Kaspersky Cryptographic Module (User Mode)

Version 3.0.1.25

FIPS 140-2 Level 1 Security Policy

Version Number: 4.0

Date: February 23, 2017

Table of Contents

1. Module Overview

Kaspersky Cryptographic Module (User Mode) is a software library that provides cryptographic services for various Kaspersky Lab applications. The module is provided as a user-mode DLL.

The cryptographic module is a software module that is executing in a modifiable operational environment by a general purpose computer.

This software module contains a single component:

- cm_um.dll (32-bit or 64-bit)

FIPS 140-2 conformance testing was performed at Security Level 1. The following configurations were tested by the lab.

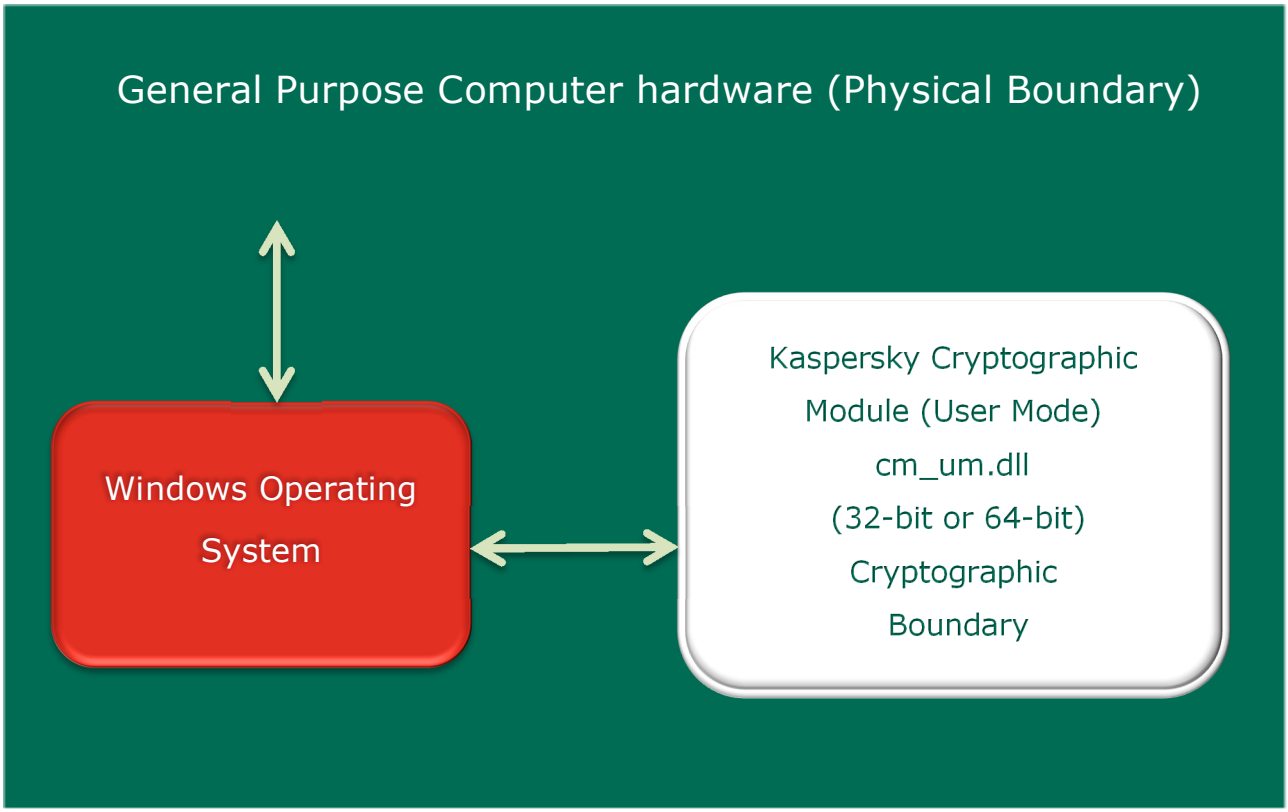
Table 1.1: Configurations tested by the lab.

Software Component	Operating System	Processor(s)	AES NI: Yes/No
cm_um.dll (32-bit)	Windows 7 Professional 32-bit	Intel(R) Core(TM)2 Duo P9600 @ 2.53GHz	No
	Windows 8.1 Enterprise 64-bit	Intel(R) Core(TM) i7-3770S CPU @ 3.10GHz	Yes
	Windows 7 Enterprise 64-bit	Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz	Yes
cm_um.dll (64-bit)	Windows 8.1 Enterprise 64-bit	Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz	Yes
	Windows 7 Enterprise 64-bit	Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz	Yes
	Windows 10 Enterprise 64 bit	Intel® Core™ i7-4600U CPU @ 2.10GHz	Yes

Table 1.2: Module Security Level Statement.

FIPS Security Area	Security Level
Cryptographic Module Specification	1
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

Figure 1: Block Diagram for Kaspersky Cryptographic Module (User Mode)



2. Modes of Operation

In the FIPS approved mode of operation the operator must only use FIPS-approved and allowed security functions listed in the Section 2.1.

In the non-FIPS mode of operation the module performs non-approved functions listed in the Section "2.2 All Other Algorithms" of this security policy. These functions shall not be used in FIPS approved mode of operation.

2.1 Approved and Allowed Cryptographic Functions

The following approved cryptographic algorithms are used in FIPS approved mode of operation.

Table 2.1: Approved Cryptographic Functions.

Algorithm	CAVP Certificate
AES (ECB, CBC, CFB8, CFB128 and XTS) using 128 and 256-bit keys Note: AES-XTS mode is only Approved for storage applications	2849, 2959, 2960, 2980

Algorithm	CAVP Certificate
SP 800-90A DRBG (Hash, HMAC and CTR)	502, 561, 890, 891, 896, 897
HMAC (SHA1, SHA224, SHA256, SHA384, SHA512)	1789, 1879
SHS (SHA1, SHA224, SHA256, SHA384, SHA512)	2391, 2492
SHA3 (224/256/384/512)	vendor affirmed
RSA (FIPS 186-4) SigGen using RSA with keys = 2048 bits/SHA512 and SigVer using 1024/2048/3072 RSA keys for ANSIX9.31, RSASSA-PKCS1_V1_5 and RSASSA-PSS	1490, 1558
PBKDF	vendor affirmed Note: keys derived from passwords, as shown in SP 800-132, may only be used in storage applications. The cryptographic module complies with SP 800-132 Option 2a. The operator must only use 256-bit or stronger random passwords. The upper bound for the probability of having this parameter guessed at random is $1/2^{256}$.

The following non-FIPS approved but allowed cryptographic algorithms are used in FIPS approved mode of operation.

Table 2.2: Non-FIPS Approved But Allowed Cryptographic Functions.

Algorithm
RSA (key wrapping; key establishment methodology provides between 112 and 270 bits of encryption strength) using RSA with keys ≥ 2048 bits
EC DH using |n| = 224, |n| = 384: CURVES(secp224k1, P-384)

2.2 All other algorithms

In the FIPS approved mode of operation the operator must not use the functions listed in the Table 2.3. These functions are available in the User role.

Table 2.3: Non-Approved Cryptographic Functions

Algorithm
(FIPS 186-2) RSA KeyGen
EC DH using |n| = 192: CURVES(secp192k1)
RSA (key wrapping; non-compliant) using RSA with keys < 2048 bits

Algorithm
RSA SigVer using RSA with keys < 1024 bits
RSA SigGen using RSA with keys ≠ 2048 bits or SHA1/SHA224/SHA256/SHA384

3. Ports and interfaces

The logical interfaces of the module are implemented via an Application Programming Interface (API). The following table describes each logical interface.

Table 3: FIPS 140-2 Logical Interfaces.

Logical Interface	Description
Data Input	Input parameters that are supplied to the API commands
Data Output	Output parameters that are returned by the API commands
Control Input	API commands
Status Output	Return status provided by API commands

4. Roles and Services

The module supports a Crypto Officer role and a User Role. The Crypto Officer installs, initializes and de-initializes the module. The Crypto Officer also uses the services provided by the module. The User uses the cryptographic services provided by the module. The module provides the following services.

Table 4: Roles and Services

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read or Execute W – Write or Create Z – Zeroize
Initialization/ de-initialization	Crypto Officer	N/A
Installation	Crypto Officer	N/A
Self-test	User Crypto Officer	N/A
Show status	User Crypto Officer	N/A
Zeroization	User Crypto Officer	All: Z
Random number generation	User Crypto Officer	DRBG CSPs: R, W
Asymmetric key generation	User Crypto Officer	RSA keys: W

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read or Execute W – Write or Create Z – Zeroize
Symmetric encryption/decryption	User Crypto Officer	AES key: R
Message digest generation	User Crypto Officer	N/A
Keyed Hash (Generating or verifying data integrity with HMAC)	User Crypto Officer	HMAC key: R
Asymmetric encryption/decryption	User Crypto Officer	RSA keys: R
Key agreement	User Crypto Officer	EC DH keys: R, W
Digital Signature Generation/Verification	User Crypto Officer	RSA keys: R
PBKDF key derivation	User Crypto Officer	AES key: W HMAC key: W Password: R

Table 4: Roles and Services

Non-Approved cryptographic services are implementations of Non-Approved algorithms. They are listed in the Section 2.2.

5. Cryptographic Keys and CSPs

The table below describes cryptographic keys and CSPs used by the module.

Table 5: Cryptographic Keys and CSPs

Key	Description/Usage	Origin	Zeroization
AES Key	Used during AES encryption and decryption	Generated using DRBG, derived using PBKDF, or provided by user	Zeroized during power cycle or reboot
HMAC Key	Used during calculation of HMAC	Generated using DRBG, derived using PBKDF, or provided by user	Zeroized during power cycle or reboot
RSA Key Pairs	Used for signature generation and verification and key wrapping	Provided by user	Zeroized during power cycle or reboot
DRBG CSPs	Used during generation of random numbers (length of entropy input depends on security strength required by the calling application)	Provided by user	Zeroized during power cycle or reboot

Key	Description/Usage	Origin	Zeroization
EC DH Key Pairs	Used for Key agreement	Generated by the module or provided by user	Zeroized during power cycle or reboot
Password	Used to derive key using PBKDF	Provided by user	Zeroized during power cycle or reboot

The Keys and CSPs are stored in plaintext within the module. Keys and CSPs used in the FIPS Approved mode of operation shall not be used while in the non-FIPS mode of operation. CSPs shall not be established while in the non-FIPS mode of operation.

6. Self-tests

The module performs the following power-up and conditional self-tests. Upon failure of a power-up self-test the module halts its operation.

Table 6: Self-Tests

Algorithm	Test
Software integrity	HMAC-SHA256 KAT
HMAC	HMAC: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KATs
AES	KAT(encryption/decryption): AES-XTS (128 and 256) AES-ECB (128 and 256) AES-CBC (128 and 256) AES-CFB8(128 and 256) AES-CFB128(128 and 256)
RSA	KAT: RSA2048 SHA512 PSS
DRBG	KATs: HASH_DRBG: SHA1, SHA224, SHA256, SHA384, SHA512 HMAC_DRBG: SHA1, SHA224, SHA256, SHA384, SHA512 CTR_DRBG: AES128, AES256
	Continuous Random Number Generator test for DRBGs
	DRBG Health Test
	Continuous Random Number Generator test for entropy source

Algorithm	Test
SHA3	SHA3-224, 256, 384, and 512 KATs
PBKDF	PBKDF2 with HMAC-SHA512 KAT
SHS	KATs: SHA1, SHA224, SHA256, SHA384, SHA512

The module performs all power-up self-tests listed above without operator intervention using DLL entry-point mechanism.