Hewlett Packard Enterprise

HPE HLR Cryptographic Module
FIPS 140-2 Non-proprietary Security Policy

Software Version: I-HLR 01.08.01

Version 4.0

2020-11-25

Communications & Media Solutions

Hewlett Packard Enterprise

10810 Farnam Drive OMA01

Omaha, Nebraska 68154

TRADEMARKS or SERVICE MARKS

The following are trademarks or service marks of Hewlett Packard Enterprise Corporation:

HEWLETT PACKARD ENTERPRISE, HPE, HLR.

All other brand names and product names are trademarks or registered trademarks of their respective companies.

COPYRIGHT

This document may be freely copied and distributed without the Author’s permission provided that it is copied and distributed in its entirety without modification.

© 2020 Hewlett Packard Enterprise / atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

(This page left intentionally blank)

© 2020 Hewlett Packard Enterprise / atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

Hewlett Packard Enterprise

Table of Contents

© 2020 Hewlett Packard Enterprise / atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

© 2020 Hewlett Packard Enterprise / atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

1. Introduction

This document is the Federal Information Processing Standards (FIPS) 140-2 non-proprietary Security Policy for the HEWLETT PACKARD ENTERPRISE (HPE) HLR Cryptographic Module to meet FIPS 140-2 security Level One requirements. This Security Policy details the secure operation of the HPE HLR Cryptographic Module version I-HLR 01.08.01, developed by HPE as required in FIPS Publication 140-2 as published by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce. The Federal Information Processing Standard Publication 140-2 (FIPS 140-2) is a U.S. government computer security standard used to accredit cryptographic modules. It was issued by the National Institute of Standards and Technology (NIST).

1.1 Audience

This document is required as a part of the FIPS 140-2 validation process. It describes the HPE HLR Cryptographic Module in relation to FIPS 140-2 requirements. The companion document "I-HLR Installation Guide[1]" provides the guidance for installing the HLR Cryptographic Module. The companion document "HPE HLR Cryptographic Module User Guide[1]" is a technical reference for Service Providers using the HLR Cryptographic Module.

1.2 Product Description

The HPE Home Location Register (HLR) is a centralized data repository of static and transient subscriber profile information that manages subscriber network access, availability, and location in wireless networks defined by European Telecommunications Standards Institute (ETSI). The ETSI-based HLR functionality is referred to as Global System for Mobile communications (GSM) and Universal Mobile Telecommunications System (UMTS).

The Authentication Center (AuC) functionality present in the HPE HLR ensures that only legitimate subscribers obtain access to the GSM/UMTS.

The HPE HLR protects sensitive subscriber data elements related to the information required to authenticate subscriber network access. The HPE HLR Cryptographic Module provides the cryptography required to protect the sensitive subscriber data elements. FIPS 140-2 approved cryptographic algorithms (for example, AES-128 ECB) are used for cryptographic key protection, subscriber AV generation, and the protection of sensitive application data (for example, GSM/UMTS Ki values).

The HLR/AuC Call Processing component uses subscriber keys in conjunction with FIPS 140-2 approved cryptographic algorithms to generate Authentication Vectors (AVs) for GSM/UMTS subscriber authentication. (An AV, in the context of this reference, is security context data that enables a UMTS/GSM wireless network to authenticate a UMTS/GSM wireless subscriber. The HPE HLR utilizes a subscriber symmetric key present in both the HLR and the subscriber's user equipment (UE) to generate the authentication vector. The HPE HLR and a Universal SIM (USIM) or Subscriber Identity Module (SIM) present in the UE contain the key value). The Authentication Vector is an array of concatenated components that are encrypted by the subscriber symmetric key. To generate Authentication vector the module uses the module's DRBG to generate random data which is then encrypted with the subscriber symmetric key using AES-ECB encryption algorithm.

[1] The reference document is provided with the module.

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

2. Cryptographic Module Specification

This section describes the module and its functionality as part of the larger product.

2.1 Module Overview

The HPE HLR Cryptographic Module (hereafter referred to as “the module” or simply “CM”) is a multi-chip standalone software module running on a GPC. The module provides the cryptographic services (e.g. symmetric encryption and decryption, message digest, and SP800-90A random number generation) required to protect the sensitive subscriber data elements. The module is implemented as a shared library. The shared library defines the logical boundary as shown by the red box in the figure below.

The HPE HLR Cryptographic Module is comprised of the following files:

libCMOD, keymgrx, libcrypt, libOSSL, libSSLF

The following figure illustrates the HPE HLR Cryptographic components. The figure references key material, key storage, utilities, and runtime components and depicts the relationships between the components and the HLR Cryptographic Module. Please note that the database files are not part of the cryptographic module boundary and are shown in the Diagram 2-1 and Table 2-1 for reference.

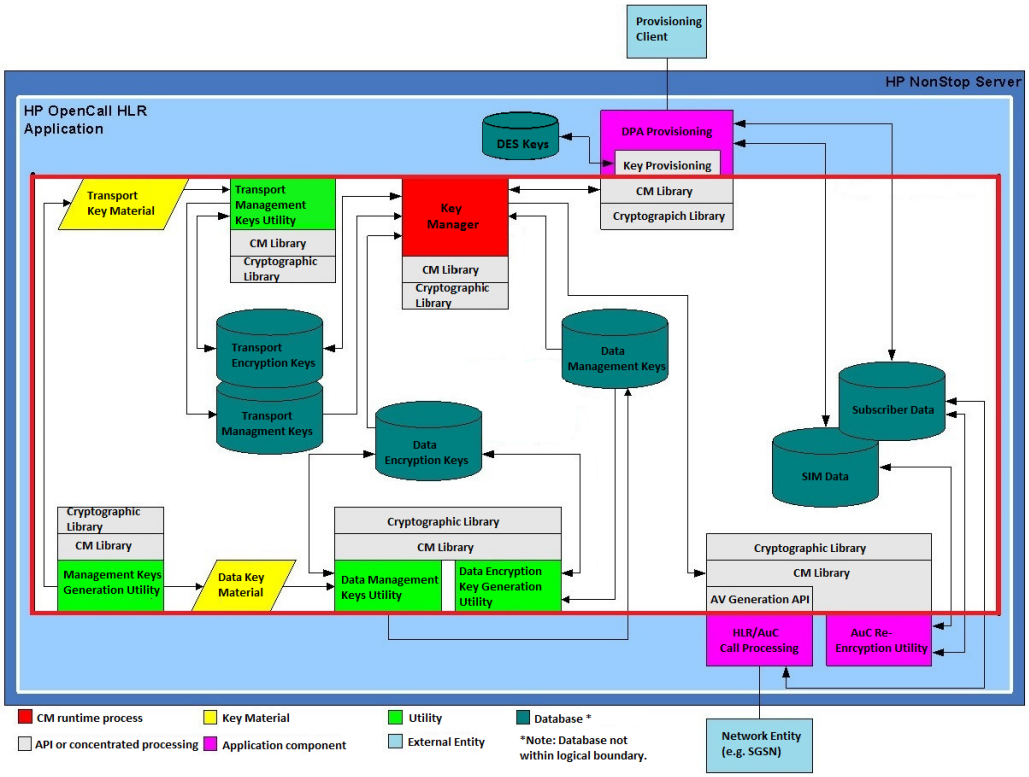

Figure 2-1: HLR Cryptographic Module

The following table provides a brief summary of the components contained within the Open Call HLR CM depicted in Figure 2-1. The KEKs listed are the Management Keys used by the Data Management Keys Utility and Transport Management Keys Utility to encrypt Data Encryption and Transport Encryption keys. This allows the Data Encryption and Transport Encryption keys to be stored encrypted in their respective databases shown in Figure 2-1

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

Component	Brief Description
Data Key Material	An encrypted file generated by the Management Keys Generation Utility. The HLR application uses the file to securely install KEKs and Master Seed Keys into the Data Management Keys data file.
Transport Key Material	An encrypted file generated by the Management Keys Generation Utility. The HLR application uses the file to securely install KEKs into the Transport Management Keys data file and the first entry in the Transport Encryption Keys data file.
Management Keys Generation Utility	Used to generate KEKs and Master Seed Keys for the Data Management Keys data file and KEKs for the Transport Management Keys and Transport Encryption Keys data files. Please note that the Master Seed Key although generated by the module but is no longer used[2].
Data Management Keys Utility	Uses the Data Key Material to install KEKs and Master Seed Keys into the Data Management Keys data file. Please note that the Master Seed Key although stored in the data file, is no longer used by the module[2].
Data Encryption Key Generation Utility	The utility uses the active KEK from the Data Management Keys data file to cover the generated cryptographic key stored in the Data Encryption Keys data file.
Transport Management Keys Utility	Uses the Transport Key Material to install KEKs into the Transport Management Keys data storage component and the first entry in the Transport Encryption Keys data storage component.
Key Manager	Distributes cryptographic keys, used to cover sensitive data attribute values, from the Data Encryption Keys data files. Also distributes cryptographic keys, used to cover sensitive data transmitted over the provisioning stream, from the Transport Encryption Keys file.
Key Provisioning	Manages the provisioning of subscriber AuC key values.
AV Generation API	Generates AVs for AuC related network traffic.
CM Library	Shared library which interfaces with the Key Manager to retrieve cryptographic keys and uses retrieved keys to encrypt and decrypt sensitive data elements stored in the Subscriber Data and SIM Data files as well as data elements transmitted over the provisioning stream. Also, provides routines that check the status of the CM module.
Cryptographic Library	Shared library which provides the cryptographic algorithms (e.g. AES and Secure Hash Algorithm (SHA)).
Data Management Keys	A data file that contains KEKs used to respectively cover and generate cryptographic keys in the Data Encryption Keys data file.
Data Encryption Keys	A data file that contains cryptographic keys used by application components (e.g. HLR AC Call Processing) to protect sensitive data elements.
Transport Management Keys	A data file that contains KEKs used to cover the cryptographic keys stored in the Transport Encryption Keys data file.

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

Transport Encryption Keys	A data file that contains cryptographic keys used to cover sensitive data elements transported over the DPA provisioning stream. All cryptographic key entries cover sensitive data elements over the provisioning stream.
Subscriber Data SIM Data	Legacy data file that contains sensitive data elements (e.g. K) covered by a cryptographic key stored in the Data Encryption Keys data file.

Table 2-1: Brief Component Description

For the software module, the physical boundary is considered to be the surface of the case of the target platform as show below:

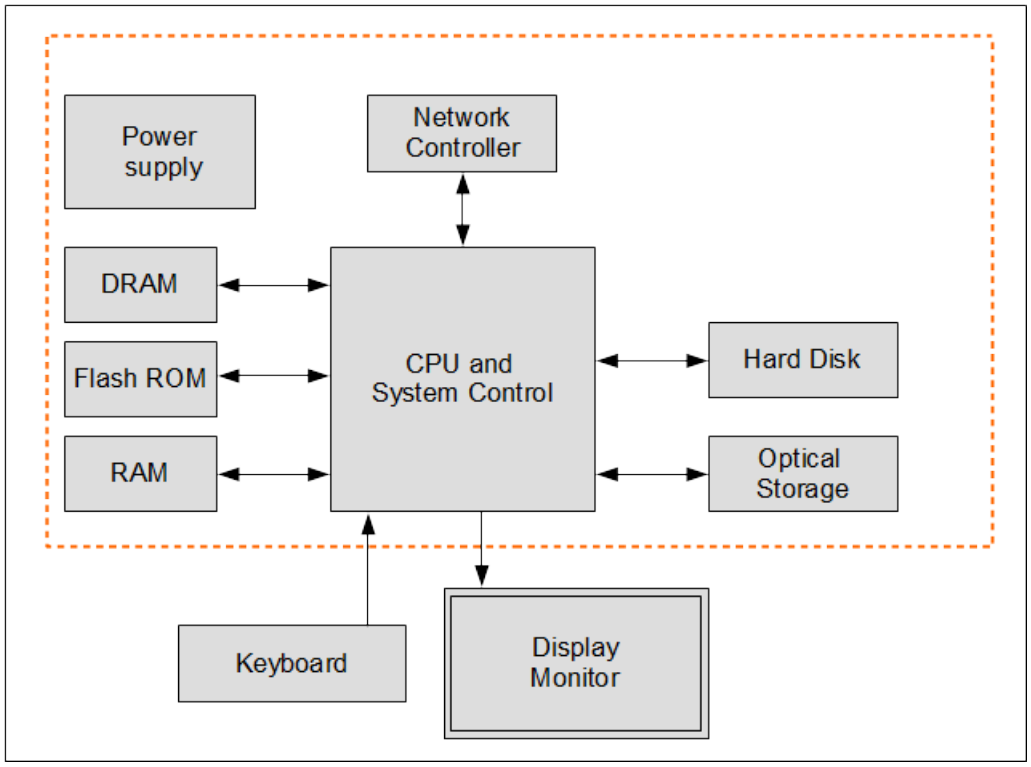

Figure 2-2: Physical Boundary

[2] The "Master seed key" is present for historical purposes and was used previously as a seed key for the X9.31 PRNG. With the module making use of SP 800-90A DRBG that does not require any seed key, the "Master seed key" is considered as inactive and is not used by any service from the module.

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

2.2 FIPS 140-2 Validation

For the purpose of the FIPS 140-2 validation, the module is a software-only, multi-chip standalone cryptographic module validated at overall security level 1. The table below shows the security level claimed for each of the eleven sections that comprise the FIPS 140-2 standard:

Security Component	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Table 2-2: Security Levels

Table 2-3 shows the platform on which the cryptographic module was tested on:

Manufacturer	Model	O/S & Version
HPE	Integrity NonStop BladeSystem NB54000c_with Intel Itanium Processor 9300	HP NonStop v J06.18
	Integrity NonStop BladeSystem NB56000c with Intel Itanium Processor 9500	HP NonStop v J06.23.01

Table 2-3: Platforms Tested

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

2.3 Modes of Operation

When installed, the module only operates in FIPS approved mode. The module provides cryptographic services to applications running in the user space of the underlying operating system through an application program interface (API). The module interacts with the operating system via system calls. The GSM/UMTS functionality within the HPE HLR can utilize the cryptographic module operating in FIPS 140-2 approved mode.

The CM Library uses the data encryption key to either decrypt or encrypt data (for example, subscriber keys to generate AVs). To retrieve a new data encryption key, the Service Provider's personnel must configure the new system-level key index (Ki) and algorithm version values that the system uses as the basis for the generation of the new data encryption key.

The following table shows the FIPS-Approved algorithms that are supported by the module:

Algorithm/Modes	Standard/Usage	Key Lengths	Certificate Number
AES ECB, CTR modes	[SP800-38A] Encryption and Decryption	128-bits (ECB only), 256-bits	#3503 and #C1713,
SHA-1, SHA-256	[FIPS180-4] Message Digest	N/A	#2890 and #C1713
HMAC SHA-1	[FIPS198-1] Message Integrity	112-bits	#2237 and #C1713
CTR_DRBG	[SP800-90A] Random Number Generation	256-bits	#872 and #C1713
CKG	[SP800-133]	128 and 256-bits	vendor affirmed

Table 2-4: FIPS-Approved Algorithms

In addition, the module implements the following FIPS-Allowed algorithms:

Algorithm/Modes	Caveat/Cert	Use
NDRNG	N/A	The module obtains entropy data from NDRNG to seed the DRBG. The module provides 256-bits of min-entropy.
AES- ECB-128	AES (Certs. #3503 and #C1713, key unwrapping)	The module performs key unwrapping using AES-ECB with 128-bit keys as allowed by IG D.9.

Table 2-5: FIPS-Allowed Algorithms

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

3. Ports and Interfaces

As a software-only module, the module does not have physical ports. For the purpose of the FIPS 140-2 validation, the physical ports are interpreted to be the physical ports of the hardware on which it runs.

The logical interfaces are the application programming interface (API) through which applications request services (as show in the table below):

Logical Interface	Description
Control In	API function calls, API input parameters for control, CLI
Status Out	API return codes, API output parameters for status, CLI
Data In	API input parameters for data, CLI
Data Out	API output parameters for data, CLI

Table 3-1: Ports and Interfaces

The Data Input interface consists of the input parameters of the API functions data received through the I/O system calls, and CLI. The Data Output interface consists of the output parameters of the API, and CLI. The Control Input interface consists of the API function calls the input parameters and the CLI used to control the behavior of the module. The Status Output interface includes the return values of the API functions, status sent through output parameters, and the CLI. The CLI is the command line interface provided by the utilities listed in table 2-1.

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

4. Roles, Services and Authentication

4.1 Roles

This section contains a table that identifies the CM components and the CM roles that have access to or run the components. Note that the roles are actually associated with the role number and the role names contained in the table are for illustrative purposes only.

#	Role	Description
1	Crypto Officer	The Crypto Officer role has the ability to install, update, and destroy the CM components. Note that the Crypto Officer role cannot run any of the CM components. Also, any updates to the CM components that deviates the module to a version different than "I-HLR 01.08.01" will no longer be considered as a FIPS 140-2 validated module.
2	FIPS Mode Manager	The FIPS Mode Manager role has the ability to use the FIPS Indicator Utility to query the CM FIPS Mode indicator in the FIPS Info file as well as query and set the key limit threshold[3].
3	Management Key Generation	The Management Key Generation role has the ability to use the Management Keys Generation Utility to generate data and transport management key material.
4	Data Management Key Installation	The Data Management Key Installation role possesses the ability to use the Data Management Keys Utility to install data management keys in the Data Management Keys file and to re-encrypt entries in the Data Encryption Keys file with the latest Data Management Keys file KEK. The Data Management Key Installation role also has the ability to initiate the destruction of the Data Management Keys file.
5	Transport Management Key Installation	The Transport Management Key Installation role has the ability to use the Transport Management Keys Utility to install transport management keys in the Transport Management Keys file, to install a KEK in the Transport Encryption Keys file default record, and to re-encrypt the entries in the Transport Encryption Keys file. The Transport Management Key Installation role also has the ability to initiate the destruction of the Transport Management Keys and Transport Encryption Keys.
6	Data Encryption Key Generation	The Data Encryption Key Generation role has the ability to use the Data Encryption Key Generation Utility to generate Data Encryption Keys and place the generated keys in the Data Encryption Keys file.

[3] The key limit threshold is a cryptoperiod that defines the duration of time that a given key can be used

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

#	Role	Description
		The Data Encryption Key Generation role also has the ability to initiate the destruction of the Data Encryption Keys files.
7	CM Operator	The CM Operator role has the ability to run the Key Manager and Transport Key Manager runtime processes.
8	Crypto Library User	The Crypto Library User role possesses the ability to use the libraries associated with the CM and runs the FIPS Command Utility.

Table 4-1: Cryptographic Module Roles

The following table illustrates the capabilities of each role in regard to each HLR component. The end of the table contains a legend that identifies the abbreviations used in the cells of the table.

The numbers starting in column two of the header rows correlate with the role numbers specified in Table 4-1.

Component/Role #	1	2	3	4	5	6	7	8
FIPS Info File	PCRW	RW	R	R	R	R	RW	R
FIPS Status File	PCRW	R	RW	RW	RW	RW	RW	RW
Data Management Keys	PCRW			RW		R	RW	
Data Encryption Keys	PCRW			RW		RW	RW	
Transport Management Keys	PCRW				RW		RW	
Transport Encryption Keys	PCRW				RW		RW	
Subscriber Data	PCRW							RW
SIM Data	PCRW							RW
Data Key Material			WC	RPC				
Transport Key Material			WC		RPC			
FIPS Indicator Utility	PCRW	E						
Management Keys Generation Utility	PCRW		E					
Data Management Keys Utility	PCRW			E				
Data Encryption Key Generation Utility	PCRW					E		
Transport Management Keys Utility	PCRW				E			
FIPS Command Utility	PCRW							E
AuC Re-Encryption Utility	PCRW							WE

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

Component/Role #	1	2	3	4	5	6	7	8
Key Manager	PCRW						WE[1]	
CM Library	PCRWE						E	E
Cryptographic Library	PCRW						E	E
Key Provisioning	PCRW						E	E
AV Generation API	PCRW						E	E
R – Read File Content W – Write, Delete, and Update File Content E – Execute File P – Purge File				C – Create File 1 – Restriction by executable and process name				

Table 4-2: Cryptographic Module Privileges by Role

Note: The components listed in column one of Table 4-2 represent all of the components of the cryptographic module with the addition of supporting components which interface with the module.

4.2 Services

The module provides services to users that assume one of the available roles. All services are described in detail in the user documentation.

The following table shows the available services, the roles that can request the service, the Critical Security Parameters involved and how they are accessed:

Service	Function	Role (Numbers from Table 4-1 Cryptographic Module Roles)	CSPs	Algorithm	Service Ports I-In, O-Out C-Command D-Data S-Status
CreateKey	Create a key material file	3	AES 128 Key, AES 256 DRBG Seed	AES, SHA-256, SP800-90A CTR_DRBG	CI, DI, SO
DEKAdd (Data Encryption Key Add)	Add a key to the Data Encryption Key DB	6	AES 128 Key	AES, SHA-256	CI, SO
DEKClear (Data Encryption Key Clear)	Clears the I-HLR registration for specified key index and algorithm version	1	AES 128 Key	AES, SHA-256	CI, SO

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

Service	Function	Role (Numbers from Table 4-1 Cryptographic Module Roles)	CSPs	Algorithm	Service Ports I-In, O-Out C-Command D-Data S-Status
DEKDeactivate (Data Encryption Key Deactivate)	Deactivate a key in the Data Encryption Key DB	1	AES 128 Key	AES, SHA-256	CI, SO
DEKDestroy (Data Encryption Key Destroy)	Destroy a key from the Data Encryption Key DB	1	AES 128 Keys	N/A	CI, SO
DEKMigrate (Data Encryption Key Migrate)	Migrate the keys in the Data Encryption Key DB	7	AES 128 Key	AES, SHA-256	CI, SO
DEKReencrypt (Data Encryption Key Reencrypt)	Re-encrypt the keys in the Data Encryption Key DB	4	AES 128 Key	AES, SHA-256	DO, DI, CI, SO
DEKReport (Data Encryption Key Report)	Reports the keys in the Data Encryption Key database	6	N/A	N/A	DO, CI, SO
DEKUsageReport (Data Encryption Key Usage Report)	Reports the references to a Data Encryption Key for a specified Key Index and algorithm Version.	1	N/A	N/A	DO, CI, SO
DMKActivate (Data Management Key Activate)	Activate a key (or keys) in the Data Management Key DB	4	N/A	N/A	CI, SO
DMKAdd	Add a key to the Data	4	AES 128 Key	AES, SHA-256	CI, DI, SO

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

Service	Function	Role (Numbers from Table 4-1 Cryptographic Module Roles)	CSPs	Algorithm	Service Ports I-In, O-Out C-Command D-Data S-Status
(Data Management Key Add)	Management Key DB				
DMKDeativate (Data Management Key Deactivate)	Deactivate a key (or keys) in the Data Management Key DB	4	N/A	N/A	CI, SO
DMKDestroy (Data Management Key Destroy)	Destroy a key from the Data Management Key DB	1	AES 128 Keys	N/A	CI, SO
DMKReport (Data Management Key Report)	Reports the keys in the Data Management Key database	4	N/A	N/A	DO, CI, SO
KMDestroy (Key Material Destroy)	Destroy a key material file	1	AES 128 Key	N/A	CI, SO
TEKAdd (Transport Encryption Key Add)	Add a key to the Transport Encryption Key DB	5	AES 128 Key	N/A	CI, SO
TEKDestroy (Transport Encryption Key Destroy)	Destroy a key from the Transport Encryption Key DB	1	AES 128 Keys	N/A	CI, SO
TEKReencrypt (Transport Encryption Key Reencrypt)	Re-encrypt the keys in the Transfer Encryption Key DB	5	AES 128 Key	AES, SHA-256	DO, DI, CI, SO
TEKReport (Transport Encryption Key Report)	Reports the keys in the Transport Encryption	5	N/A	N/A	DO, CI, SO

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

Service	Function	Role (Numbers from Table 4-1 Cryptographic Module Roles)	CSPs	Algorithm	Service Ports I-In, O-Out C-Command D-Data S-Status
	Key database				
TMKActivate (Transport Management Key Activate)	Activate a key (or keys) in the Transport Management Key DB	5	N/A	N/A	CI, SO
TMKAdd (Transport Management Key Add)	Add a key to the Transport Management Key DB	5	AES 128 Key	N/A	DI, CI, SO
TMKDeactivate (Transport Management Key Deactivate)	Deactivate a key (or keys) in the Transport Management Key DB	5	N/A	N/A	CI, SO
TMKDestroy (Transport Management Key Destroy)	Destroy a key from the Transport Management Key DB	1	AES 128 Keys	N/A	CI, SO
TMKReport (Transport Management Key Report)	Reports the keys in the Transport Management Key database	5	N/A	N/A	DO, CI, SO
CM APIs	Encrypt and decrypt data (via key index)	8	AES 128 Key	AES, SHA-256	DI, DO, SO
FIPS Command Utility	Initiate Self-Tests, Start and Stop Module	8	N/A	AES, SHA-1, HMAC-SHA-1, SHA-256, AES based SP800-90A CTR_DRBG	CI, SO

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

Service	Function	Role (Numbers from Table 4-1 Cryptographic Module Roles)	CSPs	Algorithm	Service Ports I-In, O-Out C-Command D-Data S-Status
FIPS Indicator Utility	Get FIPS Status, Alter/Query key limit threshold	FIPS_MODE_MGR[4], All roles	N/A	N/A	CI, SO
Set up and Configure Module	Install module, create files and roles	1	N/A	N/A	CI, SO

Table 4-3: Module Services

4.3 Operator Authentication

The module does not implement authentication. The role is implicitly assumed based on the service requested.

[4]All roles can query the status but only the FIPS Mode Manager can alter the threshold for cryptographic keys that are about to expire.

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

5. Operational Environment

The module operates in a modifiable operational environment per the FIPS 140-2 specifications.

5.1 Operational Environment Policy

- The OS shall be restricted to a single operator at one time (i.e., concurrent operators are explicitly excluded).
- The applications that make calls to the CM are the single user of the CM, even when the application is serving multiple clients.
- The OS enforces authentication methods to prevent unauthorized access to CM services
- The applications using the module services consist of one or more processes in which each process is utilizing a separate copy of the instance data (no data is shared between instances).
- This module is implemented in FIPS-approved mode only.

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

6. Physical Security

This module is a security Level One software module and offers no specific physical security as none is required.

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

7. Cryptographic Key and CSP Management

This section defines the cryptographic keys and Critical Security Parameters (CSPs) present in the system and how they are managed over their lifetime.

Key/CSP Type	Purpose	Location	Algorithm	Creation/ Input	Lifetime	Destruction
Data Encryption Keys (DEK)	Encryption Key (EK)	Data Encryption Key DB	AES 128/ SHA-256	Generated using SP800-90A DRBG	Permanent in encrypted storage, ephemeral and zeroized after use when in plaintext	Destruction of KEK or record containing Key
Transport Encryption Keys (TEK)	Encryption Key (EK)	Transport Encryption Key DB	AES 128/ SHA-256	Locally generated, or imported via an encrypted file and shared key	Permanent in encrypted storage, ephemeral and zeroized after use when in memory	Destruction of KEK or record containing Key
Data Management Key (DMK)	KEK	Data Management Key DB	AES 128/ SHA-256	Generated using SP800-90A DRBG or Manually input	Permanent in obfuscated plaintext storage, ephemeral and zeroized after use when in memory	Destruction of record containing Key
Transport Management Key (TMK)	KEK	Transport Management Key DB	AES 128/ SHA-256	Generated using SP800-90A DRBG or Manually input	Permanent in obfuscated plaintext storage, ephemeral and zeroized after use when in memory	Destruction of record containing Key

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

Subscriber Key[5] (used for AV generation)	symmetric key	Subscriber Data DB	AES-128/ SHA-256.	Imported via encrypted file and shared key	Permanent in encrypted storage, ephemeral and zeroized after use when in plaintext	Destruction of KEK or record containing Key
SP 800-90A DRBG CSPs (Key and V value)	symmetric keys, and random number generation	RAM for the lifetime of DRBG instance	SP800-90A CTR_DRBG	Derived on use	Ephemeral and zeroized after use	Automatically destroyed after use
entropy input and seed	seeding DRBG	RAM for the lifetime of DRBG instance	N/A	Provided by NDRNG	Ephemeral and zeroized after use	Automatically destroyed after use
HMAC-SHA-1 keys for integrity checking	HMAC-SHA-1 keys	Executable file headers	HMAC-SHA-1	Embedded at file creation	Plaintext	N/A
HMAC-SHA-1 keys for integrity checking	HMAC-SHA-1 keys	Management Keys DB	HMAC-SHA-1	Derived on use	Obfuscated Plaintext	Destruction of record containing Key

Table 7-1: Keys and CSPs

7.1 Deterministic Random Bit Generator (DRBG)

The module uses a hardware source of entropy to seed an approved DRBG. The continuous test is performed on both the seed source and the DRBG (SP800-90A AES-256 Counter (CTR) Mode) output. Additionally, the DRBG performs the health checks specified in section 11.3 of SP 800-90A, including:

- Known Answer Tests
- Instantiate Function Test
- Generate Function Test
- Reseed Function Test

The module uses NDRNG from the operational environment as the source of random numbers to seed the Approved DRBG. The entropy source is outside the logical boundary of the software module but inside the physical boundary of the platform on which the software module is executed. The module provides 256-bits bits of entropy per each request. The NDRNG seeds the CTR_DRBG with 384 bits of entropy input, providing 256-bits of security strength with each request.

[5] The subscriber key is found within the subscriber data file

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

7.2 Key Generation

AES keys are the only keys generated and are created using a SP800-90A compliant AES-256 CTR DRBG approved random number generator per FIPS 140-2 IG 7.8 Approved key generation method.

The module provides a vendor affirmed key generation service for symmetric ciphers (CKG; Vendor Affirmed). The key generation service is compliant with SP800-133 that requires the symmetric key is an XOR of the DRBG output with a value V. In case of the module, the value V is a string of zeros which implies that the key is unmodified from the output of the DRBG. It is not possible for the module to output information during the key generating process.

7.3 Key Entry and Output

Keys may be manually entered into the module in plaintext locally from the console terminal only. Those keys that are manually entered must be entered twice to verify integrity as required in FIPS 140-2 section 4.9.2. If the duplicate keys are not identical, the error message " "ERROR: Keys do not match!" is displayed on the terminal and the command is aborted.

Keys may also be imported via an encrypted file under a shared key. Key unwrapping is provided by the module using AES-ECB using 128-bits allowed by IG D.9. The module does not output keys outside its cryptographic boundary.

7.4 Key storage and Key Zeroization

Persistent keys are always stored in files which are SHA-256 hashed and encrypted using AES in ECB mode (with the exception of the master keys which are stored as obfuscated plaintext). The master keys may be zeroized by using the Destroy commands (please see Table 4-3 for the Destroy commands); this effectively zeroizes all stored keys since the remaining keys are in files which were encrypted under the now zeroized master keys.

Ephemeral keys in memory are zeroized immediately after use.

The individual record containing a key may also be erased.

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

8. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The test platform that runs the Module meets the requirements of 47 CFR FCC PART 15, Subpart B, Class A (Business use).

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

9. Self-Tests

The HPE components designated as part of the cryptographic module performs self-tests compliant with FIPS 140-2 Security Level One as described in section 4.9 of reference [2].

FIPS 140-2 security Level One compliance requires HPE to provide the ability to use power-up tests and conditional tests to validate the HPE HLR CM components present in the Service Provider's environment.

When the Power-on Self-test succeeds, a message" Successfully set the Global status to green." indicating all cryptographic algorithm self-tests have passed. If any instance associated with the CM fails the self-tests, the entire CM will enter the error state and post an error message (e.g., * failed self-test, where * indicates the failed component). Additionally, the Operator may query the module's status using the FIPS Indicator Utility service by typing "getfipsstatus" via the command line which returns "FIPS Status is RED" to indicate the module is in the Error State. The CM will not provide cryptographic services while in the error state. The CM will also post a notice that can be automatically sent to subscribing administrators.

The FIPS Indicator Utility queries the FIPS 140-2 Mode Indicator value, and the Crypto period Expiration Warning Threshold, which is present in the FIPS Info data file.

The FIPS Command Utility interfaces with runtime Cryptographic Module (CM) components to initiate self-tests compliant with FIPS 140-2 Security Level One. It also queries the FIPS Status file to obtain the CM status. CM status provides information as to whether the components within the CM can provide cryptographic services. The utility presents the results of the initiated self-tests and the CM status query to the user.

The FIPS Command Utility Self-Test can act upon a categorical runtime component (e.g., provisioning or call processing) or the cryptographic module as a whole.

9.1 Power-Up Tests

The power-up tests that apply to the HPE HLR Cryptographic Module include the cryptographic algorithm test, the software integrity test, and the critical functions test.

The HPE HLR Cryptographic Module performs cryptographic algorithm Known Answer Tests (KAT) without user interaction to ensure the proper functioning of the encryption algorithms utilized by the HLR CM. The module also allows the Crypto Library User role to perform on-demand self-tests. To perform the on-demand self-tests, the Crypto Library User first invokes the FIPS Command Utility service by typing "fipscmd" followed by "selftest" on the command line. This causes the module to perform the same self-tests which were performed at power-on.

The table shows the known answer tests (KAT) performed at power-up and on-demand:

Algorithm	Test
AES	• AES ECB, encryption/decryption tested separately
SHS	• KAT SHA-1
HMAC	• KAT HMAC-SHA-256
DRBG	• KAT AES-256 CTR_DRBG

Table 9-1 – Self-Tests

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

Integrity verification is performed as part of power up tests.

During build time, the HMAC-SHA-1 value of the keymgrx executable, libCMOD, libcrypt, libOSSL, and libSSLF libraries are calculated and embedded in the cryptographic module. At load time the power-up tests are initiated by the module. The integrity test will compute the HMAC-SHA-1 of the module and compare them to the values generated during build. If the compared values differ, the module enters the error state. Once the module is in error state, all the cryptographic operations are prohibited and the only way to recover from this state is to reboot the module.

The operator can query the status of the module by calling the FIPS Command Utility service by typing “fipscmd” followed by “getfipsstatus” on the command line. The command returns the global FIPS status (e.g., FIPS Status is Green to indicate the module successfully passed the self-tests and is available to perform cryptographic function).

9.2 Conditional Tests

The conditional tests that apply to the HPE HLR Cryptographic Module include the manual key entry test, and the continuous random number generator test.

9.3 Continuous Tests

The standard FIPS 140-2 required continuous test is performed during operation on both the seed source and the approved DRBG.

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

10. Design Assurance

The HPE HLR team adheres to internal coding practices defined for use by the HPE HLR team. The software associated with the HPE HLR Cryptographic Module is isolated into specific software packages. APIs associated with the CM module provide external access to the cryptographic functions associated with the CM. The software in the CM does not share global data between CM module components or CM module components and entities external to the CM.

The software associated with the CM is either of block-structured or object-oriented structure. The software is written in C or C++ and compiled with a C++ compiler.

The structure of the software is hierarchical. The software associated with the CM exists at a specific level (e.g. software package) in the overall software hierarchy. The functions and classes associated with the software perform specific tasks.

Software developed for the HPE HLR Cryptographic Module undergoes unit and independent-level testing.

10.1 Configuration management

HPE uses GitHub to manage the software associated with the HPE HLR Cryptographic Module. GitHub is a leader in collaborative software development and the organization that supports the HPE software management website. GitHub utilizes the Git configuration management tool.

Transmission of data on GitHub is encrypted using SSH, HTTPS (TLS), and git repository content is encrypted at rest. The GitHub limits software accessibility to users given visibility to the data stored on the website. Examples of accessibility range from read-only access to full read and write access with additional access limitations associated with groupings of software.

The configuration management structure of the HPE HLR software, including the CM, involves supporting a main thread of software referred to as a devel and branching from the devel in order to support and manage releases of the HPE HLR software. An HPE HLR configuration management group manages branches associated with software provided for use by HPE customers.

10.2 Guidance

10.2.1 Secure installation

The module is provided with detailed instructions. For complete installation instructions please see companion document: “I-HLR Installation Guide”

10.2.2 Secrets distributions

It is required that the customer will not synchronize the Data and Transport Management Keys files if they intend to operate the HPE HLR in a FIPS 140-2 Security Level One compliant mode. The synchronization of the files, which are protected by obfuscating plain text cryptographic keys, creates a scenario that does not meet FIPS 140-2 Security Level One compliance. Rather the Data and Transport Management Keys must be manually entered at the console of each system.

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

10.2.3 Initialization and start-up

The module is provided with accompanied documentation that provides detailed information for complete installation instructions please see:

“I-HLR Installation Guide”

10.2.4 Operational rules

10.2.4.1 The FIPS Status file must not be edited or modified manually.

10.2.4.2 Disabling Directory Browsing

The HPE HLR/AuC DPA provisioning will ensure that directory browsing is disabled prior to accepting HLR/AuC provisioning requests. See I-HLR Installation Guide for instructions.

10.2.4.3 A firewall should be installed and configured to prevent unauthorized network access.

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

11. Mitigation of Other Attacks

No additional mitigations will be employed.

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

12. Acronyms

AES	Advanced Encryption Standard
API	Application Programming Interface
AuC	Authentication Center
AV	Authentication Vector
CEE	CollabNet Enterprise Edition
CLI	Command Line Interface
CPU	Central Processing Unit
CM	Cryptographic Module
CSP	Critical Security Parameter
CTR	Counter
DB	Database
DPA	Dynamic Provisioning Architecture
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
EK	Encryption Key
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standards
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HLR	Home Location Register
HP	Hewlett Packard
HPE	Hewlett Packard Enterprise
IETF	Internet Engineering Task Force
KAT	Known Answer Test
KEK	Key Encryption Key
Ki	Key Index
NIST	National Institute of Standards and Technology
SCM	Software Configuration Management
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

SIM	Subscriber Identity Module
SP	Security Policy
UMTS	Universal Mobile Telecommunications System
USIM	Universal SIM

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.

13. References

The following references were utilized in preparing this SP.

1. HP, “FIPS 140-2 Security Level One Compliance FRS,” v3.6, March 26, 2010.
2. FIPS 140-2, “Security Requirements for Cryptographic Modules,” May 25, 2001.
3. I-HLR Installation Guide, Release ID: I-HSS 01.08.00, September 8, 2015.
4. HLR Security Administrators Guide, Release I-HSS 01.08.00, August 2015.
5. NIST, “Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,” Initial Release: March 28, 2003, Last Update: December 3, 2019 (link).
6. FIPS 180-4, Secure Hash Standard (SHS), August 2015 (link).
7. FIPS 198-1, The Keyed Hash Message Authentication Code (HMAC), July 2008 (link).
8. NIST Special Publication SP 800-175A, “Guideline for Implementing Cryptography In the Federal Government: Directives Mandates and Policies,” August 2016 (link).
9. NIST Special Publication SP 800-175B Rev. 1, “Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms,” March 2020 (link).
10. NIST Special Publication 800-38A, “Recommendation for Block Cipher Modes of Operation Methods and Techniques”, December 2001 (link).
11. NIST Special Publication 800-57, “Recommendation for Key Management – Part 1: General (Revised),” May 2020 (link).
12. NIST Special Publication 800-90A Rev. 1 – “Recommendation for Random Number Generation Using Deterministic Random Bit Generators”, June 2015 (link).
13. IETF “Keyprov Status Pages” (http://tools.ietf.org/wg/keyprov/)

© 2020 Hewlett Packard Enterprise /atsec information security. This document can be reproduced and distributed only whole and intact, including this copyright notice.