LG Framework Cryptographic Module

Non-Proprietary FIPS 140-2 Security Policy

Document Version: 1.0.7   Date: June 15, 2016

LG

|galois|

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the LG Framework Cryptographic Module, hereafter denoted the Module. The Module is a software only cryptographic library and is defined as a multi-chip standalone embodiment per FIPS 140-2. The Module meets FIPS 140-2 overall Level 1 requirements. The SW version is 1.0.0.

Table 1 – Cryptographic Module Configurations

Operational Environments			
CPU Family	**OS**	**JDK**	**Platforms**
Qualcomm Snapdragon 800 Series (32-bit and 64-bit)	Android 5.0.1	Android Runtime 5.0.1	LG G3 (Model VS985) LG G Flex 2 (Model LGLS996)

The Module is intended for use by US Federal agencies and other markets that require a FIPS 140-2 validated Cryptographic Library. The Module is a multi-chip standalone, software-only embodiment; the cryptographic boundary is the Java Archive (JAR) file, *bc-fips.jar*.

The FIPS 140-2 security levels for the Module are given in Table 2 as follows:

Table 2 – Security Level of Security Requirements

Security Requirement	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	1

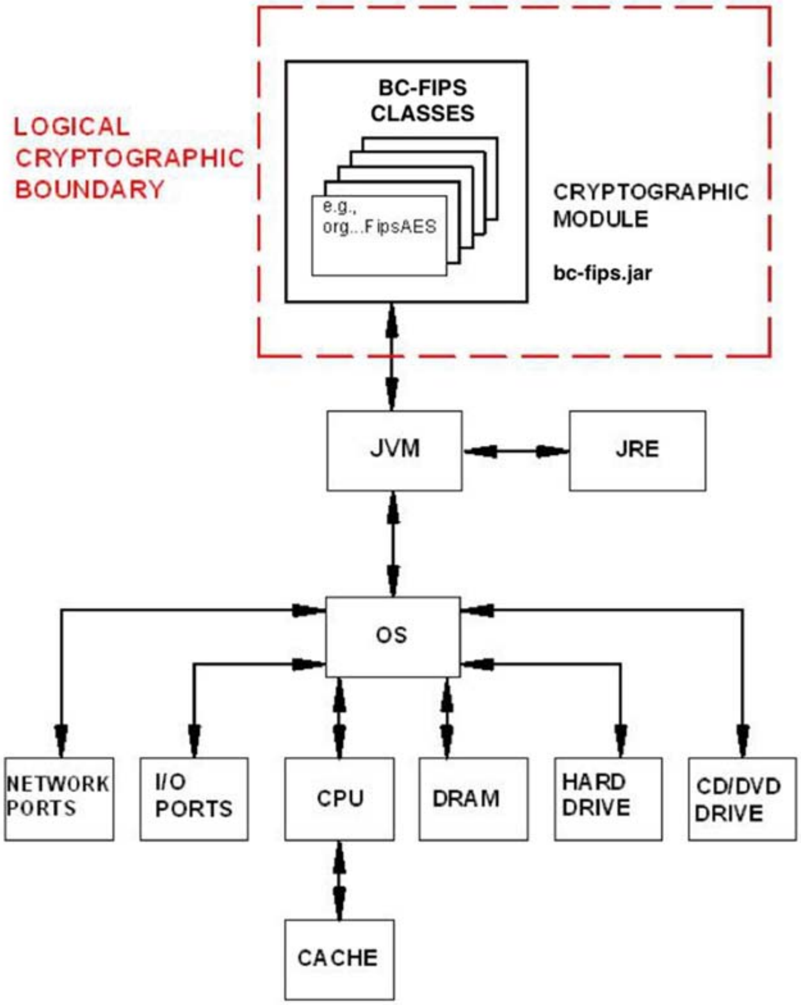
1.1 Logical and Physical Cryptographic Boundaries

1.1.1 Logical Cryptographic Boundary

The executable for the Module is*: bc-fips.jar*. This module is the only software component within the Logical Cryptographic Boundary and the only software component that carries out cryptographic functions covered by FIPS 140-2. Figure 1 shows the logical relationship of the cryptographic module to the other software and hardware components of the computer. The BC classes are executed on the Android Runtime, the interface to the Operating System (OS) that is the interface to the various physical components of the computer.

The physical components of the computer are discussed further in Section 1.1.2. Abbreviations introduced in Figure 1 that describe physical components are: Central Processing Unit (CPU), Dynamic Random Access Memory (DRAM) and Input Output (I/O).

Figure 1 – Block Diagram of the Software.



1.1.2 Physical Boundary and Ports and Interfaces

The Module runs on a General Purpose Computer (GPC). The Physical Cryptographic Boundary for the module is the case of that GPC. All the physical components are standard electronic components; there are not any custom integrated circuits or components dedicated to FIPS 140-2 related functions.

For FIPS 140-2 purposes, the Module is defined as a “multi-chip standalone module”, therefore, the module’s physical ports or interfaces are defined as those for the hardware of the GPC. These physical ports are separated into the logical interfaces defined by FIPS 140-2.

The Module is a software only module, and, therefore, control of the physical ports is outside of the module’s scope. The physical ports of the module are provided by the general purpose computer on which the module is installed. The logical interfaces are defined as the API of the cryptographic module. The module’s API supports the following logical interfaces: data input, data output, control input, and status output.

1.2 Modes of Operation

The module supports both an Approved mode and non-Approved mode of operation. During operation, the module can switch service by service between an Approved mode of operation and a non-Approved mode of operation. The module will transition to the non-Approved mode of operation when one of the non-Approved security functions listed below Table 5 is utilized in lieu of an Approved one. The module can transition back to the Approved mode of operation by utilizing an Approved security function.

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in Table 3 and Table 4 below.

Table 3 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB, CBC, OFB, CFB8, CFB128, CTR Key sizes: 128, 192, 256 bits	3289
DRBG	[SP 800-90A] Functions: Hash DRBG, HMAC DRBG, CTR DRBG (AES-128/192/256) Security Strengths:128, 192, and 256 bits	748
DSA	[FIPS 186-4] Functions: Key Pair Generation, Signature Generation, Signature Verification Key sizes: 1024 (Verification Only), 2048, 3072 bits	943
HMAC	[FIPS 198-1] Functions: Generation, Authentication SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	2087
RSA	[FIPS 186-4, ANSI X9.31-1998 and PKCS #1 v2.1 (PSS and PKCS1.5)] Functions: Key Pair Generation, Signature Generation, Signature Verification Key sizes: 1024 (Verification only), 2048, 3072 bits	1683
SHA	[FIPS 180-4] Functions: Hashing SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	2728
Triple-DES	[SP 800-20] Functions: Encryption, Decryption Modes: TECB, TCBC, TCFB8, TCFB64, TOFB Key sizes: 3-key	1874

Table 4 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
Non-SP 800-56A Compliant DH	[IG D.8] Per IG D.8, Scenario 6 – non-Approved (not Compliant with SP 800-56A) Primitive only, a partial DH Key agreement scheme is allowed in an Approved FIPS Mode of operation. No Keys are established Into the module using DH. BouncyCastle implements all parameter variations (p,g) for DH, including (but not limited to) those listed in RFCs 2409, 3526, 4306, 5114, and 5996. Bit sizes from 2048 bits to 8192 bits are allowed in the Approved mode (provides between 112 and 192 bits of strength).
Non-SP 800-56A Compliant ECDH	[IG D.8] Per IG D.8, Scenario 6 – non-Approved (not Compliant with SP 800-56A) Primitive only, a partial ECDH Key agreement scheme is allowed in an Approved FIPS Mode of operation. No Keys are established Into the module using ECDH. BouncyCastle implements ECDH abstracted over the underlying curve and domain parameters. These parameters can be supplied from either NIST Approved or alternative sources, and represent a wide variety of key sizes. Sizes from 224 to 571 bits (based on the underlying curve) are allowed in the Approved mode (provides between 112 and 256 bits of strength).
Non-SP 800-56B Compliant RSA Key Transport	[IG D.9] RSA May be used by a calling application as part of a key encapsulation scheme. No Keys are established into the module using RSA. Key sizes: 2048 and 3072 bits (provides 112 or 128 bits of strength)

Non-Approved (not tested, non-compliant) Cryptographic Functions (not allowed in Approved Mode):

- AES-CBC Ciphertext Stealing (CS)
- ANSI X9.31 RNG*
- CMAC
- DH partial key agreement using bit sizes less than 2048 (minimum supported is 768 bits)
- Dual EC DRBG*
- CTR-DRBG-Triple-DES*
- DSA 1024 SigGen
- ECDH partial key agreement using key sizes less than 224 bits (based on the underlying curve)
- ECDSA
- GCM
- GMAC
- RSA 1024 SigGen
- TLS-KDF**
- Triple-DES (2-key)

* Keys generated by the non-compliant RNG or DRBG functions are not allowed for use in the Approved mode.

**Keys derived using the TLS-KDF are not allowed for use in the Approved mode.

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

Table 5 – Critical Security Parameters (CSPs)

CSP	Description / Usage
AES Encryption Key	[FIPS-197] AES (128/192/256) encrypt key
AES Decryption Key	[FIPS-197] AES (128/192/256) decrypt key
DRBG State	CTR DRBG (AES): V (128 bits) and AES key (128/192/256) Hash DRBG: V (440/888 bits) and C (440/888 bits) HMAC DRBG: V (160/224/256/384/512 bits) and Key (160/224/256/384/512 bits)
Entropy Input to DRBG	Entropy input (length dependent on security strength)
DSA Signing Key	[FIPS 186-4] DSA (2048/3072) signature generation key
HMAC Authentication Key	[FIPS 198-1] Keyed-Hash key (SHA-1, SHA-2). Key size determined by security strength required
RSA Signing Key	[FIPS 186-4] RSA (2048 and 3072) signature generation key
RSA Key Transport Key	RSA (2048 and 3072) key transport (decryption) key
Triple-DES Encryption Key	[SP 800-67] Triple-DES 168 encryption key
Triple-DES Decryption Key	[SP 800-67] Triple-DES 168 decryption key
DH Private Component	Used to generate the agreed-upon key.
ECDH Private Component	Used to generate the agreed-upon key.

2.2 Public Keys

Table 6– Public Keys

CSP	Description / Usage
DH Agreement Key	Diffie-Hellman (>= 2048) public key agreement key
ECDH Agreement Key	EC Diffie-Hellman (>= 224) public key agreement key
DSA Verification Key	[FIPS 186-4] DSA (1024, 2048, 3072) signature verification key
RSA Key Transport Key	RSA (2048, 3072) key transport (encryption) key.
RSA Verification Key	[FIPS 186-4] RSA (1024, 2048, 3072) signature verification key

3 Roles and Services

3.1 Assumption of Roles

The module supports two distinct operator roles, User and Cryptographic Officer (CO). The cryptographic module implicitly maps the two roles to the services.

Table 7 lists all operator roles supported by the Module. The Module does not support a maintenance role or bypass capability. The Module does not support concurrent operators. The Module does not support authentication.

Table 7 – Roles Description

Role ID	Role Description	Authentication Type
CO	Cryptographic Officer – Initializes the module	N/A – Authentication not required for Level 1
User	User – The user of the complete API.	N/A – Authentication not required for Level 1

3.2 Services

All services implemented by the Module are listed in Table 8 and Table 9 below. Each service description also describes all usage of CSPs by the service.

Table 8 lists the authorized services. The second column provides a description of each service and availability to the Cryptographic Officer and User, in columns 3 and 4, respectively. Note that the same set of services is available in the non-Approved mode of operation. The only difference is that non-Approved security functions listed in Section 2 above can be used in Lieu of the Approved security functions found in Table 4 and 5.

Table 8 – Authorized Services

Service	Description	CO	U
Initialize Module and Run Self-Tests on Demand	The Android Runtime will call the static constructor for self-tests on module initialization.	X	
Show Status	A user can call *FipsStatus.IsReady()* at any time to determine the if the module is ready; a value of "true" states that the system is operating normally, and "false" indicates an error has occurred.		X
Zeroize / Power-off	The module uses the JVM garbage collector on thread termination.		X
Data Encryption	Used to encrypt data.		X
Data Decryption	Used to decrypt data.		X
Signature Authentication	Used to generate signatures (DSA, RSA).		X
Signature Verification	Used to verify digital signatures.		X
DRBG (SP800-90A) output	Used for random number and IV generation.		X
Key Agreement	Used for generating a fresh key with a third party.		X
Key Transport	Used for transporting a key between hosts.		X
Message Hashing	Used to generate a SHA-1 or SHA-2 message digest.		X
Keyed Message Hashing	Used to calculate data integrity codes with HMAC.		X

Service	Description	CO	U
NDRNG Callback	Gathers entropy in a passive manner from a user-provided function. The minimum number of bits provided during DRBG initialization is 256 bits. This is based on the default length of the entropy argument provided to the DRBG. This value can be specified by the User. The minimum number of bits provided shall not be lower than 112 bits.		X

Table 9 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The module generates the CSP.
- R = Read: The module reads the CSP. The read access is typically performed before the uses the CSP.
- E = Execute: The module executes using the CSP.
- W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, when the module generates a CSP, or when the module overwrites an existing CSP.
- Z = Zeroize: The module zeroizes the CSP.

Table 9 – CSP Access Rights within Services

Service	CSPs									
	AES Encryption/ Decryption Keys	DH Private Component	ECDH Private Component	DRBG State	Entropy Input to DRBG	DSA Signing Key	HMAC Authentication Key	RSA Signing Key	RSA Key Transport Key	Triple-DES Encryption/ Decryption Keys
Initialize Module and Run Self-Tests on Demand										
Show Status										
Zeroize / Power-off	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Data Encryption	R									R
Data Decryption	R									R
Signature Authentication						R	R	R		
Signature Verification						R	R	R		
DRBG (SP800-90A) output				R	R					
Message Hashing										
Keyed Message Hashing							R			
Key Agreement		R	R							
Key Transport								R	R	
NDRNG Callback				R						

4 Self-tests

Each time the Module is powered up, it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power-up self–tests are available on demand by power cycling the Module.

On power-up or reset, the Module performs the self-tests that are described in Table 10 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs or conditional tests fails, the Module enters the Self-Test Failure error state. The module will output an error message when *FipsStatus.isReady()* is called.

Table 10 – Power Up Self-tests

Test Target	Description
Software Integrity	HMAC-SHA256
AES	KATs: Encryption, Decryption Modes: ECB Key sizes: 256 bits
DRBG	KATs: HASH_DRBG, HMAC_DRBG, CTR_DRBG Security Strengths: 256 bits
DSA	KAT: Signature Generation, Signature Verification Key sizes: 2048 bits
HMAC	KATs: Generation, Verification SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (includes SHA KATs)
RSA	KATs: Signature Generation, Signature Verification Key sizes: 2048 bits
Triple-DES	KATs: Encryption, Decryption Modes: TECB Key sizes: 3-key

Table 11 – Conditional Self-tests

Test Target	Description
DRBG	DRBG Continuous Test performed when a random value is requested from the DRBG.
DSA	DSA Pairwise Consistency Test performed on every DSA key pair generation.
ANSI X9.31 RNG	Continuous Test performed when a random value is requested from the RNG.
RSA	RSA Pairwise Consistency Test performed on every RSA key pair generation.
DRBG Health Checks	Performed conditionally per SP 800-90A Section 11.3. Required per IG C.1.

5 Physical Security Policy

The module is a software-only module and does not have physical security mechanisms.

6 Operational Environment

The Module is as a modifiable operational environment under the FIPS 140-2 definitions.

The Module runs on a GPC running the operating system specified in the approved operational environment list. The operating system manages processes and threads in a logically separated manner. The Module's user is considered the calling application that instantiates the Module within the process space of the Java Virtual Machine.

7 Mitigation of Other Attacks Policy

The Module implements SPA/DPA (Simple Power Analysis/Differential Power Analysis) protection to prevent the leaking of RSA keys and message digest keys through electromagnetic leakage from the underlying hardware. The two counter-measures used are: Constant Time Comparisons, which protect the digest and integrity algorithms, and Numeric Blinding, which both protect the RSA algorithm.

8 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The Module shall provide two distinct operator roles: User and Cryptographic Officer.
2. The Module does not provide authentication.
3. The operator shall be capable of commanding the Module to perform the power up self-tests by cycling power or resetting the Module.
4. Power up self-tests do not require any operator action.
5. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
6. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
8. The Module does not support concurrent operators.
9. The Module does not have any external input/output devices used for entry/output of data.
10. The Module does not enter or output plaintext CSPs from the module's physical boundary.
11. The Module does not output intermediate key values.
12. AES-CBC Ciphertext stealing (CS), ANSI X9.31 RNG, CMAC, DH partial key agreement using bit sizes less than 2048, Dual EC DRBG, CTR-DRBG-Triple-DES, DSA 1024 SigGen, ECDH partial key agreement using key sizes less than 224 bits, ECDS, GCM, GMAC, RSA 1024 SigGen, TLS KDF, and Triple-DES (2-key) are not allowed for use in the FIPS Approved mode of operation. When these algorithms are used, the module is no longer operating in the FIPS Approved mode of operation. It is the responsibility of the consuming application to zeroize all keys and CSPs prior to and after utilizing these non-Approved algorithms. CSPs shall not be shared between the Approved and non-Approved modes of operation.

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 12 – References

Abbreviation	Full Specification Name
ANSI X9.31	*X9.31-1998, Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), September 9, 1998*
FIPS 140-2	*Security Requirements for Cryptographic modules, May 25, 2001*
FIPS 180-4	*Secure Hash Standard (SHS)*
FIPS 186-4	*Digital Signature Standard (DSS)*
FIPS 197	*Advanced Encryption Standard*
FIPS 198-1	*The Keyed-Hash Message Authentication Code (HMAC)*
IG	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
PKCS#1 v2.1	*RSA Cryptography Standard*
SP 800-20	*Modes of Operation Validation System for Triple Data Encryption Algorithm (TMOVS)*
SP 800-38A	*Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode*
SP 800-38F	*Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*
SP 800-56A	*Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*
SP 800-90A	*Recommendation for Random Number Generation Using Deterministic Random Bit Generators*

Table 13 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
BC	Bouncy Castle
BC-FJA	Bouncy Castle FIPS Java API
CBC	Cipher-Block Chaining
CDH	Computational Diffie-Hellman
CFB	Cipher Feedback Mode
CMAC	Cipher-based Message Authentication Code
CMVP	Crypto Module Validation Program
CO	Cryptographic Officer

Acronym	Definition
CPU	Central Processing Unit
CS	Ciphertext Stealing
CSP	Critical Security Parameter
CTR	Counter-mode
DES	Data Encryption Standard
DH	Diffie-Hellman
DRAM	Dynamic Random Access Memory
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Authority
EC	Elliptic Curve
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDSA	Ecliptic Curve Digital Signature Authority
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standards
GPC	General Purpose Computer
HMAC	key-Hashed Message Authentication Code
IG	See References
JAR	Java ARchive
JDK	Java Development Kit
JRE	Java Runtime Environment
JVM	Java Virtual Machine
IV	Initialization Vector
KAS	Key Agreement Scheme
KAT	Known Answer Test
KDF	Key Derivation Function
KW	Key Wrap
MAC	Message Authentication Code
N/A	Non Applicable
NDRNG	Non Deterministic Random Number Generator
OFB	Output Feedback
OS	Operating System
PKCS	Public Key Cryptography Standards
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm

Acronym	Definition
TCBC	TDEA Cipher-Block Chaining
TCFB	TDEA Cipher Feedback Mode
TDEA	Triple Data Encryption Algorithm
Triple-DES	Triple Data Encryption Standard
TECB	TDEA Electronic Codebook
TOFB	TDEA Output Feedback
TLS	Transport Layer Security
USB	Universal Serial Bus