HP OpenCall HLR Cryptographic Module vE10.21
Security Policy

Version 1.0

2010-04-06

Open Call Business Unit

Hewlett-Packard

10810 Farnam Drive

Omaha, Nebraska 68154

TRADEMARKS or SERVICE MARKS

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

HEWLETT PACKARD, HP, OpenCall, OpenCall HLR.

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

COPYRIGHT

Document Control

Below are the publication date, author's initials, and reason for publication for the current and any previous versions of this document.

Version	Publication Date	Author	Reason for Publication
0.1	2009-09-09	nas	Initial Draft
0.3	2010-01-15	Shw	Release draft
0.4	2010-02-02	Shw	Update
0.5	2010-03-04	SHW	Updates
0.6	2010-03-04	SHW	Update
0.7	2010-03-26	SHW	Update from revision
1.0	2010-04-06	SHW	First Release

New and Changed Information

The following table contains brief descriptions of any new or changed information and the number of the affected section.

Section	New/Changed Information

(This page left intentionally blank)

HEWLETT ®
PACKARD
invent

Table of Contents

TRADEMARKS or SERVICE MARKS ii
COPYRIGHT ii

DOCUMENT CONTROL III

NEW AND CHANGED INFORMATION III

1. INTRODUCTION 1

1.1 Audience 1

1.2 Document organization 1

1.3 References 1

1.4 Definitions 2

1.5 Acronyms 2

2. MODULE SPECIFICATION 4

2.1 Description of the Module 4

2.2 Description of the Approved Mode of Operation 4

2.3 Ports and interfaces 6

2.4 Cryptographic module design 6

2.5 Approved cryptographic algorithms 12

2.6 Non-Approved cryptographic algorithms 12

3. ROLES, SERVICES AND AUTHENTICATION 13

3.1 Roles 13

3.2 Services 16

Table 3-3: Module Services 19

3.3 Operator Authentication 19

4. OPERATIONAL ENVIRONMENT 20

4.1 Operational Environment Policy 20

5. PHYSICAL SECURITY 21

6. MITIGATION OF OTHER ATTACKS 22

7. CRYPTOGRAPHIC KEY AND CSP MANAGEMENT 23

7.1 RNG 25

7.2 Key Generation 25

7.3 Key Establishment 26

7.4 Key Entry and Output 26

7.5 Key storage and Key Zeroization 26

8. SELF-TESTS 27

8.1 Power-Up Tests 27

8.2 Conditional Tests 27

8.3 Continuous Tests 27

9. DESIGN ASSURANCE 28

9.1 Configuration management 28

9.2 Guidance 28

9.2.1 Secure installation 28

9.2.2 Secrets distributions 28

9.2.3 Initialization and start-up 29

9.2.4 Operational rules 32

9.2.4.1 The FIPS Status file must not be edited or modified manually 32

9.2.4.2 Disabling Directory Browsing 32

9.2.4.3 A firewall should be installed and configured to prevent unauthorized network access 32

1. Introduction

This document is the FIPS 140-2 security policy for the HP OpenCall HLR cryptographic module to meet FIPS 140-2 level 1 requirements. This Security Policy details the secure operation of the HP OpenCall HLR cryptographic module version E10.21 developed by HEWLETT PACKARD as required in Federal Information Processing Standards Publication 140-2 as published by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce.

The GSM/UMTS functionality supported by the HP OpenCall HLR will possess the ability to run in FIPS mode on an NonStop Itanium or Blade system. The ANSI-41 functionality supported by the HP OpenCall HLR will not have the ability to run in FIPS mode or utilize the newly implemented cryptographic algorithms (e.g. AES-128 ECB).

Note that FIPS mode support is not available on the NonStop S-Series version of the HP OpenCall HLR.

1.1 Audience

This document is required as a part of the FIPS 140-2 validation process. It describes the HP OpenCall HLR cryptographic module in relation to FIPS 140-2 requirements. The companion document HP OpenCall HLR cryptographic module User Guide is a technical reference for service providers using and installing the OpenCall HLR cryptographic module.

1.2 Document organization

This Security Policy document is one part of the FIPS 140-2 Submission Package. This document is the non-proprietary Security Policy. This document outlines the functionality provided by the module and gives high level details on the means by which the module satisfies FIPS 140-2 requirements.

1.3 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. FIPS 186-3, *Digital Signature Standard (DSS)*, June 2009.
4. NIST Special Publication 800-21, *Guideline for Implementing Cryptography In the Federal Government*, December 2005 (link)
5. NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*, Initial Release: March 28, 2003, Last Update: April 01, 2009.
6. NIST 800-57, *Recommendation for Key Management – Part 1: General (Revised)*, March, 2007.

7. atsec, *HP Authentication Center Cryptographic Module FIPS 140-2 Readiness Assessment*, v1.0, 2008-08-27.
8. IETF Keyprov Status Pages (http://tools.ietf.org/wg/keyprov/)

1.4 Definitions

Cover	To encrypt.
Cryptoperiod	The time span during which a specific key is authorized for use by legitimate entities, or the keys for a given system will remain in effect (reference [6]).
Key Encryption KEK (KEK)	A cryptographic key used for the encryption or decryption of other keys (reference [2]).
Master Seed Key	Secret values used for key derivation (reference [6]).

1.5 Acronyms

ADS	Application Database Synchronization
AES	Advanced Encryption Standard
ANSI-41	American National Standards Institute-41
API	Application Programming Interface
AuC	Authentication Center
AV	Authentication Vector
CPU	Central Processing Unit
CM	Cryptographic Module
CSP	Critical Security Parameter
DES	Data Encryption Standard
DPA	Dynamic Provisioning Architecture
DSS	Digital Signature Standard
ECB	Electronic Code Book
EK	Encryption Key
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ERAD	Exception Reporting And Distribution
ESI	Engineering Statement of Intent
FIPS	Federal Information Processing Standards
GCI	Generic Command Line Interface

GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HLR	Home Location Register
HP	Hewlett Packard
IETF	Internet Engineering Task Force
INS	Intelligent Network Server
KAT	Known Answer Test
KEK	Key Encryption Key
MSC	Mobile Switching Center
NIST	National Institute of Standards and Technology
RNG	Random Number Generator
RVU	Release Version Update
SDL	Specification Description Language
SECMON	Security Monitor
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
UMTS	Universal Mobile Telecommunications System
USIM	Universal SIM

2. Module Specification

In this section the module is described and its function as part of the larger product is identified

2.1 Description of the Module

The HP OpenCall 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) and American National Standards Institute no 41 (ANSI-41) standards. The ETSI-based HLR functionality is referred to as Global System for Mobile communications (GSM) and Universal Mobile Telecommunications System (UMTS).

The Authentication Center functionality present in the HP OpenCall HLR ensures that only legitimate subscribers obtain access to the GSM/UMTS or ANSI-41 wireless network.

The HP OpenCall HLR protects sensitive subscriber data elements related to the information required to authenticate subscriber network access. The HP OpenCall HLR Cryptographic Module (CM) provides the cryptography required to protect the sensitive subscriber data elements.

2.2 Description of the Approved Mode of Operation

HP OpenCall HLR CM.customers can operate the HP OpenCall HLR CM in a manner compliant to FIPS 140-2 Security Level One requirements. Note that the GSM/UMTS HLR functionality can operate in a FIPS 140-2 Security Level One compliant manner. The ANSI-41 HLR functionality does not currently have the ability to operate in a manner compliant to FIPS 140-2 Security Level One requirements.

The GSM/UMTS functionality within the HP OpenCall HLR can utilize the CM operating in FIPS 140-2 approved mode. The ANSI-41 functionality within the HP OpenCall HLR can not utilize the CM operating in FIPS 140-2 approved mode.

The HLR/AuC Call Processing component uses subscriber keys (for example, Ki) to generate AVs (Authentication Vectors) for GSM/UMTS subscriber authentication. In FIPS mode, FIPS 140-2 approved cryptographic algorithms are used for Authentication Vector generation. (An authentication vector, 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 HP OpenCall HLR utilizes a subscriber symmetric key (K/Ki) present in both the HLR and the subscriber's user equipment (UE) to generate the authentication vector. The HP OpenCall HLR and a USIM or SIM present in the UE contain the key value).

The HLR/AuC Call Processing component uses the AV Generation API to generate AVs to isolate the exposure of the plaintext authentication key value. The AV Generation API supports the use of AES-128.

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 and algorithm version values that the system uses as the basis for the generation of the new data encryption key.

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

The FIPS Command Utility interfaces with runtime Cryptographic Module components to initiate self-tests compliant with FIPS 140-2 Security Level One; and it queries the FIPS Status file to obtain the CM status. CM status provides information whether the components within the CM can provide cryptographic services and whether all components are in FIPS mode. The utility presents the results of the initiated self-tests and the Cryptographic Module 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.

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).

In FIPS 140-2 approved mode, the system uses FIPS 140-2 approved key generation methods and RNGs. The feature supports a cryptographic key and subscriber key (for example, Ki) zeroization method that is FIPS 140-2 approved.

In FIPS 140-2 approved mode, the HLR, via the Cryptographic Module, only uses FIPS 140-2 compliant cryptographic algorithms (for example, encryption/decryption algorithms, and RNGs) as well as adheres to all other FIPS 140-2 Security Level One requirements

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).

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 2-1 Security Levels

Manufacturer	Model	O/S & Ver.
HP	NB50000C/HP Integrity BL860C	HP Nonstop v J06.08

Table 2-2 Platforms Tested

2.3 Ports and interfaces

Function	Port
Control In	CLI, API
Status Out	CLI, API
Data In	CLI, Disk, API, Network
Data Out	Network, Disk,, API, CLI

Table 2-3 Ports and Interfaces

2.4 Cryptographic module design

This section contains figures that illustrate the HP OpenCall HLR cryptographic module components followed by information containing the details of the components contained in the figures.

The following figure illustrates the HP OpenCall HLR primary cryptographic module components. The figure references key material, key storage, utilities, and runtime components and depicts the relationships between the components.

The lines in the figure show the paths data, statuis or control take between components. The type of information may be determined by color coding of the endpoints (please see table 2-4 below).

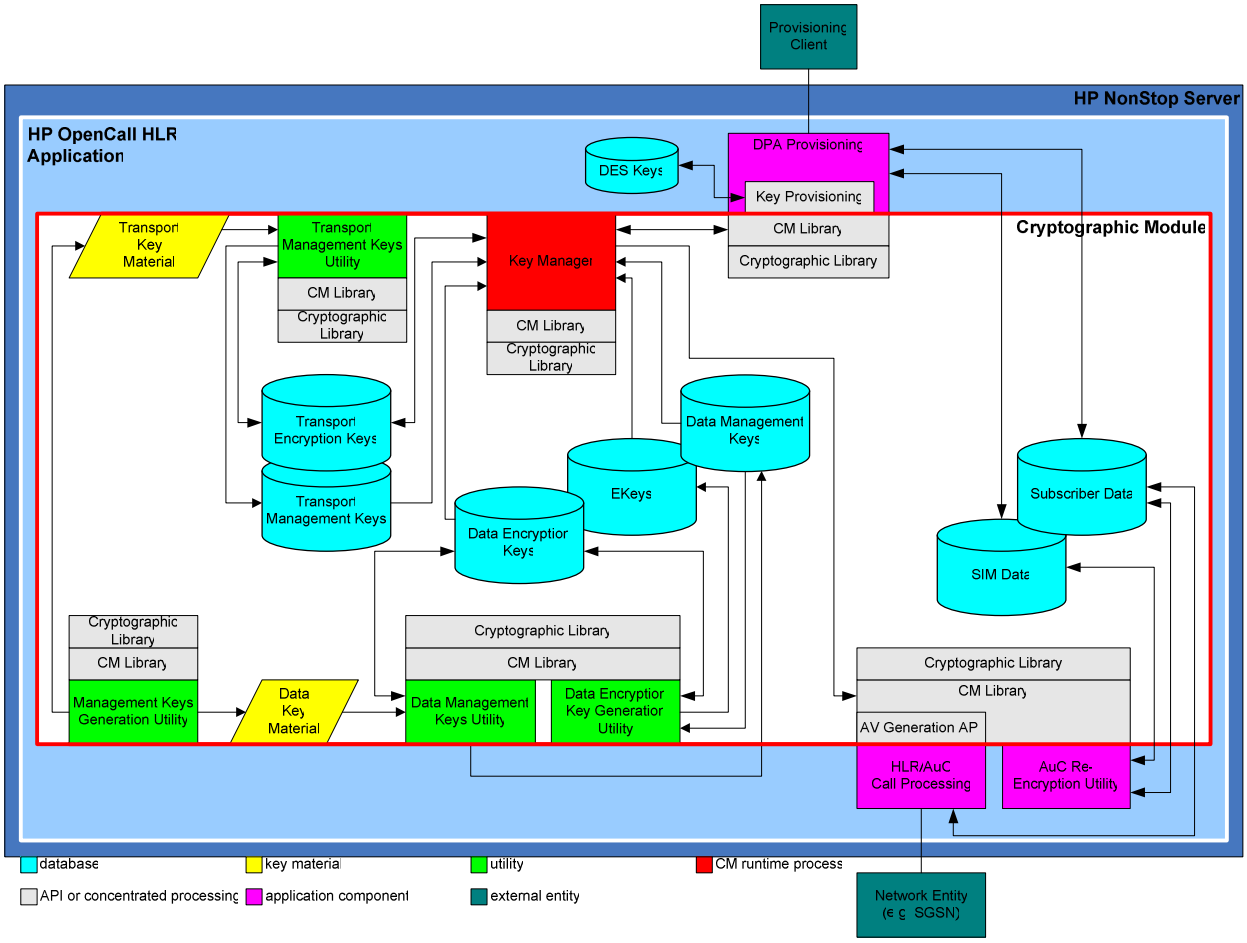

Figure 1: Primary Cryptographic Module Components

The following table provides a brief summary of the components contained within the cryptographic module depicted in the previous figures.

Component	Brief Description
Data Management Keys	A new data file that contains KEKs and Master Seed Keys used to respectively cover and generate cryptographic keys in the Data Encryption Keys data file.
Data Encryption Keys	A new data file that contains cryptographic keys used by application components (e.g. HLR AC Call Processing) to protect sensitive data elements.
Ekeys	A legacy data file that contains cryptographic keys used by application components to protect sensitive data elements.

Transport Management Keys	A new data file that contains KEKs used to cover the cryptographic keys stored in the Transport Encryption Keys data file.
Transport Encryption Keys	A new data file that contains cryptographic keys used to cover sensitive data elements transported over the DPA provisioning stream. The first entry in the Transport Encryption Keys data file contains a cryptographic key used to cover subsequent cryptographic key values during provisioning. All cryptographic key entries that proceed the first entry 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 or EKeys data file.
Data Key Material	A new encrypted file generated by the Management Keys Generation Utility. The CM uses the file to securely install KEKs and Master Seed Keys into the Data Management Keys data file.
Transport Key Material	A new encrypted file generated by the Management Keys Generation Utility. The CM 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.
Data Management Keys Utility	Uses the Data Key Material to install KEKs and Master Seed Keys into the Data Management Keys data file.
Data Encryption Key Generation Utility	Uses the active Master Seed Key from the Data Management Keys data file to generate cryptographic keys for the Data Encryption Keys and EKeys data file. 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 and EKeys data files. Also distributes cryptographic keys, used to cover sensitive data transmitted over the provisioning stream, from the Transport Encryption Keys file.

CM Library	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	Provides the cryptographic algorithms (e.g. AES and SHA) used by the CM.
Key Provisioning	Manages the provisioning of subscriber AuC key values (e.g. K).
AV Generation API	Generates AVs for AuC related network traffic.

Table 2-4: Brief CM Component Description

The next diagram identifies the cryptographic module components that use the FIPS Info file to determine whether the HLR must operate in FIPS mode.

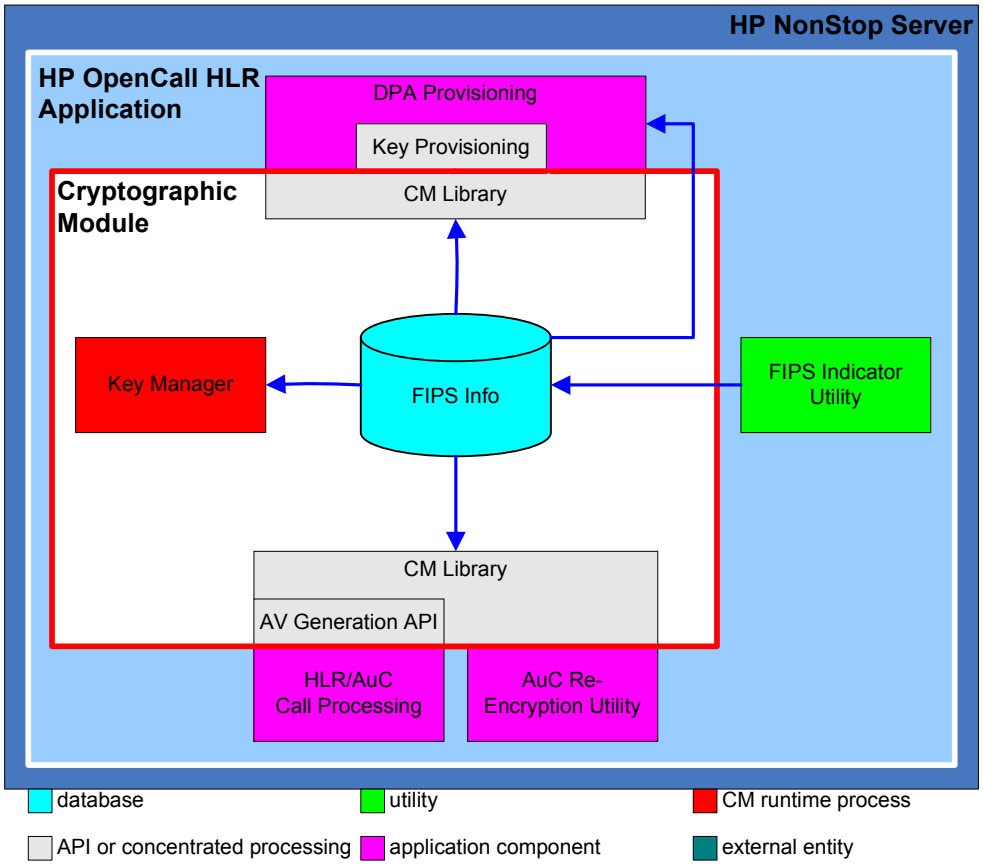

Figure 2: Cryptographic Module FIPS Mode Indicator Access

The following table provides a brief summary of the components contained within or associated with the cryptographic module-related components depicted in Figure 2 above

Component	Brief Description
FIPS Info	A new data file that contains static FIPS information such as the indicator that determines whether the system must run in FIPS mode.
FIPS Indicator Utility	Maintains and queries the content of the FIPS Info data file.

Table 2-5: Indicator Component Description

The next diagram illustrates the relationship of the CM-related components in regard to managing the availability or state of the CM. The components contained within the following figure will determine whether the CM will continue to provide cryptographic services or a component failed a self-test causing the CM to cease cryptographic operations and enter an error or unavailable state.

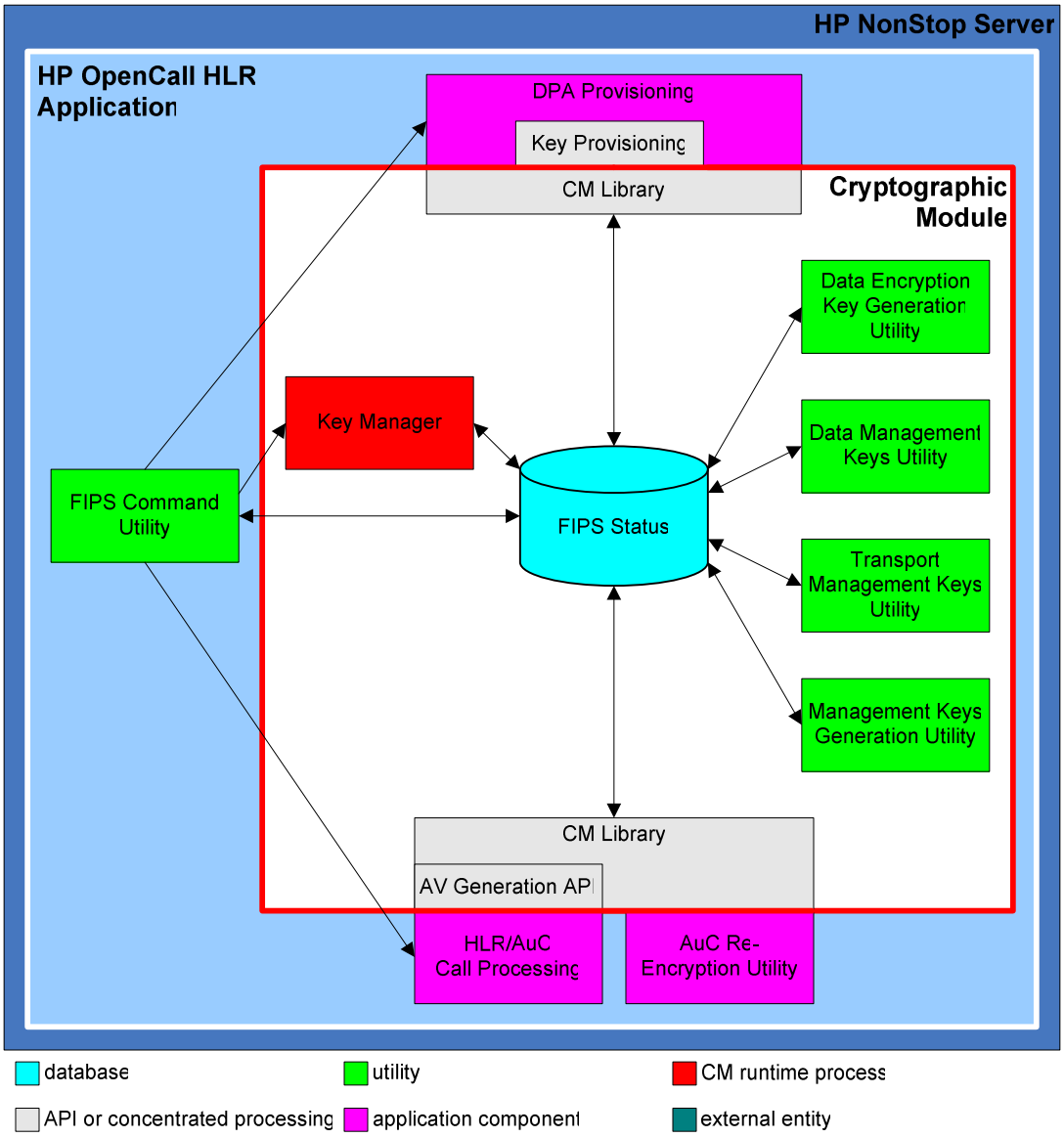

Figure 3: Cryptographic Module FIPS Mode Status and Command Utility

The following table provides a brief summary of the components contained within or associated with the cryptographic module depicted in Figure 3. Subsequent subsections within this section provider greater detail of the components.

Component	Brief Description
FIPS Status	A new data file that contains runtime FIPS status information and helps in determining whether the components within the CM can provide cryptographic services.
FIPS Command Utility	Interfaces with the runtime CM components in order to initiate Self-Tests and queries the FIPS Status file to determine and obtain CM status. The utility will present the results of the initiated Self-Tests and the CM status query to the user. The utility can act upon a single CM runtime component or the CM as a whole.

Table 2-6: Brief Component Description

2.5 Approved cryptographic algorithms

- AES 128 ECB mode (cert #1308)
- SHA 1 byte mode (cert #1196)
- SHA 256 byte mode (cert #1196)
- HMAC-SHA-1 (cert #760)
- Random Number Generation (ANSI X9.31 AES 128) (cert #730)

2.6 Non-Approved cryptographic algorithms

- HP Proprietary Algorithm – decryption only for recovery of legacy data

3. Roles, Services and Authentication

3.1 Roles

This section contains a table that identifies the Cryptographic Module components and the CM roles that have access to or run the components.

#	Role	Description
1	Crypto Officer	The Crypto Officer role possesses the ability to install and update the CM components. Note that the Crypto Officer role can not run any of the CM components.
2	FIPS Mode Manager	The FIPS Mode Manager role possesses the ability to use the FIPS Indicator Utility to alter and query the CM FIPS Mode indicator in the FIPS Info file.
3	Management Key Generation	The Management Key Generation role possesses 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.
5	Transport Management Key Installation	The Transport Management Key Installation role possesses 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.
6	Data Encryption Key Generation	The Data Encryption Key Generation role possesses 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.
7	CM Operator	The CM Operator role possesses the ability to run the Key Manager and Transport Key Manager runtime processes.
8	Crypto Library User	The Crypto Library User role possess the ability to use the libraries associated with the CM.
9	Data Synchronization	The Data Synchronization role possesses the ability to synchronize the CM Data Encryption Keys and Transport Encryption Keys files.

Table 3-1: Cryptographic Module Roles

The following table illustrates the capabilities of each role in regard to each CM 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 3-1

Component/Role #	1	2	3	4	5	6	7	8	9
FIPS Info File	PCRW	RW	R	R	R	R	R	R	
FIPS Status File	PCRW	R	RW	RW	RW	RW	RW	RW	
Data Management Keys	PCRW			RW		R	R		
Data Encryption Keys	PCRW			RW		RW	R		RW
EKeys	PCRW					RW	R		RW
Transport Management Keys	PCRW				RW		R		
Transport Encryption Keys	PCRW				RW		RW		RW
Subscriber Data	PCRW							RW	RW
SIM Data	PCRW							RW	RW
Data Key Material			WC	RPC					
Transport Key Material			WC		RPC				
FIPS Indicator Utility	PCRW	E							
Management Keys Generation Utility	PCRW		E						

Component/Role #	1	2	3	4	5	6	7	8	9
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	
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 3-2: Cryptographic Module Privileges by Role

3.2 Services

Service	Function	Role (Numbers from Table 3-2 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 128 RNG Seed Key	AES, SHA-256, ANSI X9.31 RNG	CI, DI, SO
DEKADD	Add a key to the Data Encryption Key DB	6	AES 128 Key	AES, SHA-256	CI, SO
DEKREENCRYPT	Re-encrypt the keys in the Data Encryption Key DB	4	AES 128 Key	AES, SHA-256	DO, DI, CI, SO
TEKREENCRYPT	Re-encrypt the keys in the Transfer Encryption Key DB	5	AES 128 Key	AES, SHA-256	DO, DI, CI, SO
DEKREPORT	Reports the keys in the Data Encryption Key database	6	N/A	N/A	DO, CI, SO
DMKACTIVATE	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 Management Key DB	4	AES 128 Key	AES, SHA-256	CI, DI, SO
DMKDEACTIVATE	Deactivate a key (or keys) in	4	N/A	N/A	CI, SO

Service	Function	Role (Numbers from Table 3-2 Cryptographic Module Roles)	CSPs	Algorithm	Service Ports I-In, O-Out C- Command D-Data S-Status
	the Data Management Key DB				
DMKREPORT	Reports the keys in the Data Management Key database	4	N/A	N/A	DO, CI, SO
EKEYSREPORT	Reports the keys in the EKEYs database	6	HP Proprietary Keys (read/decrypt use only)	HP Proprietary Algorithm	DO, CI, SO
TEKADD	Add a key to the Transport Encryption Key DB	5, 7	AES 128 Key	N/A	CI, SO
TEKREPORT	Reports the keys in the Transport Encryption Key database	5	N/A	N/A	DO, CI, SO
TMKACTIVATE	Activate a key (or keys) in the Transport Management Key DB	5	N/A	N/A	CI, SO
TMKADD	Add a key to the Transport Management Key DB	5	AES 128 Key	N/A	DI, CI, SO
TMKDEACTIVATE	Deactivate a key (or keys) in the Transport Management Key DB	5	N/A	N/A	CI, SO
TMKREPORT	Reports the	5	N/A	N/A	DO, CI, SO

Service	Function	Role (Numbers from Table 3-2 Cryptographic Module Roles)	CSPs	Algorithm	Service Ports I-In, O-Out C- Command D-Data S-Status
	keys in the Transport Management Key database				
CM APIs	Encrypt and decrypt data (via key index)	Crypto_LIB_USER (8)	AES 128 Key	AES, SHA-256	DI, DO, SO
FIPS Command Utility	Initiate Self Tests, Start and Stop Module	Crypto_LIB_USER (8)	N/A	AES, SHA-1, HMAC-SHA-1, SHA-256, AES based X9.31 RNG (for self tests)	CI, SO
Set up and Configure Module	Install module, create files and roles	CRYPTO_OFFICER (1)	N/A	N/A	CI, SO
FIPS Indicator Utility	Get Indicator, Set FIPS Status	FIPS_MODE_MGR[1], CRYPTO_OFFICER, All roles	N/A	N/A	CI, SO
DEKZeroize	Zeroize all keys in the Data Encryption Keys DB	Data Encryption Key Generation	AES 128 Keys	N/A	CI, SO
DMKZeroize	Zeroize all keys in the Data	Data Management Key	AES 128 Keys	N/A	CI, SO

[1] All roles can query the status but only the FIPS Mode Manager can alter the FIPS Mode Indicator value.

Service	Function	Role (Numbers from Table 3-2 Cryptographic Module Roles)	CSPs	Algorithm	Service Ports I-In, O-Out C- Command D-Data S-Status
	Management Key DB	Installation			
TMKZeroize	Zeroize all keys in the Transfer Management Key DB	Transport Management Key Installation	AES 128 Keys	N/A	CI, SO
EKeysZeroize	Zeroize all keys in the EKeys DB	Data Encryption Key Generation	HP Proprietary Keys	HP Proprietary Algorithm	CI, SO
TEKZeroize	Zeroize all keys in the TEK DB	Transport Management Key Installation	AES 128 Keys	N/A	CI, SO

Table 3-3: Module Services

3.3 Operator Authentication

Operator authentication is implicit by assumption of the role. The Operating System controls access to the system. The SAFECOM utility is used to associate user IDs with Cryptographic Module roles.

4. Operational Environment

This module will operate in a modifiable operational environment per the FIPS 140-2 specifications.

4.1 Operational Environment Policy

- The operating system shall be restricted to a single operator at one time (i.e., concurrent operators are explicitly excluded).
- The applications that make calls to the cryptographic module are the single user of the cryptographic module, even when the application is serving multiple clients.
- The Operating System enforces authentication methods to prevent unauthorized access to Module 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 implements both approved and non-approved services, the non-approved services (an HP proprietary algorithm) are only used for decryption only to recover legacy data which is then re-encrypted using an approved algorithm

5. Physical Security

This module is a security level 1 software module and offers no specific physical security as none is required.

6. Mitigation of Other Attacks

No additional mitigations will be employed.

7. Cryptographic key and CSP management

This section defines the cryptographic keys and 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	EK	Data 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 plaintext	Zeroization of KEK or record containing Key
Transport Encryption Keys	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	Zeroization of KEK or record containing Key
Data Management Key	KEK	Data Management Key DB	AES 128/SHA - 256	Manually input	Permanent in obfuscated plaintext storage, ephemeral and zeroized after use when in memory	Zeroization of record containing Key
Transport Management	KEK	Transport Management	AES 128/SHA -	Manually input	Permanent in	Zeroization of record

Key/CSP Type	Purpose	Location	Algorithm	Creation/input	Lifetime	Destruction
Key		Key DB	256		obfuscated plaintext storage, ephemeral and zeroized after use when in memory	containing Key
Data Management Master Seed Key	DRNG Seed	Data Management Key DB	AES 128/SHA - 256 for integrity and AES 128 (for use in ANSI X9.31 AES 128 based DRNG)	Manually input	Permanent in obfuscated plaintext storage, ephemeral and zeroized after use when in plaintext	Zeroization of KEK or record containing Key
HP Proprietary Keys (EKeys)	EK (Read and Decrypt Only, uses Data Management KEK)	EKeys DB	HP Proprietary Algorithm	Imported via encrypted file and shared key	Permanent in encrypted storage, ephemeral and zeroized after use when in plaintext	Zeroization of KEK or record containing Key
SIM Data	CSP	SIM Data DB	AES 128/SHA - 256 or HP Proprietary Algorithm, at first use, a record encrypted under the proprietary algorithm is re-encrypted	Imported via encrypted file and shared key	Permanent in encrypted storage, ephemeral and zeroized after use when in plaintext	Zeroization of KEK or record containing Key

Key/CSP Type	Purpose	Location	Algorithm	Creation/input	Lifetime	Destruction
			under AES 128/SHA-256.			
Subscriber Data (used for AV generation)	CSP	Subscriber Data DB	AES 128/SHA - 256 or HP Proprietary Algorithm, at first use, a record encrypted under the proprietary algorithm is re-encrypted under AES 128/SHA-256.	Imported via encrypted file and shared key	Permanent in encrypted storage, ephemeral and zeroized after use when in plaintext	Zeroization of KEK or record containing Key
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	Zeroization of record containing Key

Table 7-1: Keys and CSPs

7.1 RNG

The cryptographic module will use a hardware source of entropy to seed an approved DRNG. The continuous test will be performed on both the seed source and the DRNG (ANSI X9.31 AES 128) output.

7.2 Key Generation

AES keys are the only keys generated and are created using an approved random number generator per FIPS 140-2 section 4.7.2.

7.3 Key Establishment

Key Establishment is not supported

7.4 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

Keys may also be imported via an encrypted file under a shared key.

7.5 Key storage and Key Zeroization

Persistent keys are always stored in files which are SHA -256 hashed and encrypted (with the exception of the master keys which are stored as obfuscated plaintext). The master keys may be zeroized by using the Zeroize commands (please see table 3-3 for the Zeroize 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.

8. Self-Tests

The HP OpenCall components designated as part of the Cryptographic Module will perform 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 HP to provide the ability to use power-up tests and conditional tests to validate the HP OpenCall HLR Cryptographic Module components present in the Service Provider's environment.

If any instance associated with the CM module fails the self-tests, the entire CM will enter an error state and post an error message via the FIPS Indicator Utility indicating that the CM is an error state. The CM module will not provide cryptographic services while in an error state. The module will also post a notice that can be automatically sent to subscribing administrators when any critical event occurs.

8.1 Power-Up Tests

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

The HP OpenCall HLR Cryptographic Modules will perform cryptographic algorithm Known Answer Tests (KAT) to ensure the proper functioning of the encryption algorithms utilized by the HLR Cryptographic Module.

The software/firmware integrity test involves delivering the Cryptographic Module executable files (e.g. Key Manager) with digital signatures (HMAC-SHA-1) embedded in the header of each executable file.

Integrity verification is performed as part of power up tests..

8.2 Conditional Tests

The conditional tests that apply to the HP OpenCall HLR Cryptographic Module include the software/firmware load test, the manual key entry test, and the continuous random number generator test.

Note that part of the implementation of this feature will involve an effort to determine any differences between the software/firmware load test specified as part of the conditional test and the software/firmware integrity test included as part of the power-up tests.

8.3 Continuous Tests

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

9. Design Assurance

The HP OpenCall HLR team adheres to internal coding practices defined for use by the HP OpenCall HLR team. The software associated with the HP OpenCall HLR CM 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 cryptographic module 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 HP OpenCall HLR CM module undergoes unit and independent-level testing.

9.1 Configuration management

HP uses CollabNet to manage the software associated with the HP OpenCall Home Location Register (HLR) Cryptographic Module (CM). CollabNet is a leader in collaborative software development and the organization that supports the HP software management website. CollabNet utilizes the CollabNet CollabNet Enterprise Edition (CEE) software, which in turn utilizes the Subversion SCM tool.

The CollabNet hosted solution encrypts all data stored on the external configuration management website. The encryption occurs on the database level and restricts data access to the CEE interface. The CEE 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 HP OpenCall HLR software, including the CM, involves supporting a main thread of software referred to as a trunk and branching from the trunk in order to support and manage releases of the HP OpenCall HLR software. An HP OpenCall HLR configuration management group manages branches associated with software provided for use by HP customers.

9.2 Guidance

9.2.1 Secure installation

For complete installation instructions please see: *E10.21 OpenCall HLR Rollup Install Guide*

9.2.2 Secrets distributions

It is required that the customer will not synchronize the Data and Transport Management Keys files if they intend to operate the HP OpenCall 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.

9.2.3 Initialization and start-up

The following procedure describes how to turn on FIPS mode.

Perform the following steps using the TACL prompt:

1.Log on as node.mgr

2.Run toolrun.opcon

3.Select your node from the list

4.ads

5.stopall

Perform the following steps using the OSH prompt:

6.Disable directory browsing on the iTP Webserver by doing the following:

a.cd /usr/tandem/webserver/conf

b.vi httpd.config

c.DirectoryIndex:

1.Search for DirectoryIndex in the Region/DirectoryIndex directive.

2.Comment out (insert a # character before) the DirectoryIndex

d.save and exit (:wq)

e.su super.super

f../stop

g../start

Perform the following steps using the TACL prompt:

7.Use SAFECOM to add users and assign those users the roles the customer wants based on the information in the HLR Security Administrators Guide. A template exists in roles.rolesx. The following steps load that file:

a.Log on as super.super

b.Add specific system users

c.Edit the roles template, adding the users to specific roles

d.Run bin.cmd

e.Discover SGAPICmds

f.Loadxml roles.rolesx

8.Log on as “FIPS Mode Manager” role

9.Run macs.fipsind

a.setfipsindicator true

b.exit

10.Log on as “CM Operator” role

11.Run cmodrun.keymonr

The following two steps provide an example of how to perform the setup of encryption keys. For more information on the following commands, see the HLR Security Administrators Guide.

12.Set up Data Encryption keys as follows:

a.Log on as “Management Key Generation” role

b.Run macs.cmkeycli

c.CREATEKEY –kt dmkek_dmmsk –start <start time> -expire <end time> -a aes128 –o <filename>

d.Capture the key value from the CREATEKEY command (refer to it as KEY1).

e.Exit

f.Log on as “Data Management Key Installation” role

g.Run macs.cmkeycli

h.DMKADD –f <filename> -kmk <KEY1>

i.Exit

j.Log on as “Data Encryption Key Generation” role

k.Run macs.cmkeycli

l.DEKADD

m.Exit

13.Set up Transport Encryption keys. The key configured in the following steps will be the default transport encryption key in the first entry of the Transport Encryption Keys data file.

a.Log on as “Management Key Generation” role.

b.Run macs.cmkeycli

c.CREATEKEY –kt tmkek_tek –start <start time> -expire <end time> -a aes128 –o <filename> -k2 <clear value of the Transport Encryption Key> -k2ic < clear value of the Transport Encryption Key >

d.Capture the key value from the CREATEKEY command (refer to it as KEY2).

e.Exit

f.Log on as “Transport Management Key Installation” role.

g.Run macs.cmkeycli

h.TMKADD –f <filename> -kmk <KEY2>

i.Exit

14.Log on as node.mgr

15.Run toolrun.opcon

16.Select your node.

17.startall

18.ads

Perform the following steps using the OSH prompt:

19.Change the password encryption policy to CM by doing the following:

a.cd /usr/tandem/webserver/root/<node>/etc

b.vi Master.Config

c.Search for PasswordEncryptionPolicy

d.Change it to CM

e.Save and exit (:wq)

For complete instructions on operating the module in FIPS 140-2 approved mode, please see: ***Feature Implementation Guide: FIPS 140-2 Security Level One Compliance***

9.2.4 Operational rules

9.2.4.1 The FIPS Status file must not be edited or modified manually

9.2.4.2 Disabling Directory Browsing

The HP HLR/AuC DPA provisioning will ensure that directory browsing is disabled prior to accepting HLR/AuC provisioning requests. See step 6 in section 9.2.3 above for instructions.

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