Xperia Cryptographic Module

FIPS 140-2 Non-Proprietary Security Policy

Document Version 1.0.2

Table of Contents

1. Module Overview

This document is the non-proprietary FIPS 140-2 security policy for the Xperia Cryptographic Module.

Xperia Cryptographic Module ('the Module') is a software library providing a C language application program interface (API) for use by other processes that require cryptographic functionality. The Module is classified by FIPS 140-2 as a software module, multi-chip standalone module. The logical cryptographic boundary of the Module is the fipscanister object module, a single object module file named fipscanister.o. The Module performs no communications other than with the calling application (the process that invokes the Module services).

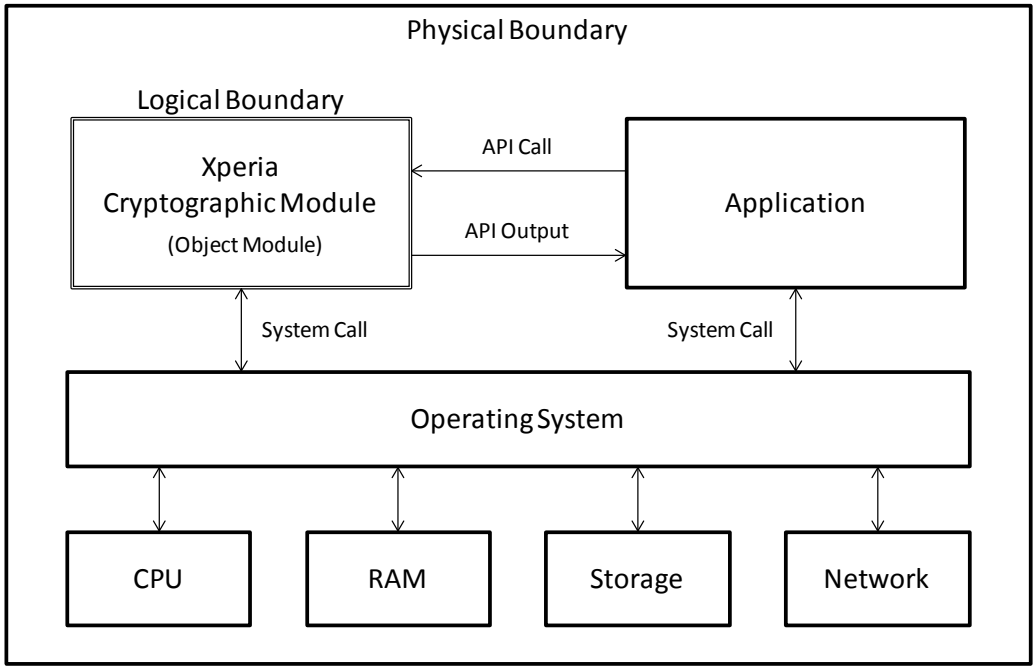

Figure 1 – Module Block Diagram

This document is written about the following validated software version of Xperia Cryptographic Module:

- Software version: 1.0.0

2. Security Level

The FIPS 140-2 security levels for Xperia Cryptographic Module are as follows:

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services and Authentication	2
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	3
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

3. Modes of Operation

Xperia Cryptographic Module is designed to support both a FIPS approved mode of operation and a Non-FIPS approved mode of operation.

3.1. Approved Mode of Operation

Xperia Cryptographic Module supports the following FIPS approved cryptographic algorithms:

Table 2 – Approved Algorithms

Algorithm		Options	Implement*	Certs. #
AES	FIPS 197	128/192/256 ECB, CBC, CFB1/8/128, OFB, CTR, XTS, CMAC Generation/Verification, CCM, GCM Note: AES XTS is approved only for use in storage applications.	C/ARM8-CI	#3329
CMAC	SP 800-38B			
CCM	SP 800-38C			
GCM	SP 800-38D			
XTS	SP 800-38E			
Triple-DES	SP 800-67	3-Key Triple-DES TECB, TCBC, TCFB, TOFB CMAC Generation/Verification	C	#1900
DRBG	SP 800-90A	Hash DRBG, HMAC DRBG, (no reseed), CTR DRBG (AES 128/192/256, derivation function, no derivation function)	C/ARM8-CI	#774
SHS	FIPS 180-4	SHA-1, SHA-2(SHA-224, SHA-256, SHA-384, SHA-512)	C/ARM8-CI	#2762
HMAC	FIPS 198-1	SHA-1, SHA-2(SHA-224, SHA-256, SHA-384, SHA-512)	C/ARM8-CI	#2120

RSA	FIPS 186-2	SigVer9.31: (1024/1536/2048/3072/4096 with SHA-1/SHA-256/SHA-384/SHA-512), SigVerPKCS1.5 (1024/1536/2048/3072/4096 with all hash sizes), SigVerPSS (1024/1536/2048/3072/4096 with all hash sizes)	C/ARM8-CI	#1709
	FIPS 186-4	SigGen9.31 (2048/3072 with SHA-256/SHA-384/SHA-512), SigGenPKCS1.5 (2048/3072 with all SHA-2) SigGen PSS (2048/3072 with all SHA-2)	C/ARM8-CI	
DSA	FIPS 186-4	PQG Gen (2048/3072 with all SHA-2 sizes) PQG Ver (1024/2048/3072 with SHA-1 and all SHA-2 sizes) Key Pair Gen (2048/3072 with SHA-224/256) Sig Gen (2048/3072 with all SHA-2 sizes) Sig Ver (1024/2048/3072 with SHA-1 and all SHA-2 sizes)	C/ARM8-CI	#946
ECDSA	FIPS 186-4	PKG: CURVES(P-224/P-256/P-384/P-521/K-233/ K-283/K-409/K-571/B-233/B-283/B-409/B-571) PKV: CURVES(P-192/P-224/P-256/P-384/P-521/ K-163/K-233/K-283/K-409/K-571/B-163/B-233/ B-283/B-409/B-571) SigGen (all SHA-2 sizes), SigVer (SHA-1 and all SHA-2 sizes)	C/ARM8-CI	#658
ECC CDH	SP 800-56A	All NIST defined B, K and P curves except sizes 163 and 192	C/ARM8-CI	#485

*C: C Language / ARM8-CI: ARM8 Cryptographic Instructions

In addition to the above algorithms the Module employs the following Allowed non-FIPS approved cryptographic algorithms for use in the FIPS approved mode of operation.

- EC DH Key Agreement (Key agreement methodology provides between 112 and 256 bits of security strength)
- RSA Key Wrapping (Key transport methodology provides between 112 and 256 bits of security strength.

As a software only cryptographic engine, the module implements EC DH and RSA key transport primitives. However, these are not used by the module to establish keys within the module.

The Module is a cryptographic engine library, which can be used only in conjunction with additional software. Aside from the use of the NIST defined elliptic curves as trusted third party domain parameters, all other FIPS 186-4 assurances are outside the scope of the Module, and are the responsibility of the calling process.

3.2. Non-Approved Mode

The Xperia Cryptographic Module supports the following cryptographic algorithms which are Non-Approved per the SP800-131A transition:

Table 3 – Non-Approved Algorithms

Algorithm		Options
DRBG (non-compliant)	SP 800-90A	Dual EC DRBG
RNG	ANSI X9.31	AES 128/192/ 256
RSA (non-compliant)	FIPS 186-2	GenKey9.31, SigGen9.31, SigGenPKCS1.5, SigGenPSS (1024/1536 with all hash sizes, 2048/3072/4096 with SHA-1)
DSA (non-compliant)	FIPS 186-2	PQG Gen, Key Pair Gen, Sig Gen (1024 with all hash sizes, 2048/3072 with SHA-1)
	FIPS 186-4	PQG Gen, Key Pair Gen, Sig Gen (1024 with all hash sizes, 2048/3072 with SHA-1)
ECDSA (non-compliant)	FIPS 186-2	PKG: CURVES(P-192 K-163 B-163) SigGen: CURVES(P-192/P-224/P-256/P-384/P-521/K-163/K-233/ K-283/K-409/K-571/B-163/B-233/B-283/B-409/B-571)

	FIPS 186-4	PKG: CURVES(P-192 K-163 B-163) SigGen: CURVES(P-192: (SHA-1, 224, 256, 384, 512)/P-224:(SHA-1) /P-256:(SHA-1) /P-384: (SHA-1) /P-521:(SHA-1)/K-163: (SHA-1, 224,256, 384, 512)/K-233:(SHA-1)/K-283:(SHA-1)/ K-409:(SHA-1)/K-571:(SHA-1)/B-163: (SHA-1, 224, 256, 384, 512)/ B-233:(SHA-1)/B-283: (SHA-1)/B-409:(SHA-1)/B-571:(SHA-1)
ECC CDH (non-compliant)	SP 800-56A	B, K and P curves sizes 163 and 192

The module must be loaded into memory and the FIPS_module_mode_set() function called in order for an operator to successfully authenticate. Once in an operational state, 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 above non-Approved security functions 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. Security Rules #7 and #8 in Section 9 below must also be followed while in the Approved mode.

4. Ports and Interfaces

The physical ports of Xperia Cryptographic Module are the same as the device on which it is executing. The logical interface is a C-language application program interface (API):

- Data Input - API entry point data input stack parameters
- Data Output - API entry point data output stack parameters
- Status Output - API entry point return values and status stack parameters
- Control Input - API entry point and corresponding stack parameters

As a software module, control of the physical ports is outside module 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).

5. Identification and Authentication Policy

5.1. Assumption of Roles

Xperia Cryptographic Module supports two distinct operator roles: User role and Crypto-Officer (C.O.) role. Only one role may be active at a time and the Module does not allow concurrent operators. The User or C.O. role is assumed by passing the appropriate password to the FIPS_module_mode_set() function. The password values may be specified at build time and must have a minimum length of 16 characters. Any attempt to authenticate with an invalid password will result in an immediate and permanent failure condition rendering the Module unable to enter the FIPS mode of operation, even with subsequent use of a correct password.

Authentication data is loaded into the Module during the Module build process, performed by the Crypto Officer, and otherwise cannot be accessed.

Table 4 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Role-based authentication	Authentication Secret Verification
Crypto-Officer	Role-based authentication	Authentication Secret Verification

5.2. Authentication Mechanism

The Xperia Cryptographic Module supports an authentication mechanism.

Table 5 - Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Authentication Secret Verification	The minimum password length that the Module accepts is 16 characters, the probability of a random successful authentication attempt in one try is a maximum of $1/256^{16}$, which is less than $1/10^{6}$. The Module permanently disables further authentication attempts after a single failure, so this probability is independent of time.

6. Access Control Policy

6.1. Roles and Services

Both Crypto-Officer (C.O.) role and User role have access to all of the services provided by the Module.

- User Role: Loading the Module and calling any of the API functions.
- C.O. Role: Installation of the Module on the host computer system and calling of any API functions.

Table 6 - Crypto-Officer and User Common Services

Service	Description
Initialization	Module initialization.
Self-Test	Perform self tests (FIPS_selftest).
Show Status	Functions that provide module status information: • Version (as unsigned long or const char *) • FIPS Mode (Boolean)
Zeroization	Functions that destroy CSPs: • fips_drbg_uninstantiate: for a given DRBG context, overwrites DRBG CSPs (Hash_DRBG CSPs, HMAC_DRBG CSPs, CTR_DRBG CSPs.)
Random Number generation	Used for random number and symmetric key generation. • Seed or reseed DRBG instance • Determine security strength of DRBG instance • Obtain random data
Asymmetric Key generation	Used to generate DSA, ECDSA and RSA keys. There is one supported entropy strength for each mechanism and algorithm type, the maximum specified in SP800-90A
Symmetric encrypt/decrypt	Used to encrypt or decrypt data. Keys are passed in by the calling process.
Symmetric digest	Used to generate or verify data integrity with CMAC. CMAC Key is passed in by the calling process.
Message digest	Used to generate a SHA-1 or SHA-2 message digest.

Service	Description
Keyed Hash	Used to generate or verify data integrity with HMAC. HMAC Key is passed in by the calling process.
Key transport	Used to encrypt or decrypt a key value on behalf of the calling process (does not establish keys into the Module). RSA Encryption and Decryption Keys are passed in by the calling process.
Key agreement	Used to perform key agreement primitives on behalf of the calling process (does not establish keys into the Module). EC DH Private Key and EC DH Public Key are passed in by the calling process.
Digital signature	Used to generate or verify RSA, DSA or ECDSA digital signatures. Keys are passed in by the calling process.
Utility	Miscellaneous helper functions.

Table 7 – Non-Approved Services

Service	Description
Random Number generation	Used for random number and symmetric key generation using Dual EC DRBG. • Seed or reseed DRBG instance • Determine security strength of DRBG instance • Obtain random data
Asymmetric Key generation	Used to generate DSA, ECDSA and RSA keys using FIPS 186-2 key generation mechanisms listed in Table 3 above. There is one supported entropy strength for each mechanism and algorithm type, the maximum specified in SP800-90A
Key transport	Used to encrypt or decrypt a key value on behalf of the calling process (does not establish keys into the Module). RSA Encryption and Decryption Keys are passed in by the calling process.
Key agreement	Used to perform key agreement primitives on behalf of the calling process (does not establish keys into the Module) using curves defined Table 3 above. EC DH Private Key and EC DH Public Key are passed in by the calling process.
Digital signature	Used to generate or verify RSA, DSA or ECDSA digital signatures using key sizes, digest sizes or curves from Table 3 above. Keys are passed in by the calling process.
Utility	Miscellaneous helper functions.

6.2. Definition of Critical Security Parameters (CSPs)

The following CSPs are included in the Xperia Cryptographic Module.

- AES Key - AES (128/192/256) encrypt / decrypt key
- AES CMAC Key - AES (128/192/256) CMAC generate / verify key
- AES GCM Key - AES (128/192/256) encrypt / decrypt / generate / verify key

- AES XTS Key - AES (128/256) XTS encrypt / decrypt key
- Triple-DES Key - Triple-DES (3-Key) encrypt / decrypt key
- Triple-DES CMAC Key - Triple-DES (3-Key) CMAC generate / verify key
- RSA Signature Key - RSA (2,048 to 16,384 bits) signature generation key
- RSA Decryption Key - RSA (2,048 to 16,384 bits) key decryption (private key transport) key
- DSA Signature Key - FIPS 186-4 DSA (2048/3072) signature generation key
- ECDSA Signature Key - ECDSA (P curves 224-521, B and K curves 233-571) signature generation key
- EC DH Private Key - EC DH (All NIST defined B, K, and P curves) private key agreement key
- HMAC Key - Keyed hash key (160/224/256/384/512)
- Hash_DRBG CSPs - V (440/888 bits) and C (440/888 bits), entropy input (length dependent on security strength)
- HMAC_DRBG CSPs - V (160/224/256/384/512 bits) and Key (160/224/256/384/512 bits), entropy input (length dependent on security strength)
- CTR_DRBG CSPs - V (128 bits) and Key (AES 128/192/256), entropy input (length dependent on security strength)
- CO-Authentication Secret - Pre-calculated HMAC-SHA-1 digest used for Crypto Officer role authentication
- User-Authentication Secret - Pre-calculated HMAC-SHA-1 digest used for User role authentication

6.3. Definition of Public Keys

The following are the public keys contained in the Xperia Cryptographic Module:

- RSA Verification Key - RSA (1024 to 16384 bits) signature verification public key
- RSA Encryption Key - RSA (2048 to 16384 bits) key encryption (public key transport) key

- DSA Verification Key - FIPS 186-4 DSA (1024/2048/3072) signature verification key / FIPS 186-2 DSA (1024) signature verification key
- ECDSA Verification Key - ECDSA (All NIST defined B, K and P curves) signature verification key
- EC DH Public Key - EC DH (All NIST defined B, K and P curves) public key agreement key.

6.4. Definition of CSP Access Modes

Table 8 defines the relationship between CSP access modes and module services. The access modes shown in Table 8 are defined as follows:

- **Generate (*G*)**: Generates the Critical Security Parameter (CSP) using an approved Random Bit Generator (RBG).
- **Use (*U*)**: Uses the CSP to perform cryptographic operations within its corresponding algorithm.
- **Entry (*E*)**: Enters the CSP into the Module.
- **Output (*O*)**: Outputs the CSP from the Module.
- **Zeroize (*Z*)**: Removes the CSP.

Table 8 - CSP Access Rights within Roles & Services

Role		Service Name	CSP (*Access Mode*)
C.O.	User		
X	X	Initialization	***U***: CO Authentication Secret, User Authentication Secret
X	X	Self-Test	-
X	X	Show Status	-
X	X	Zeroization	***Z***: DRBG CSPs, Hash_DRBG CSPs, HMAC_DRBG CSPs, CTR_DRBG CSPs All other services automatically overwrite CSPs stored in allocated memory. Stack cleanup is the responsibility of the calling application.
X	X	Random Number generation	***U***: Hash_DRBG CSPs, HMAC_DRBG CSPs, CTR_DRBG CSPs.
X	X	Asymmetric Key generation	***G***: RSA Signature Key, DSA Signature Key, ECDSA Signature Key
X	X	Symmetric encrypt/decrypt	***U***: AES Key, Triple-DES Key, AES GCM Key, AES XTS Key
X	X	Symmetric digest	***U***: AES CMAC Key, Triple-DES CMAC Key
X	X	Message digest	-
X	X	Keyed Hash	***U***: HMAC Key
X	X	Key transport	***U***: RSA Encryption Key, RSA Decryption Key
X	X	Key agreement	***U***: EC DH Private Key
X	X	Digital signature	***U***: RSA Signature Key, DSA Signature Key, ECDSA Signature Key
X	X	Utility	-

7. Operational Environment

The tested operating systems segregate user processes into separate process spaces. Each process space is logically separated from all other processes by the operating system software and hardware. The Module functions entirely within the process space of the calling application, and implicitly satisfies the FIPS 140-2 requirement for a single user mode of operation.

For FIPS 140-2 validation, the Module is tested by an accredited FIPS 140-2 testing laboratory on the following operating environment:

- Android 5.0 running on Xperia Z4 Tablet with ARMv8 Cryptographic Instructions
- Android 5.0 running on Xperia Z4 Tablet without ARMv8 Cryptographic Instructions

As allowed by FIPS 140-2 Implementation Guidance G.5, the validation status of the Module is maintained when operated in the following additional operating environments:

- Xperia Z4 (with/without ARMv8 Cryptographic Instructions)
- Xperia Z4v (with/without ARMv8 Cryptographic Instructions)
- Xperia Z3+ (with/without ARMv8 Cryptographic Instructions)

In these environments equipped with OS and CPU which are the same as them of the tested operating environments, the Module operates without any modification. The CMVP makes no statement as to the correct operation of the module on the operational environments for which operational testing was not performed.

8. Self-Tests

The Module shall perform the following self-tests.

1. Power-up Self-Tests:
    i. Cryptographic algorithm tests
        a. AES 128 ECB Encryption/Decryption: Known-Answer Tests
        b. AES CCM 192 Encryption/Decryption: Known-Answer Test
        c. AES GCM 256 Encryption/Decryption: Known-Answer Test
        d. XTS-AES 128, 256 bit key sizes to support either the 256-bit key size (for XTS-AES-128) or the 512-bit key size (for XTS-AES-256): Known-Answer Test
        e. AES CMAC 128, 192, 256 CBC Generation/Verification: Known-Answer Test
        f. 3-Key Triple-DES ECB Encryption/Decryption: Known-Answer Test
        g. 3-Key Triple-DES CMAC CBC Generation/Verification: Known-Answer Test
        h. RSA PKCS#1 v1.5 2048 with SHA-256 Signature Generation/Verification: Known-Answer Test
        i. DSA 2048 with SHA-384 Signature Generation/Verification: Known-Answer Test
        j. ECDSA P-224, K-233 with SHA-512 Key Generation/Signature Generation/Verification: Known-Answer Test
        k. HMAC-SHA1: Known-Answer Test
        l. HMAC-SHA224: Known-Answer Test
        m. HMAC-SHA256: Known-Answer Test
        n. HMAC-SHA384: Known-Answer Test
        o. HMAC-SHA512: Known-Answer Test
        p. ECC CDH Shared secret calculation per SP 800-56A: Known-Answer Test
        q. CTR_DRBG AES 256 with/without derivation function: Known-Answer Test
        r. Hash_DRBG SHA256: Known-Answer Test

ii. Software Integrity Test (HMAC-SHA1)

2. Conditional Self-Tests

   i. Continuous (RNG) Tests: DRBG

   ii. SP800-90A Section 11.3: DRBG Health Checks

   iii. Pair-wise consistency test (Signature Generation/Verification or Encryption/Decryption) on each generation of a key pair: RSA, DSA, ECDSA

The Power-up Self-Tests are run automatically during startup.

9. Security Rules

The Xperia Cryptographic Module was designed with the following security rules in mind. These rules are comprised of both those specified by FIPS 140-2 and those derived from Sony Mobile Communications' company policy.

1. The Module shall provide two distinct operator roles. These are the User role, and the Crypto-Officer role.
2. The Module shall provide role-based authentication.
3. The operator shall be capable of commanding the Module to perform the power-up self-test using recycling power or FIPS_selftest() function.
4. The Module is single-threaded and in error scenarios returns only an error value (no data output is returned).
5. The Module does not support concurrent operators.
6. The Module does not output intermediate key generation values.
7. The operator (the calling applications) shall use entropy sources that meet the security strength required for the random number generation mechanism: 128 bits for the DRNG and DRBG mechanisms. This entropy is supplied by means of callback functions. Those functions must return an error if the minimum entropy strength cannot be met.
8. To perform AES GCM, the operator shall choose DRBG with RAND_set_rand_method() function and specify at least 32-bit name field with aes_gcm_ctrl() function for compliance with Section A.5 of FIPS 140-2 Implementation Guidance. Doing so allows the Module to generate at least 96-bit IV from data provided by a strong random source such as "/dev/urandom" and "/dev/random".

10. Policy on Mitigation of Other Attacks

The Xperia Cryptographic Module was not designed to mitigate other attacks outside of the specific scope of FIPS 140-2. Therefore, this section is not applicable.

Table 9 - Mitigation of Other Attacks

Other Attack	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

11. Definitions and Acronyms

Table 10 -Definitions and Acronyms

Term	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
DRNG	Deterministic RNG
DSA	Digital Signature Algorithm
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman
ECDSA	Elliptic Curve DSA
EMI / EMC	Electromagnetic Interference / Electromagnetic Compatibility
HMAC	Hash-based Message Authentication Code
PKCS	Public Key Cryptography Standards
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm

12. Revision History

Date	Version	Description
Nov. 18, 2015	1.0.0	Initial release
July 21, 2016	1.0.1	Updates to Sections 3.1; 3.2; 4; 6.2; 6.3; 6.4 and 9
August 16, 2016	1.0.2	Updates to Sections 3.1, 3.2, 6.1, 6.2, 6.4 and 8