	3.2.2 - User (Human User and Device User) Management	6.1.3 Net- Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0047	The NGLD-M shall allow for the creation of user profile data for a minimum of thirty-two (32) users.	3.2.2.1 - Human User Management	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0048	The NGLD-M shall allow for the deletion of user profile data for a minimum of thirty-two (32) users.	3.2.2.1 - Human User Management	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0049	The NGLD-M shall allow for the storage of user profile data for a minimum of thirty-two (32) users.	3.2.2.1 - Human User Management	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0050	The NGLD-M shall allow for the update of user profile data for a minimum of thirty-two (32) users.	3.2.2.1 - Human User Management	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0051	The NGLD-M shall enforce two factor authentication (no Common Access Card (CAC) or Secret Internet Protocol Router (SIPR) tokens) for all users.	3.2.2.1 - Human User Management	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0052	The NGLD-M shall meet username and password requirements of the NGLD-M Tailored IASRD/RMF.	3.2.2.1 - Human User Management	6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0053	NGLD-M shall use at least SHA-384 to alter the password/PIN for storage protection.	3.2.2.1 - Human User Management	6.2.8 Security KSA	Analysis	T	Yes	Yes
NGLD-M_SRD_0054	NGLD-M shall apply at least SHA-384 to each logon password/PIN to compare with the stored password/PIN value to authenticate the user's identity.	3.2.2.1 - Human User Management	6.2.8 Security KSA	Analysis	T	Yes	Yes
NGLD-M_SRD_0055	NGLD-M shall generate a certificate signing request (CSR) for a Human User.	3.2.2.1 - Human User Management	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0056	NGLD-M shall receive and store Human Users Medium Assurance credentials from KMI.	3.2.2.1 - Human User Management	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0057	NGLD-M shall receive and store credentials for a Human User to access SIPRNET, NIPRNET, and TS networks.	3.2.2.1 - Human User Management	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0058	In the event a user enters the password incorrectly five (5) times, the NGLD-M shall lock the account.	3.2.2.1 - Human User Management	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0059	NGLD-M shall allow for the creation of a device users.	3.2.2.2 - Device User Management	6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0060	NGLD-M shall allow for the update of a device users.	3.2.2.2 - Device User Management	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0061	NGLD-M shall manage other external devices as device users that will authenticate to the NGLD-M as an endpoint.	3.2.2.2 - Device User Management	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0062	NGLD-M shall allow for the deletion of device users.	3.2.2.2 - Device User Management	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0063	NGLD-M shall generate a certificate signing request (CSR) for a Device User.	3.2.2.2 - Device User Management	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0064	NGLD-M shall receive and store Device Users High Assurance credentials from KMI.	3.2.2.2 - Device User Management	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0065	NGLD-M shall receive and store Device Users Medium Assurance credentials from KMI.	3.2.2.2 - Device User Management	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0066	The NGLD-M shall support role-based access control (RoBAC) with privileged operations assigned to roles.	3.2.2.3 - Access Control	6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0067	The NGLD-M shall support role-based access control (RoBAC) with the following privileged operations (at a minimum) assigned to roles: a. The NGLD-M shall support a role based user privilege for access to all users data. b. The NGLD-M shall support a role based user privilege to change other users passwords. c. The NGLD-M shall support a role based user privilege to add a user. d. The NGLD-M shall support a role based user privilege to edit a user. e. The NGLD-M shall support a role based user privilege to delete a user. f. The NGLD-M shall support a role based user privilege to access audit data. g. The NGLD-M shall support a role based user privilege to upgrade software. h. The NGLD-M shall support a role based user privilege to unlock accounts that have been locked.	3.2.2.3 - Access Control	6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0068	The NGLD-M shall provide a KMI Certificate Management Service.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0069	The NGLD-M shall support a minimum of twenty (20) internally-stored Trust Anchors.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0070	The NGLD-M Trust Anchors shall be read-only.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Test	T	Yes	No
NGLD-M_SRD_0071	The NGLD-M Trust Anchors import shall require enhanced security controls. Note: May consider up to and including Two-Person-Controls	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Test	T	Yes	No
NGLD-M_SRD_0072	The NGLD-M shall contain a permanent (unmodifiable) Electronic Serial Number (ESN) that complies with KMI-3001.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Test	T	No	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0073	The NGLD-M ESN shall be installed at the Factory prior to operational release.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Test	T	No	Yes
NGLD-M_SRD_0074	The NGLD-M shall comply with subscriber device requirements as defined in the X.509 Certificate Policy as specified in ITU RFC 5280.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Test	T	Yes	No
NGLD-M_SRD_0075	The NGLD-M shall be globally registered with KMI as a Medium Assurance Device.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Inspection	T	Yes	No
NGLD-M_SRD_0076	The NGLD-M shall be globally registered with KMI as a High Assurance Device.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Inspection	T	Yes	Yes
NGLD-M_SRD_0077	The NGLD-M shall supply device-related Core Registration information to a KMI Device Registration Manager.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0078	The NGLD-M shall associate imported X.509 public certificates with Device definitions by ESN when stored in the NGLD-M database.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0079	The NGLD-M shall display X.509 public certificates to user via a Device details view.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0080	The NGLD-M shall store imported trust anchors aligning with DoD X.509 PKI standards.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0081	The NGLD-M shall provide a mechanism to display and filter imported trust anchors details to include, but not limited to, associated Certificate Authority to the user.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0082	The NGLD-M shall store CSRs.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0083	The NGLD-M shall associate CSRs with Device definitions by ESN.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0084	The NGLD-M shall display CSRs to the user via a Device details view.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0085	The NGLD-M shall provide a notification to the user when internal X.509 PKI certificates are within a user defined Threshold of expiration.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0086	The NGLD-M shall provide the capability to generate an OTNK message instructing a KMI-Aware device to return its internal ESN.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	No

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0087	The NGLD-M shall deliver an OTNK message instructing a KMI-Aware device to return its internal ESN via the port on which the OTNK message was received (i.e. Fill port or Ethernet port).	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0088	The NGLD-M, upon receipt of an external KMI-Aware Device's ESN, shall display and provide loading option to the user of all products available on the NGLD-M destined for that ESN.	3.2.3.1 - Certificate Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0089	The NGLD-M shall provide capability to view CRLs.	3.2.3.1.1 - Certificate Revocation List (CRL) Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0090	The NGLD-M shall provide capability to delete CRLs.	3.2.3.1.1 - Certificate Revocation List (CRL) Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
			commonality KPP 6.2.8 Security KSA				
NGLD-M_SRD_0091	The NGLD-M shall provide capability to view ARLs.	3.2.3.1.2 - Authority Revocation List (ARL) Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0092	The NGLD-M shall provide capability to delete ARLs.	3.2.3.1.2 - Authority Revocation List (ARL) Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0093	The NGLD-M shall allow for the creation, deletion and management of connections to the iApp OTNK-Compliant Device PDE Storefront IAW requirements defined in KMI 3300.	3.2.3.2 - Connection Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0094	The NGLD-M shall allow for the creation, deletion and management of connections to the NGLD-M Mobile Device PDE Storefront IAW requirements defined in KMI 3300.	3.2.3.2 - Connection Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0095	The NGLD-M shall allow for the creation, deletion and management of connections to the KMI Device PDE Storefront IAW requirements defined in KMI 3300.	3.2.3.2 - Connection Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0096	The NGLD-M shall allow for the creation, deletion and management of connections to the KMI MGC Device PDE Storefront IAW requirements defined in KMI 3300.	3.2.3.2 - Connection Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0097	The NGLD-M shall allow connections to the iApp OTNK-Compliant Device PDE Storefront to be configured for High Assurance Authentication (i.e. using the NGLD-M Type 1 PKI Credentials).	3.2.3.2 - Connection Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0098	The NGLD-M shall allow connections to the NGLD-M Mobile Device PDE Storefront to be configured for High Assurance Authentication (i.e.	3.2.3.2 - Connection Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	No

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
	using the NGLD-M High Assurance PKI Credentials).		6.2.5 Data Transfer KSA				
NGLD-M_SRD_0099	The NGLD-M shall allow connections to the KMI Device PDE Storefront to be configured for High Assurance Authentication (i.e. using the NGLD-M High Assurance PKI Credentials).	3.2.3.2 - Connection Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0100	The NGLD-M shall allow connections to the KMI MGC Device PDE Storefront to be configured for High Assurance Authentication (i.e. using the NGLD-M High Assurance PKI Credentials).	3.2.3.2 - Connection Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0101	The NGLD-M shall allow connections to the iApp OTNK-Compliant Device PDE Storefront to be configured for Medium Assurance Authentication (i.e. using the NGLD-M Medium Assurance PKI Credentials).	3.2.3.2 - Connection Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0102	The NGLD-M shall allow connections to the NGLD-M Mobile Device PDE Storefront to be configured for Medium Assurance Authentication (i.e. using the NGLD-M Medium Assurance PKI Credentials).	3.2.3.2 - Connection Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0103	The NGLD-M shall allow connections to the KMI Device PDE Storefront to be configured for Medium Assurance Authentication (i.e. using the NGLD-M Medium Assurance PKI Credentials).	3.2.3.2 - Connection Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0104	The NGLD-M shall allow connections to the KMI MGC Device PDE Storefront to be configured for Medium Assurance Authentication (i.e. using the NGLD-M Medium Assurance PKI Credentials).	3.2.3.2 - Connection Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0105	The NGLD-M shall allow connections to the iApp Last Mile API (LMA) to be established.	3.2.3.2 - Connection Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0106	The NGLD-M shall allow connections to another NGLD-M Last Mile API (LMA) to be established.	3.2.3.2 - Connection Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0907	The NGLD-M shall continue to operate during network packet loss. The Vendor shall define the acceptable packet loss based type of network and type of data being transmitted,	3.2.3.2 - Connection Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0107	The NGLD-M shall support cryptographic products management capabilities.	3.2.3.3 - Cryptographic Product Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0108	The NGLD-M shall display CMS packages available on the local device that are wrapped for High Assurance KMI-Aware devices.	3.2.3.3 - Cryptographic Product Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0109	The NGLD-M shall display CMS packages available on the local device that are wrapped for Medium Assurance KMI-Aware devices.	3.2.3.3 - Cryptographic Product Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0110	The NGLD-M shall inform the user which device a CMS Package is wrapped for (i.e. Device ESN).	3.2.3.3 - Cryptographic Product Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0111	The NGLD-M shall be able to display a list of SW/FW products that have been shared (pushed to) the NGLD-M device or retrieved from the iApp Intermediary.	3.2.3.3 - Cryptographic Product Management	6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	O	Yes	Yes
NGLD-M_SRD_0112	The NGLD-M shall maintain the identifying data and history of cryptographic key holdings.	3.2.3.3 - Cryptographic Product Management	6.2.1 Mission Data Services KPP 6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0113	The NGLD-M shall support the use of keys according to their tag or ID information.	3.2.3.3 - Cryptographic Product Management	6.2.1 Mission Data Services KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0114	The NGLD-M shall support the enforcement of the security policy that specifies the classification level of each cryptographic processing services in use.	3.2.3.3 - Cryptographic Product Management	6.2.1 Mission Data Services KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0115	The NGLD-M shall ensure that keys are implemented for a specific application.	3.2.3.3 - Cryptographic Product Management	6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0116	The NGLD-M shall ensure that keys are implemented in accordance with the specified classification key.	3.2.3.3 - Cryptographic Product Management	6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0117	The NGLD-M shall ensure that keys are implemented using the specified key type.	3.2.3.3 - Cryptographic Product Management	6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0118	The NGLD-M shall ensure that keys are implemented using a key with its specified algorithm.	3.2.3.3 - Cryptographic Product Management	6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0119	The NGLD-M shall ensure that keys are implemented using the key within its specified compartment.	3.2.3.3 - Cryptographic Product Management	6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0120	The NGLD-M shall utilize keys that have passed integrity tests and reject those that do not.	3.2.3.3 - Cryptographic Product Management	6.2.1 Mission Data Services KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0121	The NGLD-M shall identify keys using the key tag standard in accordance with EKMS 308.	3.2.3.3 - Cryptographic Product Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0122	The NGLD-M shall be capable of binding key tagging and ID information to a key.	3.2.3.3 - Cryptographic Product Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0123	The NGLD-M shall provide the capability to incorporate key tag formats or data that are defined by KMI OTNK specifications.	3.2.3.3 - Cryptographic Product Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	O	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0124	The NGLD-M shall provide the capability to manage Keys and Key Tags. Manage Keys and Key Tags includes: Add, Edit, View, Delete, Assign, Unassign, Manage Effective Dates, Manage Expired Keys/Key Tags, Manage File Headers.	3.2.3.3.1 - Cryptographic Keys / Key Tag Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0125	The NGLD-M shall provide the capability to add key tag for symmetric keys.	3.2.3.3.1 - Cryptographic Keys / Key Tag Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0126	The NGLD-M shall provide the capability to view keys/key tags.	3.2.3.3.1 - Cryptographic Keys / Key Tag Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0127	The NGLD-M shall provide the capability to delete keys/key tags.	3.2.3.3.1 - Cryptographic Keys / Key Tag Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0128	The NGLD-M shall provide the capability to delete/destroy keys/key tags.	3.2.3.3.1 - Cryptographic Keys / Key Tag Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0129	The NGLD-M shall provide the capability to assign keys/key tags to device fill locations.	3.2.3.3.1 - Cryptographic Keys / Key Tag Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0130	The NGLD-M shall provide the capability to unassign keys/key tags from device fill locations.	3.2.3.3.1 - Cryptographic Keys / Key Tag Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0131	The NGLD-M shall provide the capability to manage keys/key tags effective dates.	3.2.3.3.1 - Cryptographic Keys / Key Tag Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0132	The NGLD-M shall provide the capability to manage expired keys/key tags.	3.2.3.3.1 - Cryptographic Keys / Key Tag Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0133	The NGLD-M shall provide the capability to manage file headers for keys/key tags.	3.2.3.3.1 - Cryptographic Keys / Key Tag Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0134	The NGLD-M shall support cryptographic keys in both EKMS 317 generic fill format and DS-100-1 tagged key data formats.	3.2.3.3.1 - Cryptographic Keys / Key Tag Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0135	The NGLD-M shall provide the capability to manage mission plans.	3.2.3.4 - Mission Plan Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0136	The NGLD-M shall provide the capability to manage Platform Groups.	3.2.3.4.1 - Platform Group Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0137	The NGLD-M shall provide the capability to add a platform group.	3.2.3.4.1 - Platform Group Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0138	The NGLD-M shall provide the capability to edit a platform group.	3.2.3.4.1 - Platform Group Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0139	The NGLD-M shall provide the capability to view platform groups.	3.2.3.4.1 - Platform Group Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0140	The NGLD-M shall provide the capability to delete platform group.	3.2.3.4.1 - Platform Group Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0141	The NGLD-M shall provide the capability to manage Platforms. Manage Platforms includes: Add, Edit, View, Delete, Assign, Unassign.	3.2.3.4.2 - Platform Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0142	The NGLD-M shall provide the capability to add a platform.	3.2.3.4.2 - Platform Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0143	The NGLD-M shall provide the capability to edit a platform.	3.2.3.4.2 - Platform Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0144	The NGLD-M shall provide the capability to view platforms.	3.2.3.4.2 - Platform Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0145	The NGLD-M shall provide the capability to delete platform.	3.2.3.4.2 - Platform Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0146	The NGLD-M shall provide the capability to assign platforms to platform groups.	3.2.3.4.2 - Platform Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0147	The NGLD-M shall provide the capability to unassign a platform from a platform group.	3.2.3.4.2 - Platform Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0148	The NGLD-M shall provide the capability to manage Devices. Manage Devices includes: Add, Edit, View, Delete, Assign, Unassign.	3.2.3.4.3 - Device Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0149	The NGLD-M shall provide the capability to add a device instance for the supported device types.	3.2.3.4.3 - Device Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0150	The NGLD-M shall provide the capability to edit a device instance.	3.2.3.4.3 - Device Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0151	The NGLD-M shall provide the capability to view device instances.	3.2.3.4.3 - Device Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0152	The NGLD-M shall provide the capability to delete device instances.	3.2.3.4.3 - Device Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0153	The NGLD-M shall provide the capability to assign device instances to platforms.	3.2.3.4.3 - Device Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0154	The NGLD-M shall provide the capability to unassign device instances from platforms.	3.2.3.4.3 - Device Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0155	The NGLD-M shall provide the capability to manage SOI Data. Manage SOI Data includes: Display, Delete.	3.2.3.4.4 - Signal Operating Instruction (SOI) Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0156	The NGLD-M shall provide the capability to view SOI Data.	3.2.3.4.4 - Signal Operating Instruction (SOI) Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0157	The NGLD-M shall provide the capability to delete SOI Data.	3.2.3.4.4 - Signal Operating Instruction (SOI) Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0158	The NGLD-M shall provide the capability to manage Benign Fill Messages. Manage Benign Fill Messages includes: View, Assign, Unassign, Delete.	3.2.3.4.5 - Benign Fill (BF) Message Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0159	The NGLD-M shall provide the capability to view Benign Fill Messages.	3.2.3.4.5 - Benign Fill (BF) Message Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0160	The NGLD-M shall provide the capability to delete Benign Fill Messages.	3.2.3.4.5 - Benign Fill (BF) Message Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0161	The NGLD-M shall provide the capability to assign Benign Fill Messages to device fill locations.	3.2.3.4.5 - Benign Fill (BF) Message Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0162	The NGLD-M shall provide the capability to unassign Benign Fill Messages from device fill locations.	3.2.3.4.5 - Benign Fill (BF) Message Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0163	The NGLD-M shall provide the capability to manage EP Data. Manage EP Data includes: View, Assign, Unassign, Delete.	3.2.3.4.6 - Electronic Protection (EP) Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0164	The NGLD-M shall provide the capability to view EP Data.	3.2.3.4.6 - Electronic Protection (EP) Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0165	The NGLD-M shall provide the capability to delete EP Data.	3.2.3.4.6 - Electronic Protection (EP) Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0166	The NGLD-M shall provide the capability to assign EP Data to device fill locations.	3.2.3.4.6 - Electronic Protection (EP) Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0167	The NGLD-M shall provide the capability to unassign EP Data from device fill locations.	3.2.3.4.6 - Electronic Protection (EP) Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0168	The NGLD-M shall provide the capability to manage Message Data. Manage Message Data includes: View, Assign, Unassign, Delete.	3.2.3.4.7 - Message Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0169	The NGLD-M shall provide the capability to view Message Data.	3.2.3.4.7 - Message Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0170	The NGLD-M shall provide the capability to delete Message Data.	3.2.3.4.7 - Message Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0171	The NGLD-M shall provide the capability to assign Message Data to device fill locations.	3.2.3.4.7 - Message Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0172	The NGLD-M shall provide the capability to unassign Message Data from device fill locations.	3.2.3.4.7 - Message Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0173	The NGLD-M shall provide the capability to create B1 and B2 data for specific ECUs.	3.2.3.4.7 - Message Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0174	The NGLD-M shall provide the capability to manage Radio Configuration Files (RCF). Manage Radio Configuration Files (RCF) includes: View, Delete.	3.2.3.4.8 - Radio Configuration Files (RCF) Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0175	The NGLD-M shall provide the capability to view RCF data.	3.2.3.4.8 - Radio Configuration Files (RCF) Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0176	The NGLD-M shall provide the capability to delete RCF data.	3.2.3.4.8 - Radio Configuration Files (RCF) Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0177	The NGLD-M shall provide the capability to manage Fill Device Audit Data. Manage Files includes: View, Upload, Clear.	3.2.3.5 - Audit Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0178	The NGLD-M shall provide the capability to view audit data.	3.2.3.5 - Audit Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0179	The NGLD-M shall provide the capability to upload audit data.	3.2.3.5 - Audit Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0180	The NGLD-M shall provide the capability to reset/clear audit data.	3.2.3.5 - Audit Data Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0181	The NGLD-M shall provide the capability to manage benign keying and benign fill of F-22 ECU. Manage F-22 includes: manage benign keying, manage benign fill, manage benign	3.2.3.6 - F-22 ECU Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
	rekeying, Modify the state of the F-22 ECUs, Emergency Rekey (REDBALL).						
NGLD-M_SRD_0182	The NGLD-M shall provide the capability to manage the benign keying process for the F-22 ECUs.	3.2.3.6 - F-22 ECU Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0183	The NGLD-M shall provide the capability to manage the benign fill process for the F-22 ECUs.	3.2.3.6 - F-22 ECU Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0184	The NGLD-M shall provide the capability to manage the state of the F-22 ECUs during the benign keying and benign fill process.	3.2.3.6 - F-22 ECU Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0185	The NGLD-M shall support the F-22 ECU Emergency Rekey (REDBALL) process.	3.2.3.6 - F-22 ECU Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0186	The NGLD-M shall provide the capability to manage TrKEKs. Manage TrKEKs includes: View as a key (host-side database), View filled TrKEKs, Delete filled TrKEKs.	3.2.3.7 - TrKEK Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0187	The NGLD-M shall provide the capability to view TrKEKs that are filled into the NGLD-M.	3.2.3.7 - TrKEK Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0188	The NGLD-M shall provide the capability to delete TrKEKs that are filled into the NGLD-M.	3.2.3.7 - TrKEK Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0189	The NGLD-M shall provide the capability to manage files received into system.	3.2.3.8 - File Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0190	The NGLD-M shall provide the capability to view files received into system.	3.2.3.8 - File Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0191	The NGLD-M shall provide the capability to rename files received into system.	3.2.3.8 - File Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0192	The NGLD-M shall provide the capability to delete files received into system.	3.2.3.8 - File Management	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0193	The NGLD-M shall have the ability to utilize "Cloud Operations/Data Center" to securely backup NGLD-M images for emergency restoration/cloning.	3.2.3.9 - NGLD-M System Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	O	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0194	The NGLD-M shall support the management operations for external physical interfaces.	3.2.3.9 - NGLD-M System Management	6.1.3 Net- Ready 6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0195	The NGLD-M shall support the management operations for software/firmware updates.	3.2.3.9 - NGLD-M System Management	6.1.3 Net- Ready 6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0196	The NGLD-M shall support the management operations for date/time.	3.2.3.9 - NGLD-M System Management	6.1.3 Net- Ready 6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0197	The NGLD-M shall support the ability to view the crypto subsystem status.	3.2.3.9 - NGLD-M System Management	6.1.3 Net- Ready 6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0198	The NGLD-M shall support the management operations for backup/recovery of configuration data.	3.2.3.9 - NGLD-M System Management	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0199	The NGLD-M shall allow users to post products to the local OTNK-Compliant device storefront on the NGLD-M.	3.2.3.10 - NGLD-M Mobile Device Storefront Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0200	The NGLD-M shall allow users to manage authorization / access to products posted to the local OTNK-Compliant	3.2.3.10 - NGLD-M Mobile Device Storefront Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
	device storefront on the NGLD-M.		6.2.5 Data Transfer KSA				
NGLD-M_SRD_0201	The NGLD-M shall provide an OTNK-Compliant Storefront capable of providing Product Availability Lists (PALs) to consumers / clients.	3.2.3.10 - NGLD-M Mobile Device Storefront Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0202	The NGLD-M shall allow users to view products previously posted to the local OTNK-Compliant device storefront on the NGLD-M.	3.2.3.10 - NGLD-M Mobile Device Storefront Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0203	The NGLD-M shall allow users to remove products previously posted to the local OTNK-Compliant device storefront on the NGLD-M.	3.2.3.10 - NGLD-M Mobile Device Storefront Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0204	The NGLD-M shall allow users to register / configure devices allowed to authenticate / communicate with the local OTNK-Compliant storefront on the NGLD-M.	3.2.3.10 - NGLD-M Mobile Device Storefront Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0205	The NGLD-M UAS shall allow authentication credentials / certificates to be imported and associated to known/registered devices which will be used while authenticating devices to the local OTNK-Compliant device storefront on the NGLD-M UAS.	3.2.3.10 - NGLD-M Mobile Device Storefront Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0206	The NGLD-M shall support the management of receive operations using a Fill Port interface.	3.2.4 - Receiving	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0207	The NGLD-M shall support the management of receive operations using a Network interface.	3.2.4 - Receiving	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0208	The NGLD-M shall support the management of receive operations using a USB interface.	3.2.4 - Receiving	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0209	The NGLD-M shall provide the capability to receive control/status information from the fill port interface.	3.2.4 - Receiving	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0210	The NGLD-M shall receive cryptographic keys and non-key data per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4 - Receiving	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0211	The NGLD-M shall support the DS-101/DS-102/RS-232 protocols for receipt of cryptographic key and non-key mission data in accordance with EKMS 308.	3.2.4 - Receiving	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0212	The NGLD-M shall support receipt of cryptographic keys and non-key mission data in accordance with the CT3 ICD Version 3.20 interface protocols.	3.2.4 - Receiving	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0213	The NGLD-M shall receive Mission Payload Data per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.1 - Receive Mission Plan Data	6.1.3 Net-Ready	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0214	The NGLD-M shall receive Platform Group per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.1.1 - Receive Platform Group	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0215	The NGLD-M shall receive Platform per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.1.2 - Receive Platform	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0216	The NGLD-M shall receive Device per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.1.3 - Receive Device	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0217	The NGLD-M shall receive cryptographic keys from the equipment specified in Table 6 – NGLD-M Legacy Device Key Sources.	3.2.4.1.4 - Receive Cryptographic Key/Key Tag	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0218	The NGLD-M shall receive cryptographic Keys/Key Tags using defined interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.1.4 - Receive Cryptographic Key/Key Tag	6.1.3 Net-Ready	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0219	The NGLD-M shall perform key-needed functions.	3.2.4.1.4 - Receive Cryptographic Key/Key Tag	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0220	The NGLD-M shall receive EP Data per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.1.5 - Receive EP Data	6.1.3 Net-Ready	Demonstration	T	Yes	No
NGLD-M_SRD_0221	The NGLD-M shall receive Message Data per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.1.6 - Receive Message Data	6.1.3 Net-Ready	Demonstration	T	Yes	No
NGLD-M_SRD_0222	The NGLD-M shall receive Benign Fill Messages data per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.1.7 - Receive Benign Fill (BF) Message	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0223	The NGLD-M shall support receipt of Benign fill in accordance with applicable sections of EKMS 217 (benign technique specification), EKMS 308, EKMS 317, and EKMS 322.	3.2.4.1.7 - Receive Benign Fill (BF) Message	6.1.3 Net-Ready	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0224	The NGLD-M shall receive SOI Data per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.1.8 - Receive SOI Data	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP.	Demonstration	T	Yes	No
NGLD-M_SRD_0225	The NGLD-M shall receive Radio Configuration File (RCF) data per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.1.9 - Receive RCF	6.1.3 Net-Ready	Demonstration	T	Yes	No
NGLD-M_SRD_0226	The NGLD-M shall receive SINCGARS Loadsets data per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.1.10 - Receive SINCGARS Loadset	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0227	The NGLD-M shall provide the capability to Receive Audit Data that has been shared with the NGLD-M's Last Mile API.	3.2.4.2.1 - Receive Audit Data	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0228	The NGLD-M shall receive Audit Data per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.2.1 - Receive Audit Data	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0229	The NGLD-M shall import X.509 PKI public certificates.	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0230	The NGLD-M shall import X.509 PKI public certificates via the fill port using defined serial protocols from the MGC and other NGLD-M(s).	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0231	The NGLD-M shall import X.509 PKI public certificates via the USB port using device defined standards.	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0232	The NGLD-M shall import X.509 PKI public certificates via the Ethernet port using device defined standards.	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0233	The NGLD-M shall import X.509 PKI public certificates via the Ethernet port from KMI-OTNK Compliant Storefronts.	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	O	Yes	Yes
NGLD-M_SRD_0234	The NGLD-M shall store imported X.509 public certificates.	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0235	The NGLD-M shall import trust anchors.	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0236	The NGLD-M shall import trust anchors via the fill port using defined serial protocols from the MGC and other NGLD-M(s).	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0237	The NGLD-M shall import trust anchors via the USB port using device defined standards.	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0238	The NGLD-M shall import trust anchors via the Ethernet port using device defined standards.	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0239	The NGLD-M shall import trust anchors via the Ethernet port from the LMA interface and other NGLD-M(s).	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0240	The NGLD-M shall import trust anchors via the Ethernet port from KMI-OTNK Compliant Storefront.	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	O	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0241	The NGLD-M shall import CSRs.	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0242	The NGLD-M shall import CSRs via the fill port using defined serial protocols from ECUs and other NGLD-M(s).	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0243	The NGLD-M shall import CSRs via the USB port using device defined standards.	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0244	The NGLD-M shall import CSRs via the Ethernet port using device defined standards.	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0245	The NGLD-M shall import CSRs via the Ethernet port from the LMA interface and other NGLD-M(s).	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0246	The NGLD-M shall import CSRs via the Ethernet port from KMI-OTNK Compliant Storefronts.	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	O	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0247	The NGLD-M shall receive Certificates data per the interfaces and formats identified in Table 5– NGLD-M Receiving Data Types and Interfaces.	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0248	The NGLD-M shall import X.509 PKI public certificates via the Ethernet port from the LMA interface and other NGLD-M(s).	3.2.4.2.2 - Receive Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0249	The NGLD-M shall receive Certificate Revocation Lists (CRL) data per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.2.3 - Receive CRLs	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0250	The NGLD-M shall receive Authority Revocation Lists (ARL) data per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.2.4 - Receive ARLs	6.1.3 Net-Ready	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0251	The NGLD-M shall receive Device Configuration Settings data per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.2.5 - Receive Device Configuration Settings	6.1.3 Net-Ready	Demonstration	T	Yes	No
NGLD-M_SRD_0252	The NGLD-M shall receive Software/Firmware data (including IAVA patches) per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.2.6 - Receive Software/Firmware	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0253	The NGLD-M shall receive Health and Monitoring Data that has been shared with the NGLD-M's Last Mile API.	3.2.4.2.7 - Receive Health and Monitoring Data	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0254	The NGLD-M shall receive Health and Monitoring Data per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.2.7 - Receive Health and Monitoring Data	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0255	The NGLD-M shall be able to perform decryption and processing on CMS Packages determined to have been wrapped for the High	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
	Assurance Credentials of the NGLD-M.						
NGLD-M_SRD_0256	The NGLD-M UAS shall be able to perform signature validation on CMS Packages that were retrieved from an OTNK-Compliant Device PDE Storefront using the Medium Assurance Credentials of the NGLD-M.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0257	The NGLD-M shall be able to perform decryption and processing on CMS Packages determined to have been wrapped for the Medium Assurance Credentials of the NGLD-M.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0258	The NGLD-M shall provide persistence of black products that have been processed / extracted from a CMS Package (e.g., 1208, 1213 packages).	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0259	The NGLD-M shall direct the persistence/handling/wrapping of red products that were wrapped for the NGLD-M (high assurance credentials) and have been processed /	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
	extracted from a CMS Package (e.g., 1104, 1102 packages).						
NGLD-M_SRD_0260	The NGLD-M shall display available metadata about CMS Packages that have been downloaded from an OTNK-Compliant Device PDE Storefront.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0261	The NGLD-M shall perform TLS mutual authentication when using medium assurance credentials to communicate with an OTNK-Compliant Storefront (IAW the latest KMI Over-the-Network-Keying (OTNK) Specification available, currently version 3.1.2.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0262	The NGLD-M shall perform TLS mutual authentication when using high assurance credentials to communicate with an OTNK-Compliant Storefront (IAW the latest KMI Over-the-Network-Keying (OTNK) Specification available, currently version 3.1.2.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0263	The NGLD-M shall be able to retrieve a Product Availability List (PAL) from all supported OTNK-Compliant Device PDE Storefronts using the High Assurance Credentials of the NGLD-M.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0264	The NGLD-M shall be able to retrieve a Product Availability List (PAL) from all supported OTNK-Compliant Device PDE Storefronts using the Medium Assurance Credentials of the NGLD-M.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0265	The NGLD-M shall be able handle error responses returned from all supported OTNK-Compliant Device PDE Storefronts when retrieving a PAL by using the High Assurance Credentials of the NGLD-M.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0266	The NGLD-M shall be able handle error responses returned from all supported OTNK-Compliant Device PDE Storefronts when retrieving a PAL by using the Medium Assurance Credentials of the NGLD-M.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0267	The NGLD-M shall be able to download products (using the information presented in the PAL) from all supported OTNK-Compliant Device PDE Storefronts using the High Assurance Credentials of the NGLD-M.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0268	The NGLD-M shall be able to download products (using the information presented in the PAL) from all supported OTNK-Compliant Device PDE Storefronts using the Medium Assurance Credentials of the NGLD-M.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0269	The NGLD-M shall support processing of CMS-wrapped products. Note: The Government team will define the specific CMS packages that needs to be implemented based on available templates within KMI.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0270	The NGLD-M shall display information about the CMS Packages and Products downloaded using the High Assurance Credentials of the NGLD-M.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0271	The NGLD-M shall display information about the CMS Packages and Products downloaded using the Medium Assurance Credentials of the NGLD-M.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0272	The NGLD-M shall be able handle error responses returned from all supported OTNK-Compliant Device PDE Storefronts when downloading products by using the High Assurance Credentials of the NGLD-M.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0273	The NGLD-M shall be able handle error responses returned from all supported OTNK-Compliant Device PDE Storefronts when downloading products by using the Medium Assurance Credentials of the NGLD-M.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0274	The NGLD-M shall be able to receive an OTNK message instructing the NGLD-M to return its internal ESN.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	No

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0275	The NGLD-M shall maintain the identifying data and history of cryptographic key holdings.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.2.1 Mission Data Services KPP 6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0276	The NGLD-M shall receive CMS Packages data per the interfaces and formats identified in Table 5 – NGLD-M Receiving Data Types and Interfaces.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0277	The NGLD-M shall provide persistence for CMS-wrapped products that are destined for medium assurance KMI-aware devices.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0278	The NGLD-M shall provide persistence for CMS-wrapped products that are destined for medium assurance KMI-aware devices.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0279	The NGLD-M shall provide persistence for CMS-wrapped products that are destined for high assurance KMI-aware devices.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0280	The NGLD-M shall provide persistence for CMS-wrapped products that are destined for legacy (non KMI-Aware) devices.	3.2.4.3 - Receive Cryptographic Products and CMS Packages	6.1.3 Net-Ready	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0281	The NGLD-M supports secure and non-secure storage of data such as mission data, device configuration files, audit logs, and electronic keys.	3.2.5 - Storage	6.2.6 Data Storage KSA	Test	T	Yes	Yes
NGLD-M_SRD_0282	The crypto will reserve fifty percent of its internal logic space when fully programmed for a specific implementation and fifty percent of its internal memory capacity reserve when configured for a specific implementation.	3.2.5 - Storage	6.2.6 Data Storage KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0283	The NGLD-M shall support an internal CRL of at least 4 MB in size.	3.2.5 - Storage	6.1.3 Net-Ready, 6.2.2 Interoperability, Standardization and commonality KPP, 6.2.8 Security KSA.	Demonstration	T	Yes	Yes
NGLD-M_SRD_0284	The NGLD-M shall support an internal ARL of at least 4 MB in size.	3.2.5 - Storage	6.1.3 Net-Ready, 6.2.2 Interoperability, Standardization and commonality KPP, 6.2.8 Security KSA.	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0285	The NGLD-M shall have a storage capacity of 128 GB or greater.	3.2.5 - Storage	6.1.3 - Net Ready 6.2.6 - Data Storage KSA 6.2.10 - Environmental Durability Additional Attribute 8.3.3 - NSS System Support Description 8.4 Bandwidth Requirement 11.5 Technology Readiness Level (TRL) Estimate at Milestone C 14.5 - Materiel	Test	T	No	Yes
NGLD-M_SRD_0286	The NGLD-M shall support minimum of 512 MB of program storage.	3.2.5 - Storage	6.1.3 - Net Ready 6.2.6 - Data Storage KSA 6.2.10 - Environmental Durability Additional Attribute 8.3.3 - NSS System Support Description 8.4 Bandwidth Requirement 11.5 Technology Readiness Level (TRL) Estimate at Milestone	Test	T	No	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
			C 14.5 - Materiel				
NGLD-M_SRD_0287	The NGLD-M shall support minimum of 4 GB of RAM.	3.2.5 - Storage	6.1.3 - Net Ready 6.2.6 - Data Storage KSA 6.2.10 - Environmental Durability Additional Attribute 8.3.3 - NSS System Support Description 8.4 Bandwidth Requirement 11.5 Technology Readiness Level (TRL) Estimate at Milestone C 14.5 - Materiel	Demonstration	T	No	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0288	The NGLD-M shall support storage of minimum 8 MB Audit log.	3.2.5 - Storage	6.1.3 - Net Ready 6.2.6 - Data Storage KSA 6.2.10 - Environmental Durability Additional Attribute 8.3.3 - NSS System Support Description 8.4 Bandwidth Requirement 11.5 Technology Readiness Level (TRL) Estimate at Milestone C 14.5 - Materiel	Test	T	Yes	Yes
NGLD-M_SRD_0291	The NGLD-M shall support the management of distribution operations using a Fill Port interface.	3.2.6 - Distributing	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0292	The NGLD-M shall support the management of distribution operations using a Network interface.	3.2.6 - Distributing	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0293	The NGLD-M shall support the management of distribution operations using a USB interface.	3.2.6 - Distributing	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0294	The NGLD-M shall maintain the identifying data and history of cryptographic key holdings.	3.2.6 - Distributing	6.2.1 Mission Data Services KPP 6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0295	The NGLD-M shall provide the capability to send control/status information to the fill port interface.	3.2.6 - Distributing	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0296	The NGLD-M shall support transmission of key loads in accordance with EKMS 308.	3.2.6.1 - Cryptographic Key Issue	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0297	The NGLD-M shall distribute cryptographic keys and data, using the defined protocols and formats identified in Table 7 –	3.2.6.1 - Cryptographic Key Issue	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
	NGLD-M Distribution Data Types and Interfaces.						
NGLD-M_SRD_0298	The NGLD-M shall provide the capability to distribute (cryptographic key and non-key) data to other systems.	3.2.6.1 - Cryptographic Key Issue	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0299	The NGLD-M shall issue unencrypted key packages.	3.2.6.1 - Cryptographic Key Issue	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0300	The NGLD-M shall issue encrypted key packages.	3.2.6.1 - Cryptographic Key Issue	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0301	The NGLD-M shall provide the capability to Command OTAD capable ECUs to generate keys and distribute them to other devices.	3.2.6.1 - Cryptographic Key Issue	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0302	The NGLD-M shall distribute Keys per the protocols, formats and interfaces identified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.1 - Cryptographic Key Issue	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0303	The NGLD-M shall distribute cryptographic Key and Non-Key Data to the devices specified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.1 - Cryptographic Key Issue	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0304	The NGLD-M shall support the DS-101/DS-102/RS-232 protocols for key issue in accordance with EKMS 308.	3.2.6.1 - Cryptographic Key Issue	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0305	The NGLD-M shall support the DS-101/DS-102/RS-232 protocols for key fill port in accordance with EKMS 308.	3.2.6.2 - Cryptographic Key Fill	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0306	The NGLD-M supports the transmission of key data and non-key mission data to the equipment specified in Table 8 – NGLD-M Supported Equipment Profiles	3.2.6.2 - Cryptographic Key Fill	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0307	The NGLD-M shall provide for the decryption of TrKEK encrypted keys prior to unencrypted DS-101 NSA 90-02A fill process.	3.2.6.2 - Cryptographic Key Fill	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0308	The NGLD-M shall support the DS-101/DS-102/RS-232 protocols for key fill in accordance with EKMS 308.	3.2.6.2 - Cryptographic Key Fill	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0309	The NGLD-M shall support unassigned key fill.	3.2.6.2.1 - Unassigned Cryptographic Key Fill	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0310	The NGLD-M shall support platform-based key fill.	3.2.6.2.2 - Platform-Based Cryptographic Key Fill	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0311	The NGLD-M shall support equipment-based key fill.	3.2.6.2.3 - Equipment-Based Cryptographic Key Fill	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0312	The NGLD-M shall distribute Mission Payload Data per the protocols, formats and interfaces identified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.3 - Distribute Mission Plan Data	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0313	The NGLD-M shall distribute Platform Groups per the protocols, formats and interfaces identified in Table 7	3.2.6.3.1 - Distribute Platform Group	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
	– NGLD-M Distribution Data Types and Interfaces.		6.2.5 Data Transfer KSA				
NGLD-M_SRD_0314	The NGLD-M shall distribute Platforms per the protocols, formats and interfaces identified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.3.2 - Distribute Platform	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0315	The NGLD-M shall distribute Devices per the protocols, formats and interfaces identified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.3.3 - Distribute Device	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0316	The NGLD-M shall provide capability to output key tagging and ID information.	3.2.6.3.4 - Distribute Cryptographic Key Tag	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0317	The NGLD-M shall distribute Key Tags per the protocols, formats and interfaces identified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.3.4 - Distribute Cryptographic Key Tag	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0318	The NGLD-M shall distribute EP Data per the protocols, formats and interfaces identified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.3.5 - Distribute EP Data	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0319	The NGLD-M shall distribute Message Data per the protocols, formats and interfaces identified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.3.6 - Distribute Message Data	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0320	The NGLD-M shall distribute Benign Fill Messages per the protocols, formats and interfaces identified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.3.7 - Distribute Benign Fill (BF) Message	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0321	The NGLD-M shall support the distribution of Benign fill in accordance with applicable sections of EKMS 217 (benign technique specification), EKMS 308, EKMS 317, and EKMS 322.	3.2.6.3.7 - Distribute Benign Fill (BF) Message	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0322	The NGLD-M shall distribute SOI Data per the protocols, formats and interfaces identified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.3.8 - Distribute SOI Data	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0323	The NGLD-M shall distribute Radio Configuration File (RCF) per the protocols, formats and interfaces identified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.3.9 - Distribute RCF	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0324	The NGLD-M shall distribute Device Configuration Settings per the protocols, formats and interfaces identified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.3.10 - Distribute Device Configuration Settings	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0325	The NGLD-M shall distribute Certificate Revocation Lists (CRL) per the protocols, formats and interfaces identified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.4 - Distribute CRLs	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0326	The NGLD-M shall transmit its own audit data over Fill Port.	3.2.6.5 - Distribute Audit Data	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.6 Data Storage KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0327	The NGLD-M shall distribute Fill Device Audit Data per the protocols, formats and interfaces identified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.5 - Distribute Audit Data	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0328	The NGLD-M shall transmit its own audit data over Ethernet.	3.2.6.5 - Distribute Audit Data	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0329	The NGLD-M shall distribute CMS Packages per the protocols, formats and interfaces identified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.6 - Distribute CMS Packages	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0330	The NGLD-M shall act as an intermediary to deliver CMS-wrapped products that are destined for medium assurance and high assurance KMI-aware devices.	3.2.6.6 - Distribute CMS Packages	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0331	The NGLD-M shall ensure proper tracking (when accounting is not required by policy) is performed when distributing CMS Packages that are wrapped for another High Assurance KMI-Aware device.	3.2.6.6 - Distribute CMS Packages	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0332	The NGLD-M shall ensure proper tracking (when accounting is not required by policy) is performed when distributing CMS Packages that are wrapped for another Medium Assurance KMI-Aware device.	3.2.6.6 - Distribute CMS Packages	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0333	The NGLD-M shall be capable of exporting CMS packages intact that are destined for consumption by an external target KMI-Aware Device (without any parsing or modification to the source package).	3.2.6.6 - Distribute CMS Packages	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0334	The NGLD-M shall have the ability to manage as a Mediator to deliver CMS-wrapped products that are destined for external legacy non KMI-Aware devices.	3.2.6.6 - Distribute CMS Packages	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0335	The NGLD-M shall act as an intermediary to deliver CMS-wrapped products that are destined for medium assurance and high assurance KMI-aware devices.	3.2.6.6 - Distribute CMS Packages	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0336	The NGLD-M shall have the ability to manage as a mediator to deliver CMS-wrapped products that are destined for external legacy non KMI-Aware devices. Note: NGLD-M unwraps the CMS packages and can provide products to the legacy device.	3.2.6.6 - Distribute CMS Packages	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0337	The NGLD-M shall communicate with a target KMI-Aware ECU, retrieve the Electronic Serial Number (ESN) from the target ECU, compare that ESN with The NGLD-M product inventory, and display the available products for loading to the target ECU.	3.2.6.6 - Distribute CMS Packages	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0338	The NGLD-M shall be capable of allowing for the generation and binding of key tag data. NOTE: This is objective until OTNK 3.1.1+ is released. OTNK v2.2 does not support this feature.	3.2.6.6 - Distribute CMS Packages	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	O	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0339	The NGLD-M shall be able to initiate distribution of CMS Packages that have been re-wrapped for target KMI-Aware Devices by the High Assurance Credentials of the NGLD-M.	3.2.6.6 - Distribute CMS Packages	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA	Demonstration	O	Yes	Yes
NGLD-M_SRD_0340	The NGLD-M shall be able to initiate distribution of CMS Packages that have been re-wrapped for target KMI-Aware Devices by the Medium Assurance Credentials of the NGLD-M.	3.2.6.6 - Distribute CMS Packages	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA	Demonstration	O	Yes	No
NGLD-M_SRD_0341	The NGLD-M shall distribute Certificates per the protocols, formats and interfaces identified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0342	The NGLD-M shall export X.509 PKI public certificates.	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0343	The NGLD-M shall export X.509 PKI public certificates via the fill port using defined serial protocols from the MGC and other NGLD-M(s).	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0344	The NGLD-M shall export X.509 PKI public certificates via the USB port using device defined standards.	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0345	The NGLD-M shall export X.509 PKI public certificates via the Ethernet port using device defined standards.	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0346	The NGLD-M shall export X.509 PKI public certificates via the Ethernet port from the LMA interface and other NGLD-M(s).	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0347	The NGLD-M shall export X.509 PKI public certificates via the Ethernet port from KMI-OTNK Compliant Storefronts.	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	O	Yes	Yes
NGLD-M_SRD_0348	The NGLD-M shall export trust anchors.	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0349	The NGLD-M shall export trust anchors via the fill port using defined serial protocols from the MGC and other NGLD-M(s).	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0350	The NGLD-M shall export trust anchors via the USB port using device defined standards.	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0351	The NGLD-M shall export trust anchors via the Ethernet port using device defined standards.	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0352	The NGLD-M shall export trust anchors via the Ethernet port from the LMA interface and other NGLD-M(s).	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0353	The NGLD-M shall export trust anchors via the Ethernet port from KMI-OTNK Compliant Storefronts.	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	O	Yes	Yes
NGLD-M_SRD_0354	The NGLD-M shall export CSRs.	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0355	The NGLD-M shall export CSRs via the fill port using defined serial protocols from the MGC and other NGLD-M(s).	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0356	The NGLD-M shall export CSRs via the USB port using device defined standards.	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0357	The NGLD-M shall export CSRs via the Ethernet port using device defined standards.	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0358	The NGLD-M shall export CSRs via the Ethernet port from the LMA interface and other NGLD-M(s).	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0359	The NGLD-M shall export CSRs via the Ethernet port from KMI-OTNK Compliant Storefronts.	3.2.6.7 - Distribute Certificate Products	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	O	Yes	Yes
NGLD-M_SRD_0360	The NGLD-M shall transmit its own health monitoring data over Ethernet.	3.2.6.8 - Distribute Health and Monitoring Data	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.6 Data Storage KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0361	The NGLD-M shall transmit its own health monitoring data over Fill Port.	3.2.6.8 - Distribute Health and Monitoring Data	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.6 Data Storage KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0362	The NGLD-M shall transmit its own health monitoring data over USB.	3.2.6.8 - Distribute Health and Monitoring Data	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.6 Data Storage KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0363	The NGLD-M shall distribute Health and Monitoring Data per the protocols, formats and interfaces identified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.8 - Distribute Health and Monitoring Data	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0364	The NGLD-M shall distribute Authority Revocation Lists (ARL) per the protocols, formats and interfaces identified in Table 7 – NGLD-M Distribution Data Types and Interfaces.	3.2.6.9 - Distribute ARLs	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0365	The NGLD-M Crypto shall implement the ACCORDIAN 1.3 algorithm for TrKEK encryption and decryption.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0366	The NGLD-M Crypto shall implement the ACCORDIAN 1.3 algorithm for internal key wrap.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0367	The NGLD-M Crypto shall implement the AES-256 Galois Counter Mode (GCM) algorithm for TLS.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0368	The NGLD-M Crypto shall implement the AES-256 or MEDLEY algorithm for Top Secret Data at Rest (DAR).	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0369	The NGLD-M Crypto shall implement the AES algorithm for non-security software confidentiality.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0370	The NGLD-M Crypto shall implement the SHA-256 and SHA-384 algorithm for TLS.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0371	The NGLD-M Crypto shall implement the ECDH-384 algorithm for key agreement.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0372	The NGLD-M Crypto shall implement the SPONDULIX-S algorithm for key agreement.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0373	The NGLD-M Crypto shall implement the AES Key Wrap algorithm for black key wrap.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0374	The NGLD-M Crypto shall implement the AES Key Wrap algorithm for internal key wrap.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0375	The NGLD-M shall implement the ACCORDIAN 3.0 algorithm for black key wrap.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0376	The NGLD-M shall implement the ACCORDIAN 3.0 algorithm for internal key wrap.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0377	The NGLD-M shall implement the ECDSA-384 algorithm for signatures.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0378	The NGLD-M shall implement the MEDLEY algorithm for non-security software confidentiality.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0379	The NGLD-M shall implement the WATARI algorithm for security and non-security software confidentiality.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0380	The NGLD-M shall implement the KM-TG-0002-96 algorithm for signature validation of signed software.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0381	The NGLD-M shall implement the KM-TG-0003-03 algorithm for signature validation of signed software.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0382	The NGLD-M shall implement the SILVER LINING algorithm for signature validation of signed software.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0383	The NGLD-M shall implement the RSA algorithm for signatures.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0384	The NGLD-M crypto shall be capable of instantiating any combination of the algorithms listed in Table 9 titled, "List of Algorithms".	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0385	The NGLD-M crypto shall decrypt and activate algorithms prior to operational use.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	No	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0386	The NGLD-M crypto shall test activated cryptographic algorithms for correct function prior to operational use.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Test	T	No	Yes
NGLD-M_SRD_0387	The NGLD-M shall support AES-GCM in accordance with National Institute for Standards and Technology (NIST) SP800-38D "The Galois/Counter Mode of Operation (GCM)", May 31 2005 for use with IPSEC.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0388	The NGLD-M shall support Hashed Message Authentication Code (HMAC) – Secure Hash Algorithm (SHA384) for use with IPSEC.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0389	The NGLD-M shall support ECDH for use with IPSEC.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0390	The NGLD-M shall verify digital signatures for software/firmware using ECDSA with 384 bits key length, as defined in a document: Federal Information Processing Standards Publication 186-4, “Digital Signature Standard”, July 19, 2013.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	No	Yes
NGLD-M_SRD_0391	The NGLD-M shall use WATARI algorithms for decrypting High Assurance (formerly Type 1) software distributions in accordance with NSA R21-Tech-24-05 and NSA R21-Tech-31-05.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	No	Yes
NGLD-M_SRD_0392	The NGLD-M shall use SPONDULIX – S for key agreement and key exchange.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0393	The NGLD-M shall support the Elliptic Curve Diffie-Hellman (ECDH) for key exchange and key agreement.	3.2.7.1 - Algorithms	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0394	The NGLD-M shall support the use of High Assurance and Medium Assurance certificates when a valid CIK is inserted.	3.2.7.2 - Key Pair Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.6 Data Storage KSA 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0395	The NGLD-M shall support the use of Medium Assurance certificates when a valid CIK is not inserted.	3.2.7.2 - Key Pair Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.6 Data Storage KSA 6.2.8 Security KSA	Test	T	Yes	No
NGLD-M_SRD_0396	The NGLD-M shall generate each public/private key pair and publish each public key in accordance with American National Standards Institute (ANSI) X9.42.	3.2.7.2 - Key Pair Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0397	The NGLD-M shall retain each private key, protect it from unauthorized access, and wrap it for storage.	3.2.7.2 - Key Pair Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.6 Data Storage KSA 6.2.8 Security KSA	Test	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0398	The NGLD-M shall generate certificate signing request materials based on public/private key pairs generated within the NGLD-M.	3.2.7.2 - Key Pair Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0399	The NGLD-M shall support validation of certificates whenever certificates are used by the system.	3.2.7.2 - Key Pair Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0400	The NGLD-M shall receive and manage X.509v3 signed certificates and their corresponding keys as required for KMI interoperability.	3.2.7.2 - Key Pair Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0401	The NGLD-M shall support the loading of PKI Certificates from authorized KMI PKI.	3.2.7.2 - Key Pair Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0402	The NGLD-M shall receive and manage X.509v3 signed certificates and their corresponding keys as required for Department of Defense (DoD) Public Key Infrastructure (PKI) interoperability.	3.2.7.2 - Key Pair Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0403	The NGLD-M shall support the loading of PKI Certificates from authorized DoD PKI.	3.2.7.2 - Key Pair Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0404	The NGLD-M shall accept, read, store, and utilize valid CRLs during certificate related validation operations.	3.2.7.2 - Key Pair Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0405	The NGLD-M shall accept, read, store, and utilize valid ARLs during certificate related validation operations.	3.2.7.2 - Key Pair Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0406	The NGLD-M shall provide sufficient warning before any certificate material expires.	3.2.7.2 - Key Pair Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0407	The NGLD-M shall indicate when certificate materials expire.	3.2.7.2 - Key Pair Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0408	The NGLD-M shall support the deletion of certificate materials.	3.2.7.2 - Key Pair Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.6 Data Storage	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
			KSA 6.2.8 Security KSA				
NGLD-M_SRD_0409	The NGLD-M shall support High Assurance IPSEC communication between instances of NGLD-M	3.2.7.3 - Internet Protocol Security (IPSEC)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0410	The NGLD-M shall utilize KMI provided IA(M) for security association for High Assurance IPSEC operations.	3.2.7.3 - Internet Protocol Security (IPSEC)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0411	The NGLD-M shall utilize KMI certificate authority materials for High Assurance IPSEC validation operations.	3.2.7.3 - Internet Protocol Security (IPSEC)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0412	The NGLD-M shall allow TLS communications to be routed to known distant end systems through established High Assurance IPSEC tunnels.	3.2.7.3 - Internet Protocol Security (IPSEC)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0413	The NGLD-M shall support High Assurance IPSEC communication with HAIPE devices.	3.2.7.3 - Internet Protocol Security (IPSEC)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	O	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0414	The NGLD-M shall perform digital signature verification for software/firmware in accordance with "Software Signature (S2) Implementation Guide, Appendix A", KM-TG-0003-003.	3.2.7.4 - Digital Signature Services	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0415	The NGLD-M shall perform digital signature verification of signed files.	3.2.7.4 - Digital Signature Services	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes
NGLD-M_SRD_0416	The NGLD-M shall be capable of decrypting and validating a KMI Cryptographic Message Syntax (CMS) package of at least 20 MB in size.	3.2.7.4 - Digital Signature Services	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0417	The NGLD-M shall perform digital signature verification of signed certificates when they are used.	3.2.7.4 - Digital Signature Services	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0418	The NGLD-M shall perform digital signature verification of CRL and ARL when they are used.	3.2.7.4 - Digital Signature Services	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0419	The NGLD-M shall provide a Data at Rest capability for encryption of data up to the Top Secret level of classification.	3.2.7.5 - Data at Rest Security	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.6 Data Storage KSA 6.2.8 Security KSA	Test	T	No	Yes
NGLD-M_SRD_0420	The NGLD-M shall provide a Data at Rest capability for decryption of data up to the Top Secret level of classification.	3.2.7.5 - Data at Rest Security	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.6 Data Storage KSA 6.2.8 Security KSA	Test	T	No	Yes
NGLD-M_SRD_0421	The NGLD-M shall provide a Data at Rest capability for integrity validation of data at rest up to the Top Secret level of classification.	3.2.7.5 - Data at Rest Security	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and commonality KPP 6.2.6 Data Storage KSA 6.2.8 Security KSA	Test	T	No	Yes
NGLD-M_SRD_0422	The NGLD-M shall be capable of validating and decrypting High Assurance software distributions intended for the NGLD-M.	3.2.7.6 - Decrypting Software Distribution	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.8 Security KSA	Test	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0423	The NGLD-M shall store persistent keys in encrypted (BLACK) form in accordance with NSA requirements.	3.2.7.7 - Cryptographic Key Storage	6.1.3 Net-Ready 6.2.6 Data Storage KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0424	The NGLD-M shall bind keys to their respective identification information in storage.	3.2.7.7 - Cryptographic Key Storage	6.1.3 Net-Ready 6.2.6 Data Storage KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0425	The NGLD-M shall provide the capability to securely store PKI private keys.	3.2.7.7 - Cryptographic Key Storage	6.1.3 Net-Ready 6.2.6 Data Storage KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0426	The NGLD-M shall, upon command, perform a rollover from one key to another.	3.2.7.8 - Rollover	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0427	The NGLD-M shall allow an authorized user to perform rollover to next key, on demand.	3.2.7.8 - Rollover	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0428	The NGLD-M shall allow for automatic rollover when key expires.	3.2.7.8 - Rollover	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0429	The NGLD-M shall be configurable to allow for automatic rollover to the next key when key expires.	3.2.7.8 - Rollover	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0430	The NGLD-M shall retain the expired key that triggered rollover and store it for adjudication.	3.2.7.8 - Rollover	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0431	The NGLD-M shall provide the capability to manage expired key that resulted from rollover.	3.2.7.8 - Rollover	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0432	The NGLD-M shall be programmable/re-programmable.	3.2.7.9 - Software/Firmware Programmability	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0433	The NGLD-M classified device configuration/programming data shall be saved in encrypted form when the NGLD-M is not operational.	3.2.7.9 - Software/Firmware Programmability	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0434	The NGLD-M classified device configuration/programming data shall be decrypted, validated, and loaded only when the NGLD-M is operational.	3.2.7.9 - Software/Firmware Programmability	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0435	The NGLD-M shall support field upgrade and programming/reprogramming of the cryptographic software/firmware.	3.2.7.10 - Cryptographic Software/Firmware Loading	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA 14.5.3 Support Equipment	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0436	The NGLD-M shall support the TAMP specification.	3.2.7.10 - Cryptographic Software/Firmware Loading	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	O	Yes	Yes
NGLD-M_SRD_0437	The NGLD-M shall support the use of Trust Anchors for the purpose of providing signature verification for software/firmware downloads in accordance with the "Trust Anchor Management Protocol (TAMP) specification for use with Type 1 Cryptographic Modules".	3.2.7.10 - Cryptographic Software/Firmware Loading	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA 14.5.3 Support Equipment	Demonstration	T	No	Yes
NGLD-M_SRD_0438	The NGLD-M shall support multiple Trust Anchors simultaneously.	3.2.7.10 - Cryptographic Software/Firmware Loading	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0439	The NGLD-M shall only accept cryptographic software/firmware packages signed by NSA.	3.2.7.10 - Cryptographic Software/Firmware Loading	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA 14.5.3 Support Equipment	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0440	The NGLD-M shall provide the capability for upgrading of software/firmware using the Cryptographic Message Syntax (CMS), per future OTNK upgrades for protecting firmware packages for High Assurance (formerly Type 1) Cryptographic Modules. (O – Since underlying infrastructure does not exist yet).	3.2.7.10 - Cryptographic Software/Firmware Loading	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA 14.5.3 Support Equipment	Demonstration	O	Yes	Yes
NGLD-M_SRD_0441	The NGLD-M shall perform authentication and integrity checks of received cryptographic software/firmware packages.	3.2.7.10 - Cryptographic Software/Firmware Loading	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA 14.5.3 Support Equipment	Demonstration	T	No	Yes
NGLD-M_SRD_0442	The NGLD-M shall report the result of a failed integrity check for received cryptographic software/firmware.	3.2.7.10 - Cryptographic Software/Firmware Loading	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA 14.5.3 Support Equipment	Demonstration	T	Yes	Yes
NGLD-M_SRD_0443	The NGLD-M shall be capable of being configured to not accept a version of a cryptographic software/firmware package that is older than the currently installed version.	3.2.7.10 - Cryptographic Software/Firmware Loading	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	T	No	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0444	The NGLD-M shall maintain the type and version of the cryptographic software/firmware package(s) that is (are) loaded.	3.2.7.10 - Cryptographic Software/Firmware Loading	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA 14.5.3 Support Equipment	Demonstration	T	No	Yes
NGLD-M_SRD_0445	The NGLD-M shall be capable of being software/firmware upgraded and reconfigured without the need to be returned to the factory, depot, or a trusted facility.	3.2.7.10 - Cryptographic Software/Firmware Loading	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.4 Configuration Management KSA 6.2.8 Security KSA 14.5.3 Support Equipment	Demonstration	T	No	Yes
NGLD-M_SRD_0446	The NGLD-M shall have a privilege for the ability to rollback loaded previous version of Software/Firmware.	3.2.7.10 - Cryptographic Software/Firmware Loading	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 14.5.3 Support Equipment	Demonstration	T	Yes	Yes
NGLD-M_SRD_0447	The NGLD-M shall have the capability to rollback the current version to a previous version of the cryptographic software/firmware.	3.2.7.10 - Cryptographic Software/Firmware Loading	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 14.5.3 Support Equipment	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0448	The NGLD-M shall have the capability to overwrite a previous version of stored cryptographic software/firmware. When a new version of the software/firmware is downloaded and after its authenticity and integrity has been verified, overwrite shall occur provided that at least one "known good" version (i.e., a version that has been previously authenticated and validated as operational) remains available.	3.2.7.10 - Cryptographic Software/Firmware Loading	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 14.5.3 Support Equipment	Demonstration	T	Yes	Yes
NGLD-M_SRD_0449	The NGLD-M crypto shall encrypt cryptographic software/firmware for storage.	3.2.7.11 - Cryptographic Software/Firmware Storage	6.1.3 Net-Ready 6.2.6 Data Storage KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0450	The NGLD-M crypto shall decrypt stored cryptographic software/firmware.	3.2.7.11 - Cryptographic Software/Firmware Storage	6.1.3 Net-Ready 6.2.6 Data Storage KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0451	The NGLD-M crypto shall perform integrity checks on Security Critical Packages and	3.2.7.12 - Level of Security and Classification	6.1.3 Net-Ready 6.2.6 Data Storage KSA 6.2.8 Security KSA	Demonstration	T	No	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
	files prior to instantiation or use.						
NGLD-M_SRD_0452	The NGLD-M crypto shall have the capability to store at least two boot images of cryptographic software/firmware in encrypted form.	3.2.7.12 - Level of Security and Classification	6.1.3 Net-Ready 6.2.6 Data Storage KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0453	The NGLD-M shall support cryptographic operations using unclassified, confidential, secret, or top secret key material.	3.2.7.12 - Level of Security and Classification	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0454	The NGLD-M shall not allow any other higher classification cryptographic service to run that is higher than the current crypto classicization level.	3.2.7.12 - Level of Security and Classification	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0455	The NGLD-M shall provide the capability to be rendered Unclassified or Unclassified Controlled Cryptographic Item (CCI).	3.2.7.13 - Unclassified Handling	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0456	The NGLD-M shall support the recovery from Unclassified CCI to a classified operational state.	3.2.7.13 - Unclassified Handling	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	No	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0457	The NGLD-M shall include any integrity mechanisms on the audit data transferred out of the NGLD-M.	3.2.7.14 - Audit	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0458	The NGLD-M shall digitally sign its own fill device audit data prior to exporting an audit dataset from the NGLD-M device.	3.2.7.14 - Audit	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0459	The NGLD-M shall maintain (and pass to the consumer) any integrity mechanisms on the audit data transferred out of the NGLD-M.	3.2.7.14 - Audit	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0460	The NGLD-M shall support audit capabilities in accordance with the NSA NGLD-M tailored IASRD and RMF.	3.2.7.14 - Audit	6.2.4 Configuration Management KSA 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0461	The NGLD-M shall report audit events when requested.	3.2.7.14 - Audit	6.2.4 Configuration Management KSA 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0462	The NGLD-M shall provide a minimum of 8 MB internal storage for audit events.	3.2.7.14 - Audit	6.2.4 Configuration Management KSA 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	No	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0463	The NGLD-M crypto shall overwrite the oldest audit events if the audit internal storage usage reaches maximum capacity.	3.2.7.14 - Audit	6.2.4 Configuration Management KSA 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0464	The NGLD-M crypto shall report audit internal storage overwrites.	3.2.7.14 - Audit	6.2.4 Configuration Management KSA 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0465	The NGLD-M shall store system audit data in non-volatile memory that is unaffected by changes in primary power.	3.2.7.14 - Audit	6.1.3 Net-Ready 6.2.6 Data Storage KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0466	The NGLD-M shall provide warning when 80% audit log capacity is reached.	3.2.7.14 - Audit	6.2.4 Configuration Management KSA 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0467	The NGLD-M crypto shall support a mode of operation in which a user is logged into the device and the CIK is inserted , and the user has locked the device and is not directly interacting with the system.	3.2.8 - Discrete Operation	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0468	The NGLD-M shall require the user to perform a secure lock/unlock action to place the device in Discrete mode and to exit Discrete mode.	3.2.8 - Discrete Operation	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0469	The NGLD-M Discrete mode will not be available until after the device is initially configured.	3.2.8 - Discrete Operation	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0470	The NGLD-M shall not allow a user to perform any actions while the device is locked and in Discrete mode.	3.2.8 - Discrete Operation	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0471	The NGLD-M shall allow authorized and limited automated download actions while the device is locked and in Discrete mode.	3.2.8 - Discrete Operation	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0472	The NGLD-M shall allow authorized and limited PDE and LMA services while the device is locked and in Discrete mode.	3.2.8 - Discrete Operation	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0473	The NGLD-M shall display limited informational status of the activities that are taking place in Discrete mode.	3.2.8 - Discrete Operation	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	O	Yes	Yes
NGLD-M_SRD_0474	The NGLD-M shall provide BIT and health status in accordance with the NSA NGLD-M tailored IASRD.	3.2.9 - Built-In Test and Health Status	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0475	The NGLD-M BIT shall validate correctness of functionality of hardware/firmware/software components.	3.2.9 - Built-In Test and Health Status	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Test	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0476	The NGLD-M BIT shall validate processors.	3.2.9 - Built-In Test and Health Status	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0477	The NGLD-M BIT shall validate volatile and non-volatile memory.	3.2.9 - Built-In Test and Health Status	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0478	The NGLD-M BIT shall validate internal control and data buses.	3.2.9 - Built-In Test and Health Status	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0479	The NGLD-M BIT shall validate interfaces.	3.2.9 - Built-In Test and Health Status	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0480	The NGLD-M BIT shall validate the signatures of firmware and software.	3.2.9 - Built-In Test and Health Status	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0481	The NGLD-M BIT shall validate the functionality of cryptographic algorithms.	3.2.9 - Built-In Test and Health Status	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0482	The NGLD-M BIT shall isolate failed component(s).	3.2.9 - Built-In Test and Health Status	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0483	The NGLD-M BIT shall persist detected failures in a non-editable log.	3.2.9 - Built-In Test and Health Status	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Test	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0484	The NGLD-M shall perform voltage monitoring of all power supplies.	3.2.9 - Built-In Test and Health Status	6.1.3 Net- Ready 6.2.3 SWAP KPP 6.2.7 Tamper Detection KSA	Test	T	Yes	Yes
NGLD-M_SRD_0485	The NGLD-M shall not activate the inactive power off timer during data transmission over an external interfaces.	3.2.9 - Built-In Test and Health Status	6.1.3 Net- Ready	Demonstration	T	No	Yes
NGLD-M_SRD_0486	The NGLD-M shall incorporate integrity mechanisms on health and monitoring data transferred out of the NGLD-M.	3.2.9.1 - Health and Monitoring Data	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Demonstration	O	Yes	No
NGLD-M_SRD_0487	The NGLD-M shall be capable of sending (NGLD-M Fill Device) health and monitoring data to the iApp Last Mile API (LMA).	3.2.9.1 - Health and Monitoring Data	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Demonstration	O	Yes	Yes
NGLD-M_SRD_0488	The NGLD-M shall implement self-test(s) that provide assurance that the security service(s) offered and the components (e.g. algorithm, processor, randomizer, memory, etc.) implementing these services are operating properly.	3.2.9.1 - Health and Monitoring Data	6.1.3 Net-Ready 6.2.6 Data Storage KSA 6.2.8 Security KSA	Test	T	No	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0489	The NGLD-M initiation of health status tests, including security critical functions, shall take place whenever a system is powered on, periodically during operation, when system installation or reconfiguration is performed, and after occurrence of system malfunction.	3.2.9.1 - Health and Monitoring Data	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0490	The NGLD-M shall validate the integrity of hardware, software, and sensitive data using approved cryptographic hashing algorithms.	3.2.9.1 - Health and Monitoring Data	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0491	The NGLD-M shall provide protection mechanisms to ensure the integrity of any remotely controlled availability health testing capability.	3.2.9.1 - Health and Monitoring Data	6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0492	The NGLD-M shall support health monitoring capability via network interface.	3.2.9.1 - Health and Monitoring Data	6.1.3 Net-Ready 6.2.8 Security KSA 6.2.9 (U) Operational Availability (Ao) KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0493	The NGLD-M shall provide the capability to persist health monitoring status information.	3.2.9.1 - Health and Monitoring Data	6.1.3 Net-Ready 6.2.6 Data Storage KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0494	The NGLD-M shall persist details collected in relation to	3.2.10 - Alarm	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Inspection	T	No	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
	all generated alarms in a non-editable log.						
NGLD-M_SRD_0495	The NGLD-M shall present alarm condition to the user on NGLD-M display.	3.2.10 - Alarm	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0496	The NGLD-M shall generate an alarm if the operational battery pack is removed.	3.2.10 - Alarm	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0497	The NGLD-M shall generate an alarm if the operational battery charge is less than 5%.	3.2.10 - Alarm	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0498	The NGLD-M crypto shall system alarms in accordance with the NSA NGLD-M tailored IASRD.	3.2.10 - Alarm	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0499	The NGLD-M shall provide the ability to obtain network time from the ACES/iApp management station services when connected via an IP-based external interface.	3.2.11 - Configuration Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	O	Yes	Yes
NGLD-M_SRD_0500	The NGLD-M shall allow network/COMSEC manager to configure or reconfigure network devices in five minutes or less. **Note: Awaiting a clarification from TCM N&S on this requirements since this is not testable as it is written**	3.2.11 - Configuration Management	6.2.4 Configuration Management KSA	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0501	The NGLD-M zeroization capabilities shall be available in the absence of external power.	3.2.12 - Zeroization	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Test	T	No	Yes
NGLD-M_SRD_0502	When the Zeroize button is pressed, the NGLD-M shall transition into the zeroization state. **Note: The Army is not providing a design here. Zeroize could be done with the touch screen and/or buton could be a fallback**	3.2.12 - Zeroization	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0503	The NGLD-M shall support selective zeroization.	3.2.12 - Zeroization	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0504	The NGLD-M shall support recoverable zeroization.	3.2.12 - Zeroization	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0505	The NGLD-M shall support destructive zeroization.	3.2.12 - Zeroization	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0506	The NGLD-M shall support passive zeroization.	3.2.12 - Zeroization	6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0507	The NGLD-M shall use Human User or Device User credentials to gain access to the NIPRNET domain.	3.2.13 - Multi-Domain Support	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0508	The NGLD-M shall limit access to NIPRNET sites allowing user browsing to only OTNK-Compliant Storefront and ACES/iApp Last Mile API (LMA) services defined in the NGLD-M's connection definitions.	3.2.13 - Multi-Domain Support	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0509	The NGLD-M shall use Human User or Device User credentials to gain access to the SIPRNET domain.	3.2.13 - Multi-Domain Support	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0510	The NGLD-M shall limit access to SIPRNET sites allowing user browsing to only OTNK-Compliant Storefront and ACES/iApp Last Mile API (LMA) services defined in the NGLD-M's connection definitions.	3.2.13 - Multi-Domain Support	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0511	The NGLD-M shall use Human User or Device User credentials to gain access to the Tactical Secret domain.	3.2.13 - Multi-Domain Support	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0512	The NGLD-M shall use Human User or Device User credentials to gain access to the JWICS domain.	3.2.13 - Multi-Domain Support	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	O	Yes	Yes
NGLD-M_SRD_0513	The NGLD-M shall limit access to JWICS sites allowing user browsing to only OTNK-Compliant Storefront and ACES/iApp Last Mile API (LMA) services defined in the NGLD-M's connection definitions.	3.2.13 - Multi-Domain Support	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	O	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0514	The NGLD-M shall only support one configuration of the device that supports all networks (NIPRNET, SIPRNET, Tactical Secret, JWICS).	3.2.13 - Multi-Domain Support	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0515	The NGLD-M shall support the ability to import, persist and process trusted ECU profile data received from another NGLD-M to instantiate and provide support for ECU Profiles not currently known to the NGLD-M.	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA 6.2.6 Data Storage KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0516	The NGLD-M shall support the ability to import, persist and process trusted ECU profile data from an external-supported ACES/iApp to instantiate and provide support for ECU Profiles not currently known to the NGLD-M.	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA 6.2.6 Data Storage KSA	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0517	The NGLD-M shall ensure ECU Profile Data import is restricted to users possessing the privilege to establish a new ECU Profile on the NGLD-M.	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	No
NGLD-M_SRD_0518	The NGLD-M shall verify the integrity of the imported ECU profile prior to accepting to ensure it is from a trusted source.	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA 6.2.6 Data Storage KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0519	The NGLD-M shall verify the integrity of the imported ECU profile prior to accepting to ensure it has not been modified following its source generation.	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA 6.2.6 Data Storage KSA	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0520	The NGLD-M shall be capable of detecting duplicate ECU Profiles during import (if an equipment profile is provided via import that already exists on the NGLD-M).	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA 6.2.6 Data Storage KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0521	The NGLD-M shall allow a user with the privilege to manage ECU profiles to lock an existing ECU profile to prevent it from being updated with future ECU profile imports.	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA 6.2.6 Data Storage KSA	Demonstration	T	Yes	No

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0522	The NGLD-M shall allow a user with the privilege to manage ECU profiles to un-lock an existing ECU profile allowing it to be updated with future ECU profile imports.	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA 6.2.6 Data Storage KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0523	The NGLD-M shall inform the user of duplicate ECU profiles detected during an import and prompt the user to continue (overwrite) the existing ECU profile or cancel the import process.	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA 6.2.6 Data Storage KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0524	The NGLD-M shall support a workflow allowing users with the privilege to generate a new ECU profile to create a new ECU profile on the NGLD-M. NOTE: The workflow shall guide the operator in creating	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	O	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
	key slots and assigning profile elements. Reference SKL IDD						
NGLD-M_SRD_0525	The NGLD-M dynamic profiles shall support the legacy ECU profile parameters provisioned in the SKL (reference SKL IDD) including, at a minimum, support for the following ECU specific information: Equipment type, Equipment Location, Transmit Profile, Receive Profile if applicable, Electronic Protection data, Communication Protocol Information, Communication Parameter data.	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA 6.2.6 Data Storage KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0526	The NGLD-M shall allow users possessing the appropriate privileges the capability to view existing ECU profiles.	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	No

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0527	The NGLD-M shall allow users possessing the appropriate privileges the capability to manage ECU Profile data, allowing the user to search/filter for ECU Profile Data in the process.	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	No
NGLD-M_SRD_0528	The NGLD-M shall allow users possessing the appropriate privileges the capability to export selected ECU profiles.	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA 6.2.6 Data Storage KSA	Demonstration	O	Yes	No
NGLD-M_SRD_0529	The NGLD-M shall provide integrity controls while exporting equipment profiles so the recipient of this profile data can verify the source and that the contents are unchanged.	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA 6.2.6 Data Storage KSA	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0530	The NGLD-M shall allow users possessing the appropriate privileges the capability to remove ECU profile data.	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.6 Data Storage KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0531	The NGLD-M shall provide the ability to import ECU Profile data from media / File I/O received through an approved interface (i.e. USB).	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA 6.2.6 Data Storage KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0532	The NGLD-M shall provide the ability to retrieve ECU Profile data from the ACES/iApp Last Mile API (LMA) Interface.	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA 6.2.6 Data Storage KSA	Demonstration	O	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0533	The NGLD-M shall provide the ability to send ECU Profile data to the ACES/iApp Last Mile API (LMA) Interface.	3.2.14 - ECU-Profile Management	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA 6.2.6 Data Storage KSA	Demonstration	O	Yes	No
NGLD-M_SRD_0534	The NGLD-M shall support the Delivery Standard 101 (DS-101) interfaces per EKMS 308F.	3.2.15 - Legacy Interfaces/Backward Compatibility	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0535	The NGLD-M shall support the Delivery Standard 102 (DS-102) interfaces per EKMS 308F.	3.2.15 - Legacy Interfaces/Backward Compatibility	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0536	The NGLD-M fill logic shall support the DS-102 Common Fill Device (CFD) interfaces per EKMS 603B Section 3.2.2.1.3	3.2.15 - Legacy Interfaces/Backward Compatibility	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0537	The NGLD-M shall support the RS-232 interfaces per EKMS 308F.	3.2.15 - Legacy Interfaces/Backward Compatibility	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0538	The NGLD-M shall support SINCGARS Mode 1, (ICOM and Non-ICOM modes – reference EKMS 603C) loading	3.2.15 - Legacy Interfaces/Backward Compatibility	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0539	The NGLD-M shall support SINCGARS Mode 2, (Army and Air Forces modes – reference EKMS 603C) loading.	3.2.15 - Legacy Interfaces/Backward Compatibility	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0540	The NGLD-M shall support Over-the-Air-Distribution (OTAD) functions	3.2.15 - Legacy Interfaces/Backward Compatibility	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0541	The NGLD-M shall support a Key Load Status (KLS) Log.	3.2.15 - Legacy Interfaces/Backward Compatibility	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0542	The NGLD-M shall provide an ECU Management capability with the following commands: Query Status, Get Date and Time, Set Date and Time, Set Battery Date and Time, Key Status/Zeroize Select, Level 3 Zeroization.	3.2.15 - Legacy Interfaces/Backward Compatibility	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0543	The NGLD-M shall provide a capability to send the following low level ECU Commands: Set Station Address, Set Station ID, Zeroize All, Zeroize EEPROM, Zeroize All RAM, and Zeroize RAM to the following ECUs: ADDI, JTIDS, KGV-23, RT-1794, MIDS JTRS, Mode 5 IFF, LINK16CM, IFDL and TTN equipment.	3.2.15 - Legacy Interfaces/Backward Compatibility	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0544	The NGLD-M shall provide the capability to perform a bus query to obtain a bus address for a piece of equipment.	3.2.15 - Legacy Interfaces/Backward Compatibility	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0545	The NGLD-M shall support the interface function Receive (Key) to receive red and black electronic key from KMI Tier 2/3 devices and via Secure Terminal Equipment (STE)/vIPer.	3.2.15 - Legacy Interfaces/Backward Compatibility	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0546	The NGLD-M shall support the interface function Receive (Key) to receive a red key from a KOI-18 KMI Tier 3 device, (paper tape key loader) and the KYK-13 Electronic Key Loader.	3.2.15 - Legacy Interfaces/Backward Compatibility	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0547	The NGLD-M shall support battery charging accessory and/or cable to recharge the battery.	3.2.16 - Accessory	6.2.3 SWAP (size, weight, and power) KPP 6.2.9 Operational Availability (Ao) KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0548	The NGLD-M shall support the use of a commercially available Ethernet cable that meets EMI and TEMPEST requirements.	3.2.16 - Accessory	6.2.3 SWAP (size, weight, and power) KPP 6.2.9 Operational Availability (Ao) KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0549	The NGLD-M battery charging accessory and/or cable shall be compatible with the solar power charging interface.	3.2.16 - Accessory	6.2.3 SWAP (size, weight, and power) KPP	Demonstration	T	No	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
			6.2.9 Operational Availability (Ao) KSA				
NGLD-M_SRD_0550	The NGLD-M shall support the use of a commercially available USB cable.	3.2.16 - Accessory	6.2.3 SWAP (size, weight, and power) KPP 6.2.9 Operational Availability (Ao) KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0551	The NGLD-M shall support the use of a commercially available six pin audio fill cable.	3.2.16 - Accessory	6.2.3 SWAP (size, weight, and power) KPP 6.2.9 Operational Availability (Ao) KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0552	The NGLD-M shall perform power down activities upon detection of the power down stimulus.	3.2.17 - Power-Down	6.1.3 Net- Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0553	The NGLD-M shall have a defined default value the internal device inactivity power off timer.	3.2.17 - Power-Down	6.1.3 Net- Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0554	The NGLD-M shall have an inactivity power off timer that is user configurable.	3.2.17 - Power-Down	6.1.3 Net- Ready	Demonstration	T	Yes	Yes
NGLD-M_SRD_0555	The NGLD-M shall provide access to Help Desk Contact Information.	3.2.18 - Seeking Help	6.1.3 Net- Ready 6.2.9 (U) Operational Availability (Ao) KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0556	The NGLD-M shall provide access to the NGLD-M Quick Reference Guide (QRG).	3.2.18 - Seeking Help	6.1.3 Net- Ready 6.2.9 (U) Operational Availability (Ao) KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0557	The NGLD-M UAS shall provide a user interface with icon based navigation that provides the user access to functions.	3.2.19 - General User Interface	6.1.3 Net-Ready	Demonstration	T	Yes	No
NGLD-M_SRD_0558	The NGLD-M UAS shall provide a Home Screen that allows access for functions available to the user.	3.2.19 - General User Interface	6.1.3 Net-Ready	Demonstration	T	Yes	No
NGLD-M_SRD_0559	The NGLD-M UAS shall provide the user a method to activate all of the supported capabilities.	3.2.19 - General User Interface	6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0560	The NGLD-M UAS shall always display a classification banner showing the highest level of classification based on the operating environment.	3.2.19 - General User Interface	6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0561	The NGLD-M UAS shall provide the capability to set the classification banners.	3.2.19 - General User Interface	6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0562	The NGLD-M UAS shall audit the setting of the classification banners.	3.2.19 - General User Interface	6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0563	The NGLD-M UAS shall always display current date, time, and battery level.	3.2.19 - General User Interface		Demonstration	T	Yes	No
NGLD-M_SRD_0564	The NGLD-M UAS shall provide a navigation mechanism to allow the user to traverse through the UAS.	3.2.19 - General User Interface		Demonstration	T	Yes	No

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0565	The NGLD-M UAS shall provide a virtual keyboard to allow user inputs.	3.2.19 - General User Interface		Demonstration	T	Yes	No
NGLD-M_SRD_0566	The NGLD-M UAS shall expose features based on user assigned privilege.	3.2.19 - General User Interface	6.2.8 Security KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0567	The NGLD-M UAS shall provide context sensitive help system to the user.	3.2.19 - General User Interface	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP	Demonstration	T	Yes	No
NGLD-M_SRD_0568	The NGLD-M UAS shall allow the user to perform their work based on Tasks.	3.2.19 - General User Interface		Demonstration	T	Yes	No
NGLD-M_SRD_0569	The NGLD-M shall support data search and filter capabilities.	3.2.19 - General User Interface		Demonstration	T	Yes	No
NGLD-M_SRD_0570	The NGLD-M shall provide user ability to view, scroll, and select data.	3.2.19 - General User Interface		Demonstration	T	Yes	No
NGLD-M_SRD_0571	The NGLD-M shall support DS-101, DS-102, MIL-STD-188-114, RS-232, USB, Ethernet, and wireless protocols.	3.3.2 - Physical External Interfaces	6.1.3 Net-Ready 6.2.3 SWAP (Size, weight, and power) KPP 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	Yes	Yes
NGLD-M_SRD_0572	The NGLD-M shall design for best display size based on the Size, Weight, and Power (SWAP) requirements.	3.3.2.1. - Display	6.2.3 SWAP (Size, weight, and power) KPP 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	No	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0573	The NGLD-M shall include an impact and scratch resistant display.	3.3.2.1. - Display	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes
NGLD-M_SRD_0574	The NGLD-M shall include a touch panel compatible with finger touch and stylus user interface.	3.3.2.1. - Display	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	Yes	Yes
NGLD-M_SRD_0575	The NGLD-M display shall provide multi-touch support.	3.3.2.1. - Display	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	Yes	Yes
NGLD-M_SRD_0576	The NGLD-M shall provide usable touch support for users equipped up to Mission Oriented Protective Posture (MOPP) Level 4.	3.3.2.1. - Display	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	Yes	Yes
NGLD-M_SRD_0577	The NGLD-M shall provide a brightness control mechanism that is selectable between automatic brightness control and manual brightness control.	3.3.2.1. - Display	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	No	Yes
NGLD-M_SRD_0578	The NGLD-M shall be configurable to set a default display lighting mode of operation.	3.3.2.1. - Display	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	Yes	Yes
NGLD-M_SRD_0579	The NGLD-M shall be readable in low light.	3.3.2.1. - Display	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0580	The NGLD-M shall be readable in Sunlight.	3.3.2.1. - Display	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	Yes	Yes
NGLD-M_SRD_0581	The NGLD-M shall be readable in Night Vision.	3.3.2.1. - Display	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	Yes	Yes
NGLD-M_SRD_0582	The NGLD-M shall support grayscale (monochrome) mode of operation.	3.3.2.1. - Display	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	Yes	Yes
NGLD-M_SRD_0583	The NGLD-M display shall support maximum resolution possible.	3.3.2.1. - Display	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes
NGLD-M_SRD_0584	The NGLD-M display contrast ratio shall be sufficiently high in all lighting modes.	3.3.2.1. - Display	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes
NGLD-M_SRD_0585	The NGLD-M shall support both portrait and landscape configuration.	3.3.2.1. - Display	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	No	Yes
NGLD-M_SRD_0586	The NGLD-M shall provide the user the ability to select either portrait or landscape configuration as a default.	3.3.2.1. - Display	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0587	The NGLD-M shall automatically change to either a portrait or landscape configuration based on a user default selection.	3.3.2.1. - Display	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	Yes	Yes
NGLD-M_SRD_0588	The NGLD-M display shall support minimum of 262K colors.	3.3.2.1. - Display	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes
NGLD-M_SRD_0589	The NGLD-M shall support HDMI port.	3.3.2.1. - Display	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	O	No	Yes
NGLD-M_SRD_0590	The NGLD-M shall support a keypad interface for navigation control capabilities of the display.	3.3.2.2. - Keypad	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	Yes	Yes
NGLD-M_SRD_0591	The NGLD-M shall support power on/off operation of the NGLD-M.	3.3.2.2. - Keypad	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	Yes	Yes
NGLD-M_SRD_0592	The NGLD-M shall support brightness control capabilities.	3.3.2.2. - Keypad	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	Yes	Yes
NGLD-M_SRD_0593	The NGLD-M shall provide the capability to show the current display mode.	3.3.2.2. - Keypad	6.1.3 Net-Ready 6.2.10 Environmental Durability Additional Attribute	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0594	The NGLD-M shall provide a zeroize function via button(s) press by the user. **Note: The Army is not providing a design here. Zeroize could be done with the touch screen and/or buton could be a fallback**	3.3.2.2. - Keypad	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0595	The NGLD-M zeroize function shall be designed to prevent accidental activation of zeroization functions.	3.3.2.2. - Keypad	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0596	The NGLD-M shall contain a fill port interface.	3.3.2.3. - Fill Port	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	No	Yes
NGLD-M_SRD_0597	The NGLD-M fill port shall support fill port interface communication.	3.3.2.3. - Fill Port	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0598	The NGLD-M fill port shall support RS-232 at a minimum of 9600 bps.	3.3.2.3. - Fill Port	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0599	The NGLD-M fill port shall support DS-101 at a minimum of 64 kbps.	3.3.2.3. - Fill Port	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0600	The NGLD-M fill port shall support DS-102 at a minimum of 64 kbps.	3.3.2.3. - Fill Port	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0601	The NGLD-M shall support updating of software/firmware via fill port.	3.3.2.3. - Fill Port	6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
			6.2.4 Configuration Management KSA				
NGLD-M_SRD_0602	The NGLD-M shall support a fill port, supporting 6 pin audio connector.	3.3.2.3. - Fill Port	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	No	Yes
NGLD-M_SRD_0603	The NGLD-M shall support Cryptographic Ignition Key (CIK).	3.3.2.4. - Cryptographic Ignition Key (CIK)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	No	Yes
NGLD-M_SRD_0604	The NGLD-M shall provide a CIK interface.	3.3.2.4. - Cryptographic Ignition Key (CIK)	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0605	The NGLD-M shall be designed to operate with CIK.	3.3.2.4. - Cryptographic Ignition Key (CIK)	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0606	The NGLD-M fill port interface shall only be active when CIK login is in use.	3.3.2.4. - Cryptographic Ignition Key (CIK)	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0607	The NGLD-M shall contain a Universal Service Bus (USB) interface.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	No	Yes
NGLD-M_SRD_0608	The NGLD-M shall contain minimum High Speed Mode USB 2.0 interface.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	No	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0609	The NGLD-M shall support USB memory peripherals.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	No	Yes
NGLD-M_SRD_0610	The NGLD-M shall support operating as a USB mass storage device.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0611	The NGLD-M shall support operating virtual ethernet via the USB interface.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0612	The NGLD-M shall allow software/firmware updates via USB interface.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0613	The NGLD-M shall support charging of batteries via USB interface.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.3 SWAP (size, weight, and power)	Test	T	No	No
NGLD-M_SRD_0614	The NGLD-M shall receive PKI certificates via USB interface.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0615	The NGLD-M shall transmit PKI certificates via USB interface.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0616	The NGLD-M shall receive mission plans via USB interface.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0617	The NGLD-M shall receive profiles via USB interface.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	No
NGLD-M_SRD_0618	The NGLD-M shall allow transmission of mission plans via USB interface.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0619	The NGLD-M shall allow transmission of profile via USB interface.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	No
NGLD-M_SRD_0620	The NGLD-M shall allow the receiving of KMI IA(I) certificate via USB interface.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	No
NGLD-M_SRD_0621	The NGLD-M shall allow the transmission of KMI IA(I) via USB interface.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0622	The NGLD-M shall allow the receiving of KMI IA(M) certificate via USB interface.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0623	The NGLD-M shall allow the transmission of KMI IA(M) certificate via USB interface.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0624	The NGLD-M shall allow the receiving of KMI KE(I) certificate via USB interface.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0625	The NGLD-M shall allow the transmission of KMI KE(I) certificate via USB interface.	3.3.2.5. - Universal Serial Bus (USB)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0626	The NGLD-M shall provide a wired Ethernet (RJ45) interface.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	No	Yes
NGLD-M_SRD_0627	The NGLD-M shall support Gigabit Ethernet interface (1,000 Mbps).	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	No	Yes
NGLD-M_SRD_0628	The NGLD-M shall receive PKI certificates via Ethernet (RJ45) interface.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0629	The NGLD-M shall transmit PKI certificates via Ethernet (RJ45) interface.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0630	The NGLD-M Ethernet (RJ45) shall support the loading and configuration of ECUs.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0631	The NGLD-M Ethernet (RJ45) port shall support software download and updates.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.4 Configuration Management KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0632	The NGLD-M Ethernet (RJ45) port shall support firmware download and updates.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.4 Configuration Management KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0633	The NGLD-M Ethernet (RJ45) port shall support data storage and bi-directional file transfers.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.6 Data Storage KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0634	The NGLD-M Ethernet (RJ45) port shall support Simple Network Management Protocol (SNMP) per IETF standard 62 and IETF standard 78.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0635	The NGLD-M Ethernet (RJ45) port shall support SNMP protocol v1, v2 and v3.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0636	The NGLD-M Ethernet (RJ45) port shall support communication with KMI storefront and local OTNK compliant intermediaries utilizing OTNK.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0637	The NGLD-M shall support accessing Secret Internet Protocol Router (SIPRNET).	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0638	The NGLD-M shall support accessing Tactical networks including and up to the Secret classification level.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0639	The NGLD-M shall support accessing Non-Classified Protocol Router Network (NIPRNET).	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0640	The NGLD-M shall support accessing networks classified Top Secret.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	O	Yes	Yes
NGLD-M_SRD_0641	The NGLD-M Ethernet (RJ45) port shall support interface with and management by Net Ops tool sets. **Note: This is threshold since CPD requires it but the Army does not have a clarity on Net Ops Tool set**	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	O	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0642	The NGLD-M shall support the Transport Layer Security (TLS) protocol versions identified in the OTNK specification.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0643	The NGLD-M shall support backward compatibility to previous version of TLS.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0644	The NGLD-M shall support the File Transfer Protocol Secure (FTPS) protocol.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0645	The NGLD-M Ethernet (RJ45) port shall allow the receiving of mission plans.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0646	The NGLD-M Ethernet (RJ45) port shall allow the receiving of profiles.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0647	The NGLD-M Ethernet (RJ45) port shall allow the transmission of mission plans.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	No
NGLD-M_SRD_0648	The NGLD-M Ethernet (RJ45) port shall allow the transmission of profiles.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0649	The NGLD-M Ethernet (RJ45) port shall allow the receiving of Certification Revocation List (CRL) data.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0650	The NGLD-M Ethernet (RJ45) port shall allow the transmission of CRL data.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0651	The NGLD-M Ethernet (RJ45) port shall allow the receiving of Authority Revocation List (ARL) data.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0652	The NGLD-M Ethernet (RJ45) port shall allow the transmission of Authority Revocation List (ARL) data.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0653	The NGLD-M Ethernet port shall allow the receiving of KMI IA(I) certificate data.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0654	The NGLD-M Ethernet port shall allow the transmission of KMI IA(I) data.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0655	The NGLD-M Ethernet port shall allow the receiving of KMI IA(M) certificate data.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0656	The NGLD-M Ethernet port shall allow the transmission of KMI IA(M) certificate data.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0657	The NGLD-M Ethernet port shall allow the receiving of KMI KE(I) certificate data.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0658	The NGLD-M Ethernet port shall allow the transmission of KMI KE(I) certificate data.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0659	The NGLD-M shall support receiving Cryptographic Message Syntax (CMS) wrapped keys via Ethernet (RJ45) network.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
			6.2.5 Data Transfer KSA				
NGLD-M_SRD_0660	The NGLD-M shall support transmit CMS wrapped keys with Ethernet (RJ45) network.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0661	The NGLD-M shall support Trivial File Transfer Protocol (TFTP) protocol.	3.3.2.6. - Ethernet (RJ45)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0662	The NGLD-M shall provide a wireless network interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	No	Yes
NGLD-M_SRD_0663	The NGLD-M shall have its wireless network interface disabled by default.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0664	The NGLD-M shall be configurable to enable and disable wireless network interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0665	The NGLD-M shall support cryptographically secured wireless protocols.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0666	The NGLD-M shall be designed to receive mission plans via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0667	The NGLD-M shall be designed to transmit mission plans via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0668	The NGLD-M shall be designed to receive profiles via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0669	The NGLD-M shall be designed to transmit profiles via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0670	The NGLD-M shall be designed to receive PKI certificates via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0671	The NGLD-M shall be designed to transmit PKI certificates via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0672	The NGLD-M shall allow the receiving of Certification Revocation List (CRL) data via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0673	The NGLD-M shall allow the transmission of CRL data via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0674	The NGLD-M shall allow the receiving of Authority Revocation List (ARL) data via wireless interface	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0675	The NGLD-M shall allow the transmission of Authority Revocation List (ARL) data via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0676	The NGLD-M shall support receiving Cryptographic Message Syntax (CMS) wrapped keys via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0677	The NGLD-M shall support transmit CMS wrapped keys via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0678	The NGLD-M shall support receiving Key Encryption Key (KEK) wrapped keys via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0679	The NGLD-M shall support transmit KEK wrapped keys via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0680	The NGLD-M shall support software download and updates via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.4 Configuration Management KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0681	The NGLD-M shall support firmware download and updates via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.4 Configuration Management KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0682	The NGLD-M shall support the Transport Layer Security (TLS) protocol 1.2 or the latest version via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0683	The NGLD-M shall support backward compatibility to previous version of TLS via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0684	The NGLD-M shall support the File Transfer Protocol Secure (FTPS) protocol via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0685	The NGLD-M shall support Trivial File Transfer Protocol (TFTP) protocol via wireless interface.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0686	The NGLD-M wireless interface shall support SNMP protocol v1, v2 and v3.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0687	The NGLD-M wireless interface shall support communication with KMI storefront and local OTNK compliant intermediaries.	3.3.2.7. - Wireless	6.1.3 Net-Ready 6.2.1 (U) Mission Data Services KPP 6.2.2 Interoperability,	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
			Standardization and Commonality KPP				
NGLD-M_SRD_0688	The NGLD-M shall include rechargeable, no memory, low maintenance, non-spill, and thermal safe battery pack.	3.3.2.8. - Operational Battery	6.2.3 SWAP (size, weight, and power) KPP	Inspection	T	No	Yes
NGLD-M_SRD_0689	The NGLD-M battery pack shall be rechargeable in no more than 48 hours.	3.3.2.8. - Operational Battery	6.2.3 SWAP (size, weight, and power) KPP	Demonstration	T	No	Yes
NGLD-M_SRD_0690	The NGLD-M shall have the rechargeable capabilities via worldwide AC power.	3.3.2.8. - Operational Battery	6.2.3 SWAP (size, weight, and power) KPP	Demonstration	T	No	Yes
NGLD-M_SRD_0906	The NGLD-M battery health shall include battery charge level, and remaining battery life compare to new battery.	3.3.2.8. - Operational Battery	6.2.3 SWAP (size, weight, and power) KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0691	The NGLD-M Ethernet port shall support an interface to the KMI (PRSN) Device PDE Storefront.	3.3.3.1 - KMI Device PDE Storefront (PUI:KMIDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0692	The NGLD-M shall support an interface to the KMI (PRSN) Device PDE Storefront using NGLD-M (UAS) Medium Assurance Credentials.	3.3.3.1 - KMI Device PDE Storefront (PUI:KMIDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0693	The NGLD-M shall support an interface to the KMI (PRSN) Device PDE Storefront using NGLD-M High Assurance Credentials.	3.3.3.1 - KMI Device PDE Storefront (PUI:KMIDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0694	The NGLD-M interface to the KMI (PRSN) Device PDE Storefront shall be Product Delivery Enclave Enabled (PDE-E) IAW requirements defined in KMI 3300.	3.3.3.1 - KMI Device PDE Storefront (PUI:KMIDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0695	The NGLD-M shall adhere to the latest OTNK Specification (currently Over-the-Network-Keying (OTNK) Specification, version 3.1.2) for communications with the KMI (PRSN) Device PDE Storefront, specifically regarding authentication, PAL / Product standards and CMS processing.	3.3.3.1 - KMI Device PDE Storefront (PUI:KMIDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0696	The NGLD-M shall be able to perform signature validation on CMS Packages that were retrieved from an OTNK-Compliant Device PDE Storefront using the High Assurance Credentials of the NGLD-M.	3.3.3.1 - KMI Device PDE Storefront (PUI:KMIDPDE)	6.1.3 Net-Ready 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0697	The NGLD-M Ethernet port shall support an interface to the KMI MGC Device PDE Storefront.	3.3.3.2 - KMI MGC Device PDE Storefront (PUI:MGCDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0698	The NGLD-M shall support an interface to the KMI MGC Device PDE Storefront using NGLD-M (UAS) Medium Assurance Credentials.	3.3.3.2 - KMI MGC Device PDE Storefront (PUI:MGCDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0699	The NGLD-M shall support an interface to the KMI MGC Device PDE Storefront using NGLD-M High Assurance Credentials.	3.3.3.2 - KMI MGC Device PDE Storefront (PUI:MGCDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0700	The NGLD-M interface to the KMI MGC Device PDE Storefront shall be Product Delivery Enclave Enabled (PDE-	3.3.3.2 - KMI MGC Device PDE Storefront (PUI:MGCDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
	E) IAW requirements defined in KMI 3300.		6.2.5 Data Transfer KSA				
NGLD-M_SRD_0701	The NGLD-M shall adhere to the latest OTNK Specification (currently Over-the-Network-Keying (OTNK) Specification, version 3.1.2) for communications with the KMI MGC Device PDE Storefront, specifically regarding authentication, PAL / Product standards and CMS processing.	3.3.3.2 - KMI MGC Device PDE Storefront (PUI:MGCDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0702	The NGLD-M Ethernet port shall support an interface to the iApp OTNK Device PDE Storefront.	3.3.3.3 - ACES/iApp OTNK Device PDE Storefront (PUI:IDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0703	The NGLD-M shall support an interface to the iApp OTNK Device PDE Storefront using NGLD-M (UAS) Medium Assurance Credentials.	3.3.3.3 - ACES/iApp OTNK Device PDE Storefront (PUI:IDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0704	The NGLD-M shall support an interface to the iApp OTNK Device PDE Storefront using NGLD-M High Assurance Credentials.	3.3.3.3 - ACES/iApp OTNK Device PDE Storefront (PUI:IDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0705	The NGLD-M interface to the iApp OTNK Device PDE Storefront shall be Product Delivery Enclave Enabled (PDE-E) IAW requirements defined in KMI 3300.	3.3.3.3 - ACES/iApp OTNK Device PDE Storefront (PUI:IDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0706	The NGLD-M shall adhere to the latest OTNK Specification (currently Over-the-Network-Keying (OTNK) Specification, version 3.1.2) for communications with the iApp OTNK Device PDE Storefront, specifically regarding authentication, PAL / Product standards and CMS processing.	3.3.3.3 - ACES/iApp OTNK Device PDE Storefront (PUI:IDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0707	The NGLD-M shall be capable of interfacing to the iApp Last Mile API (LMA) to send pertinent data.	3.3.3.4 - ACES/iApp Last Mile API (PUI:ILMA)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0708	The NGLD-M UAS shall utilize mutual authentication when sending data to the iApp Last Mile API (LMA).	3.3.3.4 - ACES/iApp Last Mile API (PUI:ILMA)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0709	The NGLD-M shall be capable of sending (NGLD-M Fill Device) audit data to the iApp Last Mile API (LMA).	3.3.3.4 - ACES/iApp Last Mile API (PUI:ILMA)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0710	The NGLD-M shall include any integrity mechanisms on the audit data transferred over the iApp Last Mile API (LMA).	3.3.3.4 - ACES/iApp Last Mile API (PUI:ILMA)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0711	The NGLD-M shall transfer data to the iApp Last Mile API (LMA) to support accounting per SF-153.	3.3.3.4 - ACES/iApp Last Mile API (PUI:ILMA)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0712	The NGLD-M shall be capable of sending health and monitoring data to the iApp Last Mile API (LMA).	3.3.3.4 - ACES/iApp Last Mile API (PUI:ILMA)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0713	The NGLD-M shall be able to retrieve software / application updates from the ACES/iApp Intermediary over the iApp Last Mile API	3.3.3.4 - ACES/iApp Last Mile API (PUI:ILMA)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	O	Yes	No
NGLD-M_SRD_0714	The NGLD-M shall provide a Last Mile API (LMA) to allow trusted systems / clients (e.g., another NGLD-M, ACES/iApp Workstation) to share data with an NGLD-M.	3.3.3.5 - NGLD-M Last Mile API (PUI:NLMA)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	O	Yes	No
NGLD-M_SRD_0715	The NGLD-M shall allow a trusted ACES/iApp workstation to push products to The NGLD-M's Last Mile API (LMA).	3.3.3.5 - NGLD-M Last Mile API (PUI:NLMA)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	O	Yes	No
NGLD-M_SRD_0716	The NGLD-M shall allow another NGLD-M to send audit data to The NGLD-M's Last Mile API (LMA).	3.3.3.5 - NGLD-M Last Mile API (PUI:NLMA)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	O	Yes	No
NGLD-M_SRD_0717	The NGLD-M shall receive (pushed) cryptographic products from the ACES/iApp Workstation.	3.3.3.5 - NGLD-M Last Mile API (PUI:NLMA)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	O	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0718	The NGLD-M shall allow an iApp Intermediary to push software / application updates to the NGLD-M.	3.3.3.5 - NGLD-M Last Mile API (PUI:NLMA)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	O	Yes	No
NGLD-M_SRD_0719	The NGLD-M shall be capable of being a Storefront to ECUs.	3.3.3.6 - NGLD-M Mobile Device PDE Storefront (PUI:NMDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0720	The NGLD-M shall provide an OTNK-Compliant Storefront allowing connections from approved High Assurance KMI-Aware Devices.	3.3.3.6 - NGLD-M Mobile Device PDE Storefront (PUI:NMDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0721	The NGLD-M shall provide an OTNK-Compliant Storefront allowing connections from approved Medium Assurance KMI-Aware Devices.	3.3.3.6 - NGLD-M Mobile Device PDE Storefront (PUI:NMDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0722	The NGLD-M shall provide an OTNK-Compliant Storefront capable of providing Product Availability Lists (PALs) to consumers / clients.	3.3.3.6 - NGLD-M Mobile Device PDE Storefront (PUI:NMDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0723	The NGLD-M shall provide an OTNK-Compliant Storefront capable of providing product downloads to consumers / clients.	3.3.3.6 - NGLD-M Mobile Device PDE Storefront (PUI:NMDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0724	The NGLD-M shall provide mutual authentication for connected consumers / clients at its OTNK-Compliant Storefront.	3.3.3.6 - NGLD-M Mobile Device PDE Storefront (PUI:NMDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0725	The NGLD-M OTNK-Compliant Storefront shall perform Trust and CRL checks during authentication.	3.3.3.6 - NGLD-M Mobile Device PDE Storefront (PUI:NMDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0726	The NGLD-M OTNK-Compliant Storefront shall perform access control checks to ensure only authorized consumers / clients can make requests.	3.3.3.6 - NGLD-M Mobile Device PDE Storefront (PUI:NMDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No
NGLD-M_SRD_0727	The NGLD-M shall provide tracking for PALs and Products/Packages downloaded from the local OTNK-Compliant device storefront on the NGLD-M.	3.3.3.6 - NGLD-M Mobile Device PDE Storefront (PUI:NMDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	No

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0728	The NGLD-M shall adhere to the latest OTNK Specification (currently Over-the-Network-Keying (OTNK) Specification, version 3.1.2) for communications with the NGLD-M Mobile Device PDE Storefront, specifically regarding authentication, PAL / Product standards and CMS processing.	3.3.3.6 - NGLD-M Mobile Device PDE Storefront (PUI:NMDPDE)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0729	The NGLD-M shall support connections to external OTNK-Compliant Storefronts by proxying / brokering a connection through a networked iApp Workstation.	3.3.3.7 - NGLD-M iApp Proxy Connection (PUI:NIPXY)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.5 Data Transfer KSA	Demonstration	T	Yes	Yes
NGLD-M_SRD_0730	The NGLD-M shall support an interface for data exchange between the UAS and other components of the internal architecture.	3.4 - System internal interface requirements	6.2.1 Mission Data Services KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0731	The NGLD-M shall support an interface for data exchange between the Operating System other components of the internal architecture.	3.4 - System internal interface requirements	6.2.1 Mission Data Services KPP	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0732	The NGLD-M shall support an interface between physical device drivers other components of the internal architecture to support the ability to move data in and out of the NGLD-M.	3.4 - System internal interface requirements	6.2.1 Mission Data Services KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0733	The NGLD-M shall support an interface for data exchange between the High Assurance Cryptographic Module and other components of the internal architecture.	3.4 - System internal interface requirements	6.2.1 Mission Data Services KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0734	The NGLD-M internal interfaces shall be configured and architected in compliance with IASRD and RMF guidelines.	3.4 - System internal interface requirements	6.2.1 Mission Data Services KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0735	The NGLD-M shall provide the capability to store favorites which will minimize the number of user steps required to perform a saved transmit or receive operation.	3.4 - System internal interface requirements	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	No
NGLD-M_SRD_0736	The NGLD-M shall support a BIT testing framework to determine if the device is in a compromised state.	3.4 - System internal interface requirements	6.2.1 Mission Data Services KPP	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0737	The NGLD-M shall display crypto status via an LED.	3.4 - System internal interface requirements	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0738	The NGLD-M shall incorporate LED status indicators to incorporate following system states: zeroize, user not logged in, user logged in, and alarm condition.	3.4 - System internal interface requirements	6.1.3 Net-Ready 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0739	The NGLD-M shall comply with the environmental, safety, and health requirements of appropriate sections of DODD 5000.1, DODD 5000.2, DOD Memorandum “Major Defense Acquisition Programs (MDAPS) and Major Automated Information Systems (MAIS) Acquisition Programs dated 23 October 2002, and all other Federal Environmental safety and health (ESH) laws and regulations.	3.7 - Environmental, Safety, and Operational Health (ESOH) requirements	15.3.2 System Safety	Inspection	T	No	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0740	The NGLD-M shall reduce environmental to lowest extent possible and any residual risks are accepted by risk decision authority IAW AR 385-10/DA PAM 385-16.	3.7 - Environmental, Safety, and Operational Health (ESOH) requirements	15.3.2 System Safety	Inspection	T	No	Yes
NGLD-M_SRD_0741	The NGLD-M shall provide a Health Hazard Assessment (HHA) IAW AR 40-10 at each milestone decision to review and identify Health Hazards.	3.7 - Environmental, Safety, and Operational Health (ESOH) requirements	15.3.2 System Safety	Inspection	T	No	Yes
NGLD-M_SRD_0742	NGLD-M shall meet Chemical, Biological, Radiological, and Nuclear (CBRN) requirements as outlined in the MIL-STD-3056 23 dated: November 2016 US and the Army Nuclear and Chemical Agency's (USANCA) Nuclear, Biological, and Chemical (NBC) Survivability Criteria for Army Materiel, tailored to requirements identified in the CPD.	3.7.1 - Chemical, Biological, Radiological, and Nuclear (CBRNE)	15.3.2 System Safety 6.2.10 Environmental Durability Additional Attribute 15.7.2 CBRN Survivability	Test	T	No	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0743	The NGLD-M shall operate IAW the NGLD-M Operational Mode Summary/Mission Profile (OMS/MP) in a Chemical environment for 72 hours, per contamination guidelines in USANCA Section 6. a.	3.7.1 - Chemical, Biological, Radiological, and Nuclear (CBRNE)	15.3.2 System Safety 6.2.10 Environmental Durability Additional Attribute 15.7.2 CBRN Survivability	Test	T	No	Yes
NGLD-M_SRD_0744	The NGLD-M shall operate IAW OMS/MP in a radioactive, alpha environment for 72, per guidelines in USANCA.	3.7.1 - Chemical, Biological, Radiological, and Nuclear (CBRNE)	15.3.2 System Safety 6.2.10 Environmental Durability Additional Attribute 15.7.2 CBRN Survivability	Test	T	No	Yes
NGLD-M_SRD_0745	The NGLD-M shall operate IAW OMS/MP in a Biological environment for 72 hours, per guidelines in USANCA Section 6. a.	3.7.1 - Chemical, Biological, Radiological, and Nuclear (CBRNE)	15.3.2 System Safety 6.2.10 Environmental Durability Additional Attribute 15.7.2 CBRN Survivability	Test	T	No	Yes
NGLD-M_SRD_0746	The NGLD-M shall operate IAW OMS/MP in a radioactive, beta environment for 72 hours, per guidelines in USANCA.	3.7.1 - Chemical, Biological, Radiological, and Nuclear (CBRNE)	15.3.2 System Safety 6.2.10 Environmental Durability Additional Attribute 15.7.2 CBRN Survivability	Test	T	No	Yes
NGLD-M_SRD_0747	The NGLD-M shall operate IAW OMS/MP in a radioactive, gamma environment for 72 hours, per guidelines in USANCA.	3.7.1 - Chemical, Biological, Radiological, and Nuclear (CBRNE)	15.3.2 System Safety 6.2.10 Environmental Durability Additional Attribute 15.7.2 CBRN Survivability	Test	T	No	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0748	Upon contamination, the NGLD-M device shall be decontaminated, per guidelines in USANCA, Section 6.a. for Decontaminability Criteria.	3.7.1 - Chemical, Biological, Radiological, and Nuclear (CBRNE)	15.3.2 System Safety 6.2.10 Environmental Durability Additional Attribute 15.7.2 CBRN Survivability	Test	T	No	Yes
NGLD-M_SRD_0749	Once decontaminated IAW 007 above, NGLD-M shall be rendered safe IAW USANCA Table 1 and disposed of IAW all relevant federal, state, and local regulations.	3.7.1 - Chemical, Biological, Radiological, and Nuclear (CBRNE3.9.2)	15.3.2 System Safety 6.2.10 Environmental Durability Additional Attribute 15.7.2 CBRN Survivability	Test	T	No	Yes
NGLD-M_SRD_0750	The NGLD-M shall meet requirements for the NGLD-M tailored IASRD.	3.8 - Security and privacy requirements	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Inspection	T	Yes	Yes
NGLD-M_SRD_0751	The NGLD-M shall be compliant with RMF controls for High, High, High classifications for Confidentiality, Integrity, and Availability with classified and tactical overlays.	3.8 - Security and privacy requirements	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Inspection	T	Yes	Yes
NGLD-M_SRD_0752	The NGLD-M shall prevent unauthorized physical access to all internal software, firmware, and hardware elements of the NGLD-M.	3.8.1 - General Security and privacy	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Test	T	No	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0753	The NGLD-M shall support mechanism that guarantees completion of the action once initiated.	3.8.1 - General Security and privacy	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Test	T	No	Yes
NGLD-M_SRD_0754	The NGLD-M Operating System shall provide external interfaces enable/disable control.	3.8.1 - General Security and privacy	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0755	The NGLD-M shall require an explicit user login onto the crypto interface after a hardware reset if a recognized and valid CIK is inserted.	3.8.1 - General Security and privacy	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Demonstration	T	No	Yes
NGLD-M_SRD_0756	The NGLD-M shall support TAMPER protection, as applicable, in accordance with the NSA NGLD-M tailored IASRD.	3.8.2 - Tamper	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Test	T	No	Yes
NGLD-M_SRD_0757	The NGLD-M shall support field TAMPER recovery.	3.8.2 - Tamper	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Test	T	No	Yes
NGLD-M_SRD_0758	The NGLD-M anti-TAMPER capabilities shall be available in the absence of external power.	3.8.2 - Tamper	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Test	T	No	Yes
NGLD-M_SRD_0759	The NGLD-M shall protect software and firmware within the INFOSEC boundary.	3.8.2 - Tamper	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Test	T	No	Yes
NGLD-M_SRD_0760	The NGLD-M shall support TEMPEST protection, as applicable, in accordance with	3.8.3 - TEMPEST	6.2.7 Tamper Detection KSA 6.2.8 Security KSA	Test	T	No	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
	the NSA NGLD-M tailored IASRD Level I requirements.						
NGLD-M_SRD_0761	The NGLD-M shall provide a defined set of auditable events, alerts, and monitoring strategy (continuous, aperiodic, periodic, or some combination of these and handling of audit overflow) in accordance with NGLD-M Tailored IASRD.	3.8.4 - Information Assurance Standards and Certification	6.1.3 Net-Ready 6.2.6 Data Storage KSA 6.2.8 Security KSA	Inspection	T	Yes	Yes
NGLD-M_SRD_0762	The NGLD-M shall meet the requirements of Fail Safe Design Analysis (FSDA) as defined in the NSA NGLD-M tailored IASRD.	3.8.4 - Information Assurance Standards and Certification	6.2.4 Configuration Management KSA 6.2.8 Security KSA	Inspection, Analysis, Demonstration, Test	T	No	Yes
NGLD-M_SRD_0763	The NGLD-M shall include security mechanisms to satisfy the requirements in the NSA NGLD-M tailored IASRD.	3.8.4 - Information Assurance Standards and Certification	6.2.4 Configuration Management KSA 6.2.8 Security KSA	Inspection, Analysis, Demonstration, Test	T	No	Yes
NGLD-M_SRD_0764	The NGLD-M development personnel shall be U.S. citizens and possess Secret or higher clearances.	3.8.4 - Information Assurance Standards and Certification	6.2.4 Configuration Management KSA 6.2.8 Security KSA	Inspection	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0765	The NGLD-M crypto shall be developed in a facility cleared for Secret or higher activities.	3.8.4 - Information Assurance Standards and Certification	6.2.4 Configuration Management KSA 6.2.8 Security KSA	Inspection	T	Yes	Yes
NGLD-M_SRD_0766	The NGLD-M shall implement NGLD-M tailored OSD requirements.	3.8.5 - NGLD-M Operational Security Doctrine (OSD)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Inspection, Analysis, Demonstration, Test	T	Yes	Yes
NGLD-M_SRD_0767	The NGLD-M shall comply with the NGLD-M Operational Security Doctrine.	3.8.5 - NGLD-M Operational Security Doctrine (OSD)	6.2.8 Security KSA	Analysis	T	Yes	Yes
NGLD-M_SRD_0768	The NGLD-M shall provide a defined set of auditable events, alerts, and monitoring strategy (continuous, aperiodic, periodic, or some combination of these and handling of audit overflow) in accordance with RMF security requirements.	3.8.6 - Risk Management Framework (RMF)	6.1.3 Net-Ready 6.2.6 Data Storage KSA 6.2.8 Security KSA	Demonstration	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0769	The NGLD-M shall meet requirements for Risk Management Framework (RMF) certification and be in compliance with all applicable DISA STIGS and SRGs required for accreditation and maintaining the certification.	3.8.6 - Risk Management Framework (RMF)	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.4 Configuration Management KSA 6.2.8 Security KSA	Inspection, Analysis, Demonstration, Test	T	Yes	Yes
NGLD-M_SRD_0770	The NGLD-M shall be internally and externally compatible with other equipment, MIL-STD-464C, within the systems' expected operational electromagnetic environment.	3.9.1 - Environment	6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes
NGLD-M_SRD_0771	The NGLD-M shall meet a high temperature operation requirement of 45°C. The NGLD-M operational temperature testing shall be performed in accordance with MIL-STD-810 G Method 501.5 Procedure II (Operational). The NGLD-M operational temperature testing shall be performed for 2 hours after stabilization.	3.9.1 - Environment	6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0772	The NGLD-M shall operate after being exposed to altitude for two (2) 1 hour cycles at a 10 m/sec rate change under at standard ambient temperature (25°C). The first cycle shall be conducted at altitude of +30,000 feet. The second cycle shall be conducted at altitude of -110 feet. The NGLD-M altitude test shall be performed in accordance with MIL-STD-810 G, Method 500.5 Low Pressure Altitude, and Procedure II – Operation.	3.9.1 - Environment	6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes
NGLD-M_SRD_0773	The NGLD-M shall meet a low temperature operation requirement of -22°C. The NGLD-M operational temperature testing shall be performed in accordance with MIL-STD-810 G Method 501.5 Procedure II (Operational). The NGLD-M operational temperature testing shall be performed for 2 hours after stabilization.	3.9.1 - Environment	6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0774	The NGLD-M shall operate after being exposed for 90 minutes to blowing sand at temperature of 60°C with sand concentration of 2.2± 0.5 g/m3 and an air velocity of 18 m/s (40 – 65 mph). Humidity shall not exceed 30% during the test. The NGLD-M shall be positioned in such a way that the top face of the unit is exposed to the sand stream. The NGLD-M Sand testing shall be performed in accordance with MIL-STD-810 G, Method 510.5 Sand and Dust, Procedure II – Blowing Sand.	3.9.1 - Environment	6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes
NGLD-M_SRD_0775	The NGLD-M shall meet a high temperature storage requirement of +71°C. The NGLD-M storage temperature testing shall be performed in accordance with MIL-STD-810 G Method 501.5 Procedure I (storage) for 7 cycles and 1\24 hours of operation per cycle. The MGLD-M storage temperature testing shall be performed using Table 501.5-III, High temperature cycles,	3.9.1 - Environment	6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
	climatic category A1 – Hot Dry (Induced Conditions).						
NGLD-M_SRD_0776	The NGLD-M shall meet the MIL-STD-810G method 509.5 for storage and operation in the presence of salt fog to determine the effects of salt deposits on the physical and electrical aspects of NGLD-M. Use a 5 ± 1 percent salt solution concentration (paragraph 6.1, reference b.). Use water as described in Part One, paragraph 5.16, 48 hours of exposure and 48 hours of drying time.	3.9.1 - Environment	6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0777	The NGLD-M shall operate after immersion depth of 1.5 meters at 25°C temperature for 30 minutes. The NGLD-M shall be conditioned prior to the test for 2 hours at 25°C temperature. The NGLD-M Immersion testing shall be performed in accordance with MIL-STD-810 G, Method 512.5 Immersion, Procedure I.	3.9.1 - Environment	6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes
NGLD-M_SRD_0778	The NGLD-M shall not ignite the 3.8% n-hexane and air mixture when switched on and off and operated at sea and at 40,000 ft. (12,200m) levels while under 60°C temperature. The NGLD-M Explosive Atmosphere testing shall be performed in accordance with MIL-STD-810G, method 511.5, Procedure I – Explosive Atmosphere.	3.9.1 - Environment	6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes
NGLD-M_SRD_0779	The NGLD-M shall operate after being exposed to each axis of random vibration for 2 hour cycle (one cycle per axis) with functional test conducted after each cycle using Vibration Environment Category 20 – Operation Ground Vehicles	3.9.1 - Environment	6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
	(see Table 514.6-I, MIL-STD-810 G for reference).						
NGLD-M_SRD_0780	The NGLD-M shall operate after 26 transit drops on a plywood surface on each face and corner from the hi\eight of 48". The NGLD-M transit drop testing shall be performed in accordance with MIL-STD-810 G, Method 516.6 Shock, and Procedure IV – Transit Drop with functional test conducted after each drop.	3.9.1 - Environment	6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes
NGLD-M_SRD_0781	The NGLD-M vibration testing shall be performed in accordance with MIL-STD-810 G, Method 514.6 Vibration, Procedure I-General Vibration using profile outlined in Figure 514.6C-3 and Table 514.6C-VI, Category 4 – Composite Wheeled Vehicle Vibration Exposure.	3.9.1 - Environment	6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0782	The NGLD-M conducted emissions shall comply with the values in RE102 for power leads, 10 KHz to 18 GHz in accordance with MIL-STD-461E. The levels used for this test shall be those indicated for Fixed Wing Internal.	3.9.1 - Environment	6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes
NGLD-M_SRD_0783	The NGLD-M conducted susceptibility shall comply with the bulk cable injection values in CE 102 MIL-STD-461G is applicable from 10 kHz to 10 MHz for all power leads, including returns, which obtain power from other sources not part of the EUT.	3.9.1 - Environment	6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes
NGLD-M_SRD_0784	The NGLD-M conducted susceptibility shall comply with the bulk cable injection values in CS114 MIL-STD-461E Aircraft Internal in Table VI, 10 KHz to 200 MHz.	3.9.1 - Environment	6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes
NGLD-M_SRD_0785	The NGLD-M radiated susceptibility shall comply with the electric field values in RS103, 75 V/m from 2 MHz to 40 GHz in accordance with MIL-STD-461E All Ships (Above Decks) and Submarines	3.9.1 - Environment	6.2.10 Environmental Durability Additional Attribute	Test	T	No	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
	(External) at the Army and Navy levels in Table VII.						
NGLD-M_SRD_0786	The NGLD-M shall meet High-Altitude Electromagnetic Pulse (HEMP) requirements as defined in MIL-STD-2169B, when it is not turned on and with no external cables are attached.	3.9.2 - High-Altitude Electromagnetic Pulse (HEMP)	6.2.10 Environmental Durability Additional Attribute	Test	O	No	Yes
NGLD-M_SRD_0787	The NGLD-M shall have an operating system that meets all DoD security requirements/regulation.	3.10.3.1 - Operating System	6.2.4 Configuration Management KSA 6.2.8 Security KSA	Test	T	No	Yes
NGLD-M_SRD_0788	The NGLD-M shall have an operating system that allows the execution of all capabilities within the device.	3.10.3.1 - Operating System	6.2.4 Configuration Management KSA 6.2.8 Security KSA	Test	T	No	No
NGLD-M_SRD_0789	The NGLD-M shall generate and maintain a plan for maintaining scheduled operating system IAVA updates.	3.10.3.1 - Operating System	6.2.4 Configuration Management KSA 6.2.8 Security KSA	Analysis	T	No	No
NGLD-M_SRD_0790	The NGLD-M shall have an operating system that can be fixed/patched in the field (operational state) for identified security	3.10.3.1 - Operating System	6.2.4 Configuration Management KSA 6.2.8 Security KSA	Test	T	No	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
	vulnerabilities without adversely impacting system operations.						
NGLD-M_SRD_0791	The NGLD-M shall have an operating system that adheres to all applicable Security Technical Implementation Guides (STIGs).	3.10.3.1 - Operating System	6.2.4 Configuration Management KSA 6.2.8 Security KSA	Test	T	No	Yes
NGLD-M_SRD_0792	The NGLD-M shall have an operating system that adheres to all applicable Security Requirements Guides (SRG).	3.10.3.1 - Operating System	6.2.4 Configuration Management KSA 6.2.8 Security KSA	Test	T	No	Yes
NGLD-M_SRD_0793	The NGLD-M shall have a system Mean Time Between Failures (MTBF) of greater than or equal to 864 (Objective: 1,774 hours) hours with 80% confidence under conditions outlined in the OMS/OP.	3.11.1 - Reliability, Availability, Maintainability (RAM)	6.2.9 Operational Availability (Ao) KSA	Test	T	No	Yes
NGLD-M_SRD_0794	The NGLD-M shall have a Mean Time To Repair (MTTR) of no greater than 20 minutes with 80% confidence. The MTTR shall include both hardware and software repairs.	3.11.1 - Reliability, Availability, Maintainability (RAM)	6.2.9 Operational Availability (Ao) KSA	Test	T	No	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0795	The NGLD-M shall have an Inherent Availability (IA) of 99.9%.	3.11.1 - Reliability, Availability, Maintainability (RAM)	6.2.9 Operational Availability (Ao) KSA	Test, Analysis	T	No	Yes
NGLD-M_SRD_0796	The NGLD-M shall support field updates for all embedded software and firmware.	3.11.1 - Reliability, Availability, Maintainability (RAM)	6.2.9 Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0797	The NGLD-M operational battery pack should be user replaceable.	3.11.1 - Reliability, Availability, Maintainability (RAM)	6.2.3 SWAP (size, weight, and power) KPP 6.2.9 Operational Availability (Ao) KSA	Test	T	No	Yes
NGLD-M_SRD_0900	The NGLD-M shall calculate the total run time. The run time is defined as the time the NGLD-M power is turned on until the NGLD-M power is turned off.	3.11.1 - Reliability, Availability, Maintainability (RAM)	6.2.9 Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0901	The NGLD-M run time shall be calculated in seconds (unit of run time is seconds).	3.11.1 - Reliability, Availability, Maintainability (RAM)	6.2.9 Operational Availability (Ao) KSA	Test	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0902	The NGLD-M runtime shall be accumulative during the NGLD-M lifetime.	3.11.1 - Reliability, Availability, Maintainability (RAM)	6.2.9 Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0903	The NGLD-M runtime shall not be reset.	3.11.1 - Reliability, Availability, Maintainability (RAM)	6.2.9 Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0904	The NGLD-M shall allow administrator user to retrieve accumulative runtime.	3.11.1 - Reliability, Availability, Maintainability (RAM)	6.2.9 Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0905	The NGLD-M run time shall be included in a log file.	3.11.1 - Reliability, Availability, Maintainability (RAM)	6.2.9 Operational Availability (Ao) KSA	Test	T	Yes	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0798	The NGLD-M design shall support additional functionality growth.	3.11.2 - Expandability	6.1.3 Net-Ready 6.2.1 Mission Data Services KPP 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.3 SWAP (size, weight, and power) KPP 6.2.4 Configuration Management KSA 6.2.5 Data Transfer KSA 6.2.6 Data Storage KSA 6.2.7 Tamper Detection KSA 6.2.8. Security KSA 6.2.9 Operational Availability (Ao) KSA	Inspection / Analysis	T	No	Yes
NGLD-M_SRD_0799	The NGLD-M shall be in the range of 6.14”(L) x 3.03” (W) x 1.46” (D) to 8.75” (L) x 10” (W) x 2.75” (D)	3.11.3 - Performance	6.2.3 SWAP (size, weight, and power) KPP	Test	T	No	Yes
NGLD-M_SRD_0800	The NGLD-M display shall be maximized as to extent possible.	3.11.3 - Performance	6.2.3 SWAP (size, weight, and power) KPP	Test	T	No	Yes
NGLD-M_SRD_0801	The NGLD-M vendor shall support depot maintenance of NGLD-M.	3.15 - Logistics-related requirements	14.4.5 Unit (Sustainment) Training 14.4.8 Logistics Management	Test	T	No	Yes

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
			Information Data Collection				
NGLD-M_SRD_0802	The NGLD-M vendor shall integrate Government Furnished Software (GFS), termed User Application Software (UAS), developed by Naval Information Center, Pacific (NIWC-PAC).	3.16.1 - User Application Software (UAS) Integration	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP	Demonstration	T	Yes	Yes
NGLD-M_SRD_0803	The NGLD-M system shall have a Software Update Tool to load and or update NGLD-M software/firmware.	3.16.2 - Supporting Tools	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 14.5.3 Support Equipment	Test	T	Yes	No
NGLD-M_SRD_0804	The NGLD-M Software Update Tool shall embed a set of instructions to the user related to the software/firmware updates available for the NGLD-M.	3.16.2 - Supporting Tools	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 14.5.3 Support Equipment	Test	T	Yes	No
NGLD-M_SRD_0805	The NGLD-M Software Update Tool shall dynamically determine the type of the NGLD-M hardware platform.	3.16.2 - Supporting Tools	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 14.5.3 Support Equipment	Test	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0806	The NGLD-M Software Update Tool shall provide to the user a list of software versions available for the software/firmware updates based on the identified NGLD-M hardware platform.	3.16.2 - Supporting Tools	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 14.5.3 Support Equipment	Test	T	Yes	No
NGLD-M_SRD_0807	The NGLD-M Software Update Tool shall support all the external interfaces, to include but not limited to Fill Port, USB, Ethernet, to load/update the NGLD-M software/firmware.	3.16.2 - Supporting Tools	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 14.5.3 Support Equipment	Test	T	Yes	Yes
NGLD-M_SRD_0808	The NGLD-M Software Update Tool shall provide a user selectable option for the external interface through which software/firmware update will be loaded, to include but not limited to Fill Port, USB, or Ethernet.	3.16.2 - Supporting Tools	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 14.5.3 Support Equipment	Test	T	Yes	No
NGLD-M_SRD_0809	The NGLD-M Software Update Tool shall provide to the user a list of options for standalone updates for various software/firmware components of the NGLD-M.	3.16.2 - Supporting Tools	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 14.5.3 Support Equipment	Test	T	Yes	No

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0810	The NGLD-M shall have a tool to generate ECU profiles that can be ingested into the NGLD-M allowing the NGLD-M to support new and existing ECUs.	3.16.2 - Supporting Tools	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 14.5.3 Support Equipment	Test	T	Yes	No
NGLD-M_SRD_0811	The NGLD-M ECU Profile Definition Tool shall adhere to requirements listed for ECU Profile generation in section 3.2.14 - ECU-Profile Management.	3.16.2 - Supporting Tools	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 14.5.3 Support Equipment	Test	T	Yes	No
NGLD-M_SRD_0812	The NGLD-M shall provide a production representative Test Asset configuration.	3.16.3 - Test Asset	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.9 Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0813	The NGLD-M Test Asset configuration shall use production representative developmental software.	3.16.3 - Test Asset	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.9 Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0814	The NGLD-M Test Asset configuration and/or representative development software shall provide a clear label denoting the device as "TEST ONLY".	3.16.3 - Test Asset	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.9 Operational Availability (Ao) KSA	Inspection	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0815	The NGLD-M Test Asset production representative development software shall perform identical functionality as the production software.	3.16.3 - Test Asset	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.9 Operational Availability (Ao) KSA	Test	T	No	No
NGLD-M_SRD_0816	The NGLD-M Test Assets shall provide Operating System file system access.	3.16.3 - Test Asset	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.9 Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0817	The NGLD-M Test Asset developmental software shall include software debug tools and features.	3.16.3 - Test Asset	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.9 Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0818	The NGLD-M Test Asset shall support an automated method to load software unsigned NSA software.	3.16.3 - Test Asset	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.9 Operational Availability (Ao) KSA	Test	T	Yes	Yes
NGLD-M_SRD_0819	The NGLD-M Test Asset shall support production representative peripheral interfaces.	3.16.3 - Test Asset	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.9 Operational Availability (Ao) KSA	Test	T	Yes	Yes

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SRD PUI	SRD Requirement Text	SRD Section (# - Title)	CPD Reference	Qualification Method	Threshold / Objective	UAS?	Vendor ?
NGLD-M_SRD_0820	The NGLD-M Test Asset shall have a unique hardware configuration part number and name that is separate from the NGLD-M production model.	3.16.3 - Test Asset	6.1.3 Net-Ready 6.2.2 Interoperability, Standardization and Commonality KPP 6.2.9 Operational Availability (Ao) KSA	Test	T	Yes	No

UNCLASSIFIED//FOR OFFICIAL USE ONLY