LG Kernel Loadable Cryptographic Module
FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Version: 5.0
Date: February 3, 2017

CHANGE RECORD

Revision	Date	Author	Description of Change
1	June 3rd, 2016	Gossamer	Updated security policy based on new algorithm certificates
2	September 28th, 2016	Gossamer	Updated security policy
3	October 26th, 2016	Gossamer	Updated security policy
4	January 20th, 2017	Gossamer	Updated security policy
5	February 3rd, 2017	Gossamer	Minor updates

1. Module Description

This document is the non-proprietary security policy for the LG Kernel Cryptographic Module, hereafter referred to as the module.

The module is a loadable kernel module that executes within an Android operating system's kernel space. The module provides a C-language application program interface (API) for use by user and kernel applications that require cryptographic functionality. Since LG compiles the module to utilize either the ARMv8 Crypto Extension (CE) or ARMv7 NEON instruction set to accelerate cryptography, FIPS 140-2 classifies the module as a software-hybrid module, multi-chip standalone module embodiment. The physical cryptographic boundary is the physical perimeter of the general-purpose computer (GPC) or mobile device on which the module executes. Qualcomm manufactures the Snapdragon processors contained within the mobile devices (used during validation) using standard production-grade material. The mobile devices have ports and interfaces comparable to that of a GPC. The logical cryptographic boundary of the module encompasses the LG loadable kernel module (lgecrypto_module.ko, version 1.0) and the Qualcomm ARM CPU CE & NEON instructions.

The module performs no communications other than with the calling application (the process that invokes the module services).

The FIPS 140-2 security levels for the module are as follows:

Table 1: Module Security Level Specification

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	1
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Overall, the module has security level 1. It has been tested in the following mobile device configurations:

Table 2: Platform Configurations

Kernel Version	Platform	Operating System	Qualcomm Processor
3.18	LG G5 Model VS987	Android 6.0.1	Qualcomm Snapdragon 820 (64-bit with CE)
3.10	LG V10 Model VS990	Android 6.0.1	Qualcomm Snapdragon 808 (64-bit with CE)
3.10	LG Vista2 Model LG-H740	Android 6.0.1	Qualcomm Snapdragon 617 (32-bit with CE)
3.10	LG Vista2 Model LG-H740	Android 6.0.1	Qualcomm Snapdragon 617 (32-bit with NEON)

Below are images of the devices:

Figure 1 - LG G5

Figure 2 - LG V10

Figure 3 - LG Vista 2

2. Cryptographic Module Boundary

2.1. Software Block Diagram

The figure below illustrates the relationship of the module to the kernel and GPC.

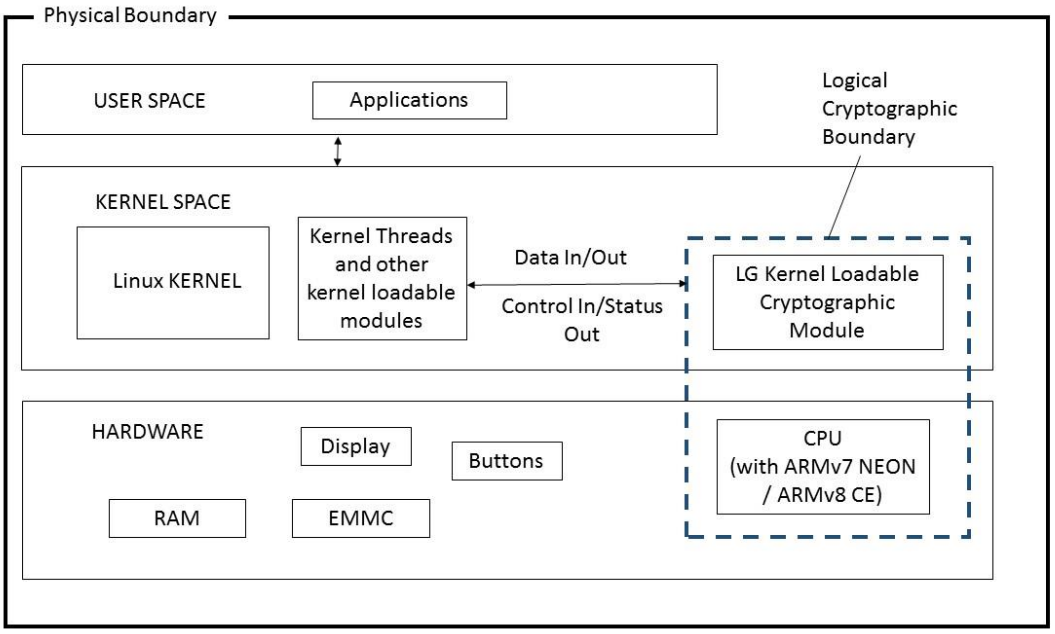

Figure 4: Software Block Diagram

3. Ports and Interfaces

The physical ports of the module are the same as the computer system on which it is executing. The logical interface is a C-language application program interface (API).

Table 3: Ports and Interfaces

Logical Interface Type	Description
Control Input	API entry point and corresponding stack parameters.
Data Input	API entry point's data input stack parameters.
Status Output	API entry point return values and status stack parameters.
Data Output	API entry point's data output stack parameters.

As a software-hybrid module, control of the mobile device's physical ports is outside the module's scope. However, when the module is performing self-tests, or is in an error state, all output on the

logical data output interface is inhibited. The module is single- threaded and in error scenarios returns only an error value (no data output is returned).

4. Modes of Operation and Cryptographic Functionality

The module only supports an Approved mode of operation. Only FIPS Approved and tested algorithms are used.

The module provides the following approved algorithms:

Table 4: Approved Algorithms for Approved Mode of Operation

Function	Algorithm	Options	Certificates
Random Number Generation	800-90A DRBG	AES-CTR (128/192/256), Hash (SHA-1, 256, 384, 512), HMAC (SHA-1, 256, 384, 512)	#1166, #1167 and #1168
Encryption, Decryption	Triple-DES	3-key ECB, CBC, and CTR	#2178, #2179 and #2180
	AES	128/192/256-bit keys for ECB, CBC, CTR; 128/256-bit keys for XTS[1]	#3973, #3974 and #3975
Message Digest	SHA	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	#3278, #3279 and #3280
Keyed Hash	HMAC	HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	#2591, #2592 and #2593

The module also uses the following non-Approved but Allowed algorithm:

- NDRNG

The NDRNG is the processor's Non-Deterministic Random Number Generator, which is the module's entropy source. The NDRNG produces 256 bits of entropy per call.

The module must be loaded into memory in order to operate. As a part of the mobile devices' boot process, the mobile device module loads the module and during the loading process the module automatically begins to perform the required power-up self-tests. Any failure of the self-tests causes the module to print a message (or series of messages) to log and enter the FIPS error state. When the module is in the FIPS error state, it is unusable via any interface.

The module is a cryptographic loadable kernel module that LG distributes as part of an overall phone image specific to a model of phone.

[1] AES-XTS is only allowed for storage applications. The module also meets FIPS 140-2 Implementation Guidance A.9 by checking that the two concatenated keys comprising the AES-XTS key do not equal each other.

4.1. Critical Security Parameters

All CSPs used by the module are described in this section. All access to these CSPs by module services are described in Section 4. The CSP names are generic, corresponding to API parameter data structures.

Table 5: Critical Security Parameters and Descriptions

CSP Name	Description
AES EDK	AES (128 / 192 / 256) encrypt / decrypt key (EDK)
TDES EDK	Triple-DES (3-Key) encrypt / decrypt key (EDK)
HMAC Key	Keyed hash key (160 / 224 / 256 / 384 / 512)
AES-CTR DRBG V Value	Secret internal state value
AES-CTR DRBG Key Value	Secret internal state value
HMAC DRBG Key Value	Secret internal state value
HMAC DRBG V Value	Secret internal state value
HASH DRBG V Value	Secret internal state value
HASH DRBG C Value	Secret internal state value
DRBG entropy input	Random data from entropy source for the DRBG
DRBG seed	Input that determines the initial DRBG state

The module does not output intermediate key generation values.

For all CSPs:

Storage RAM, associated to entities by memory location. The module uses CSPs passed in by the calling application on the stack. The module does not store any CSP persistently (beyond the lifetime of an API call).

Generation CSPs are provided externally via API. The module implements SP 800-90A compliant RNG services. It is the responsibility of the calling application to utilize an Approved RNG for the creation of the symmetric keys as shown in the table of CSPs above. The calling application is responsible for storage of generated keys returned by the module. A minimum of 256 bits of entropy must be provided.

Entry All CSPs enter the module's logical boundary in plaintext as API parameters, associated by memory location. However, none cross the physical boundary.

Output The module does not output CSPs, other than as explicit results of key generation services. However, none cross the physical boundary.

Destruction Zeroization of sensitive data is performed automatically by API function calls for temporarily stored CSPs. The calling application is responsible for parameters passed in and out of the module. Module power off is also a valid means of zeroizing all keys and CSPs.

The module makes a call to /dev/random to gather entropy and seeds to generate keys. The keys, entropy input and seeds are destroyed when released by the appropriate API function calls. Keys residing in internally allocated data structures (during the lifetime of an API call) can only be accessed using the module defined API. The operating system protects memory and process space from unauthorized access. All API functions are executed by the invoking calling application in a non-overlapping sequence such that no two API functions will execute concurrently. An application operating on behalf of an authorized Crypto-Officer or User has access to all key data used during the operation of the module.

5. Roles, Authentication, and Services

The module meets all FIPS 140-2 level 1 requirements for Roles and Services. The Module does not allow concurrent operators.

Both roles have access to all of the services provided by the module.

- User Role (User): Access to user space usage
- Crypto Officer Role (CO): Access to kernel space usage

All services implemented by the module are listed below, along with a description of service CSP access.

Table 6: Roles and Services

Service	Role	Description
Initialize	User, CO	Module initialization. Does not access CSPs.
Self-Test	User, CO	Perform self-tests. Does not access CSPs.
Show Status	User, CO	Functions that provide module status information (FIPS Setting) do not access CSPs.
Zeroize	User, CO	All services automatically overwrite CSPs stored in allocated memory. Stack cleanup is the responsibility of the calling application.

Key Generation	User, CO	Used to generate keys for encryption / decryption. Executes using random number seeds, passed in by the calling process. Has access to all CSPs.
Random Number Generation	User, CO	Generates random numbers used in key generation. Executes using AES EDK, HMAC Key, AES-CTR DRBG V Value, AES-CTR DRBG Key Value, HMAC DRBG Key Value, HMAC DRBG V Value, HASH DRBG V Value, HASH DRBG C Value, DRBG entropy input, and the DRBG seed
Symmetric Encrypt / Decrypt	User, CO	Used to encrypt or decrypt data. Executes using AES EDK, TDES EDK, passed in by the calling process.
Message Digest	User, CO	Used to generate a SHA-1 or SHA2 message digest. Does not access CSPs.
Keyed Hash	User, CO	Used to generate or verify data integrity with HMAC. Executes using HMAC key provided by calling process.
Utility	User, CO	Miscellaneous helper functions that do not access CSPs.
Crypto Extension (CE) and NEON Instruction Sets	User, CO	Additional CPU instructions in ARM processors that allow acceleration of cryptographic functions. Information for both instruction sets are found in Reference [2] and [3].

6. Self-Tests

The module performs the self-tests listed below at boot time during the module's loading process. The module performs its software integrity check after performing its algorithm self-tests; if the binary kernel module image has been modified, the integrity check fails. This is described in more detail below. If any self-test or integrity test fails, the module enters an error state and becomes nonfunctional. The operator can re-run all power-up self-tests by power cycling the GPC/device, thereby causing reloading of the module and automatically reinitiating all self-tests. The kernel loadable module executes self-tests without operator intervention.

The mobile device sets a kernel proc file to indicate when the device has the module loaded and whether the module is in an error state.

[2] http://infocenter.arm.com/help/topic/com.arm.doc.dui0801f/DUI0801F_armasm_user_guide.pdf
[3] http://infocenter.arm.com/help/topic/com.arm.doc.den0024a/DEN0024A_v8_architecture_PG.pdf

The process file `/proc/sys/crypto/fips_enabled` serves as a flag to indicate whether the device has loaded the module, and the process file `/proc/sys/crypto/fips_error` serves as a flag to indicate whether the module is in the error state. The possible combinations of these flags have the following meanings:

Table 7: Combination Legend

fips_enabled	fips_error	Meaning
0	0	Device is not configured to use the LG Kernel Loadable Cryptographic Module
0	1	Impossible Combination
1	0	Device is using the LG Kernel Loadable Cryptographic Module (all tests passed)
1	1	Device attempted to use the LG Kernel Loadable Cryptographic Module (module is in FIPS error state)

The self-test process is completely automatic and occurs during loading of the kernel module; the commands to load the kernel module are embedded into the signed mobile device system image supplied by LG Electronics, and the image is not modifiable by the user of the mobile device.

Table 8: Self-Tests

Algorithm	Type	Test Attributes
Software Integrity	KAT	HMAC-SHA-256
SHS	KAT	One KAT each for SHA1, SHA224, SHA256, SHA384 and SHA512.
HMAC	KAT	One KAT each for SHA1, SHA224, SHA256, SHA384 and SHA512.
AES	KAT	Separate encrypt and decrypt, ECB/CBC/CTR/XTS modes, 128/192/256 bit key lengths.
Triple-DES	KAT	Separate encrypt and decrypt, CBC/CTR/ECB modes, 3-Key.
SP 800-90A DRBG	KATs	CTR_DRBG (128-bit AES key), HASH_DRBG (SHA-256), and HMAC_DRBG (HMAC-SHA256)

SP 800-90A DRBG	Conditional	Continuous RNG tests to each of CTR_DRBG (128-bit AES key), HASH_DRBG (SHA-256), and HMAC_DRBG (HMAC-SHA256)
Non-Approved RNG	Conditional	Continuous RNG test for the entropy source

6.1. Integrity Check Details

At build time, an HMAC-SHA-256 is calculated on the LG Kernel Loadable Cryptographic Module and stored along with the kernel module itself. This HMAC-SHA-256, as a 64-character hexadecimal string, is read from a file during module load time and used as the integrity expected value.

At load time, the module loads the expected HMAC-SHA-256 checksum. After all the algorithm self-tests are complete, the kernel integrity test routine does the following:

1. Calculate the HMAC checksum over the kernel module's file image.
2. Compare the resulting HMAC to the HMAC read from the HMAC file.
3. If the calculated and command line values do not match, enter the error state.

7. Security Rules

The user does not need to take any special action. The module is designed to always operate in a FIPS-compliant manner.

8. Operational Environment

The FIPS 140-2 module covers the static kernel binary that executes from within the kernel space of the GPC. The module operates only in a single-operator mode.

9. Mitigation of Other Attacks

The module is not designed to mitigate against attacks that are outside the scope of FIPS 140-2.