[redacted]

Entrust, Inc.

Cryptographic Module Security Policy

Entrust Security Kernel 7.1

Author: Jean-Pierre Fiset

Date: June, 2007

Document Issue: 1.3

Table of Contents

1 References

Author	Title
NIST	[1] FIPS PUB 140-2: Security Requirements For Cryptographic Modules, December 2002
NIST	[2] Derived Test Requirements for FIPS PUB 140-2, March 2004
NIST	[3] Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, May 2006
Entrust	[CR] Cryptographic Module Validation Cross-Reference for the Entrust Security Kernel 7.1, October 2006
Entrust	[DD] Entrust V7.1 SK Design Description, September 2006
Entrust	[FD] Entrust v7.1 Release SK Functional Description, November 2006
Dell	[UG] Dell OptiPlex GX620 Systems User's Guide – Mini Tower Computer (English), Dell, (http://support.dell.com/support/edocs/systems/opgx620/en/ug/A02/tindex.htm)
Dell	[QRG] Dell OptiPlex GX620 Quick Reference Guide, Dell, 2005 (http://support.dell.com/support/edocs/systems/opgx620/QRG_AMF/K8502A00.pdf)

2 Target Audience

This document is intended to be part of the package of documents that are sent for FIPS validation. It is intended for the following people:

- NIST and the FIPS 140-2 validation group
- CSE
- Developers working on the release
- Product Verification
- Documentation
- Product and Development Managers
- Security Assurance

3 Introduction

This document contains a description of the Entrust Security Kernel (SK) Cryptographic Module Security Policy. It contains a specification of the rules under which the SK cryptographic module must operate. These security rules were derived from the requirements of FIPS 140-2 [1].

3.1 Purpose of the Security Policy

There are three major reasons that a security policy is defined for and must be followed by the cryptographic module:

- It is required for FIPS 140-2 validation.
- It allows individuals and organizations to determine whether the cryptographic module, as implemented, satisfies the stated security policy.
- It describes the capabilities, protection, and access rights provided by the cryptographic module, allowing individuals and organizations to determine whether it will meet their security requirements.

3.2 Cryptographic Module Definition

This section defines the cryptographic module that is being submitted for validation to FIPS 140-2, level 1. The SK cryptographic module is defined as a multi-chip standalone cryptographic module according to FIPS 140-2.

The module consists of the following generic components:

1. A commercially available general-purpose hardware-computing platform. A generic high-level block diagram for such a platform is provided in Figure 1.
2. A commercially available Operating System (OS) that runs on the above platform.
3. A software component, the SK that runs on the above platform and operating system. This component is custom designed and written by Entrust in the C and C++ computer languages, with some small performance-critical sections being written in assembly language. This component is identical, at the source code level, for all identified hardware platforms and operating systems. It is compiled into specific executable object code for each identified platform and linked with an ANSI C library. An Application Programming Interface (API) is defined as the interface to the cryptographic module.

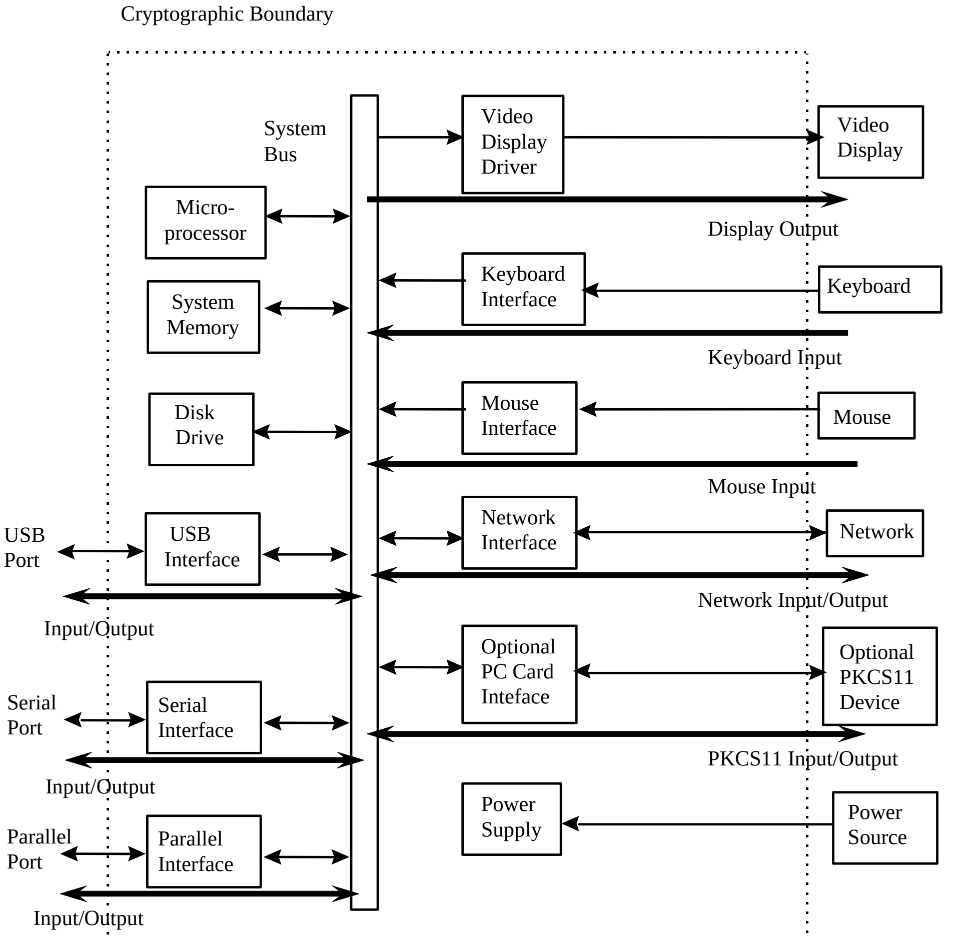
The cryptographic module was tested on the following hardware computing platform and operating system:

1. A Dell™ OptiPlex™ GX620 Mini Tower Computer with:
    - Intel® Pentium® D dual-core 3.2 GHz Processor
    - 2x1GB DDR2 RAM DIMMs
    - Disk Drives WDC WD1600JS-75NCB1 149.0Gb Disk Drive
    - HL-DT-ST DVD+-RW GWA4164B CD/DVD Drive
    - Intel(R) 82945G Express Chipset Family 224Mb
    - NEC 1..44MB Floppy Disk Drive
    - Sound Devices SoundMAX Integrated Digital Audio
    - Bradcom NetXtreme 57xx Gigabit Controller
    - 305 watt power supply

2. Operating Systems:
    - Windows Server 2003

A detailed technical description of the Dell Optiplex GX620 platform is included in [UG] and [QRG].

The SK cryptographic module is also suitable for platforms from the same or other manufacturers, based on compatible processors with equivalent or greater system resources and equivalent or later Operating System versions. Also, the SK cryptographic module used on all Microsoft Operating Systems is identical.



Note: All arrows indicate data flow, however; only bold arrows indicate data (plaintext and encrypted) flows into and out of the Cryptographic Module via physical ports

Figure 1: Cryptographic module block diagram for hardware.

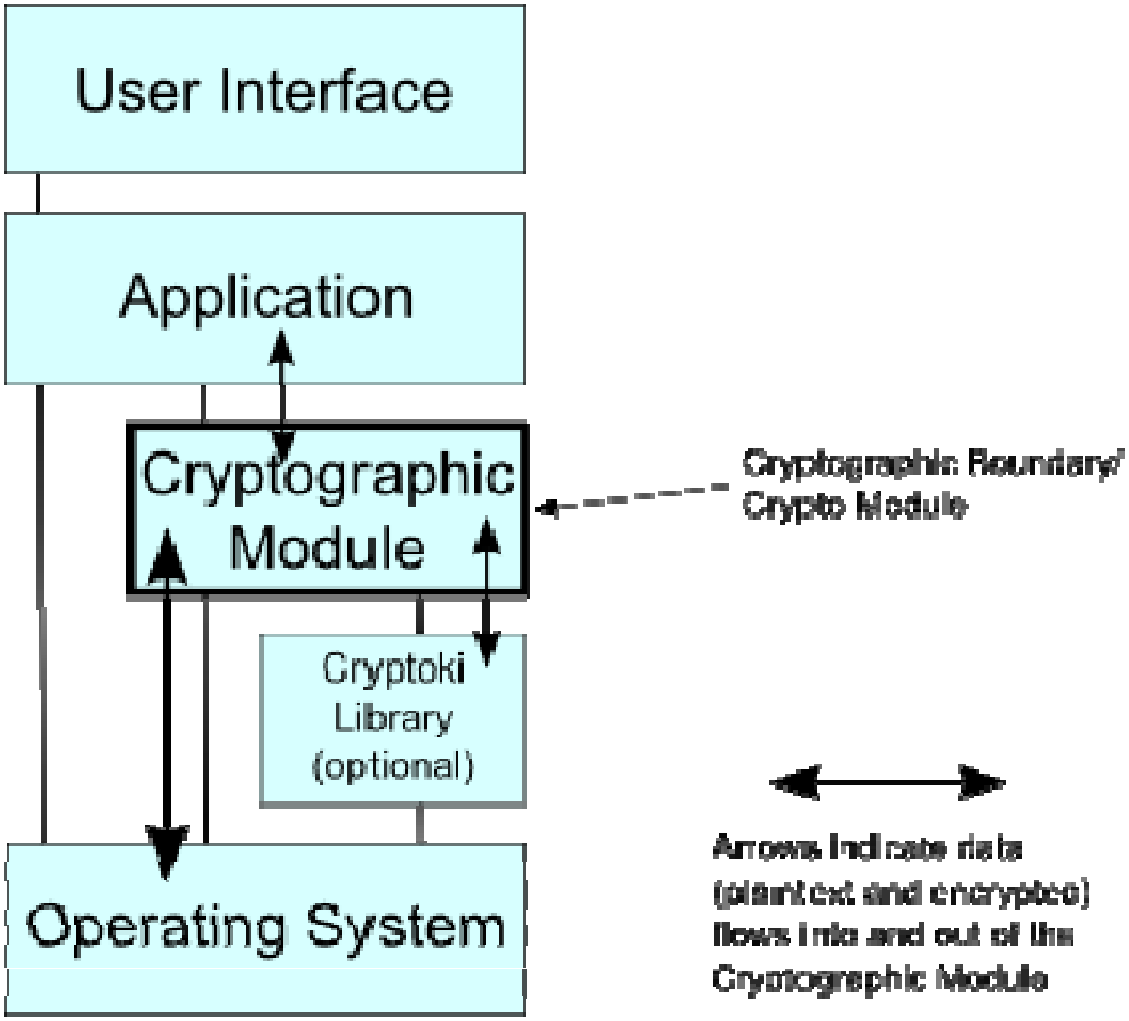

User Interface
Application
Cryptographic Module
Cryptographic Boundary/ Crypto Module
Cryptoki Library (optional)
Operating System
Arrows indicate data (plaintext and encrypted) flows into and out of the Cryptographic Module

Figure 2: Cryptographic module block diagram for software.

3.3 Cryptographic Module Description

The cryptographic module consists of a defined set of C and C++ files that compiled with various Entrust projects. The cryptographic module provides a set of functions (API) that allows developers to integrate the cryptographic module security features into the applications they design. The cryptographic module API is described in detail in the Functional Description [FD] companion document.

The purpose of the cryptographic module is to provide application developers with the access to cryptographic algorithms, and the ability to integrate security into the applications they design. The types of cryptographic algorithms provided include:

- Symmetric Ciphers (encryption/decryption/key generation)
- Asymmetric Ciphers (encryption/decryption/key generation)
- Message Digests (hashing)
- Signatures (signing/verification)
- Message Authentication Codes (creation)
- Keyed-Hash Message Authentication Codes (creation)
- Random Number/Seed Generation
- Key Agreement

- Key Derivation Algorithms

3.4 Module Ports and Interfaces

The SK cryptographic module is considered according to the requirements of FIPS 140-2 to be a multi chip standalone module. The table below describes a mapping of logical interfaces to physical ports:

FIPS 140-2 Interface	Logical Interface	Physical Interface
Data Input Interface	Input parameters of module function calls	Ethernet/Network Port, USB Port, Parallel Port
Data Output Interface	Output parameters and return values of module function calls	Ethernet/Network Port, USB Port, Parallel Port
Control Input Interface	Module control function calls	Keyboard and Mouse
Status Output Interface	Return values from module status function calls	Monitor
Power Interface	Initialization function	Power Interface

Table 1: Mapping Logical Interfaces to Physical Ports

4 Specification of the Security Policy

4.1 Identification and Authentication Policy

The cryptographic module does not identify nor authenticate any user (in any role) that is accessing the cryptographic module. This is only acceptable for FIPS 140-2 level 1 validation.

Role	Type of Authentication	Authentication Data
User	None	N/A
Cryptographic Officer	None	N/A

Table 2: Roles and Required Identification and Authentication

Authentication Mechanism	Strength of Mechanism
None	N/A

Table 3: Strengths of Authentication Mechanisms

4.2 Access Control Policy

The cryptographic module supports two roles: User and Cryptographic Officer. Each service is explicitly assumed by the assigned role. An operator performing a service within any role can read/write cryptographic keys and critical security parameters (CSP) only through the invocation of a service by use of the cryptographic module API. Thus, that user can read/write the cryptographic keys and CSPs that the given API call allows. The type of services corresponding to each of the supported roles is described in the table below.

Role	Authorized Services	Cryptographic Keys and CSPs	Access Type
Cryptographic Officer	Initialization of the Cryptographic Module	None	Execute
	Initiate Cryptographic Module Self Tests	None	Execute
	Key Input/Output	AES, Triple-DES, RSA, DSA, ECDSA, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512 keys	Execute
	Key Generation (FIPS 186-2)	AES, Triple-DES, RSA, DSA, ECDSA, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512 keys	Execute, Write
	Module Status	None	Read
User	Symmetric Encryption/Decryption	AES, Triple-DES keys	Execute
	Digital Signature Generation/Verification	DSA, ECDSA, RSA keys	Execute
	Hash Generation	None	Execute
	MAC Generation	Triple-DES, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512 keys	Execute
	Key Agreement	Diffie-Hellman keys	Execute
	Random Number/Seed Generation	None	Execute

Table 4: Services Authorized for Roles

The following is a list of the validated FIPS Approved algorithms (including appropriate algorithm certificates) that can be used in FIPS mode:

FIPS Approved Algorithm	Certificate Number
FIPS186 RNG	#261
Triple DES	#495
Triple DES-MAC	#495
AES	#484
RSA	#198
DSA	#196
ECDSA	#45
SHA-1	#551
SHA-256	#551
SHA-384	#551
SHA-512	#551
HMAC-SHA1	#238
HMAC-SHA256	#238
HMAC-SHA384	#238
HMAC-SHA512	#238

Table 5: FIPS-Approved Algorithms

The following is a list of FIPS Allowed algorithms which are non-FIPS Approved but can nevertheless be used in FIPS mode since they are no equivalent algorithms approved in FIPS:

- Diffie-Hellman supports key lengths of 1024 bits. Diffie-Hellman (key agreement; key establishment methodology provides 80 bits of encryption strength)
- RSA supports key sizes between 1024 bits and 8192 bits. RSA (key wrapping; key establishment methodology provides between 80 and 201 bits of encryption strength)

The following is a list of non-FIPS Approved algorithms that are implemented but cannot be used when operating in FIPS mode:

- NIST 800-90 DRBG RNG
- CAST
- CAST3
- CAST5
- RC2
- RC4
- IDEA
- MD2
- MD5
- RIPEMD-160
- PAKE
- DES
- DES MAC
- AES MAC

4.3 Self-Tests

The cryptographic module contains the following self-tests to verify its correct operation. The Power-On Self-Tests are run automatically when the module is initialized. The Continuous Tests are run during normal operations of the module. These tests are required in order to operate the module in FIPS Approved Mode of operation:

Power-On Self-Tests:

- Software integrity test using Triple-DES-MAC
- FIP186-2 RNG KAT and continuous test
- AES KAT for encrypt/decrypt
- Triple-DES KAT for encrypt/decrypt
- SHA-1, SHA-256, SHA-384, SHA-512 KATs
-
- Triple-DES MAC KAT
- HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512 KATs
- RSA/SHA1 KAT for sign/verify
- RSA pair-wise consistency test
- DSA/SHA1 KAT for sign/verify
- DSA pair-wise consistency test
- ECDSA/SHA1 KAT for sign/verify
- ECDSA pair-wise consistency test
- NIST 800-90 DRBG RNG KAT and continuous test

Conditional Tests:

- FIPS 186-2 RNG continuous test
- NIST 800-90 DRBG RNG continuous test
- RSA pair-wise consistency test
- DSA pair-wise consistency test
- ECDSA pair-wise consistency test

4.4 Physical Security Policy

The physical security of the cryptographic module is provided by the PC that it is being used on. For more detailed information on the physical security please refer to [UG], [QRG], and [SM].

4.5 Operational Environment

4.5.1 Assumptions

The following assumptions are made about the operating environment of the cryptographic module:

- Unauthorized reading, writing, or modification of the module’s memory space (code and data) by an intruder (human or machine) is not possible; this is prevented by the process memory management of the Operating System.
- Replacement or modification of the legitimate cryptographic module code by an intruder (human or machine) is not feasible.
- The module is initialized to the FIPS 140-2 mode of operation.

4.5.2 Installation and Initialization

The following steps must be performed to install and initialize the SK cryptographic module for operating in a FIPS 140-2 compliant manner:

- All the executable files shipped with the SK must be copied to the machine on which the SK is being used. These files are generally called “etfile32.dll” or “etsesn32.dll”, depending on the product, and are copied during the software installation of an Entrust product.
  To operate the SK in a FIPS 140-2 compliant mode, the cryptographic module must be initialized specially; this is done by calling SK_Initialize(TRUE), followed by the necessary calls to an instance of class SK_SoftwareAuthenticator.

4.5.3 Policy

The following policy must always be followed in order to achieve a FIPS 140-2 mode of operation:

- All keys entered into the cryptographic module must be verified as being legitimate and belonging to the correct entity by software running on the same machine as the cryptographic module.
- Virtual memory that exists on the machine when the cryptographic module runs must be configured to reside on a local, not a networked, drive.
- Input/Output of plaintext private or secret cryptographic keys and CSPs on/from any physical port must be prohibited by the operator of the cryptographic module.
- Only FIPS approved algorithms must be requested from the Entrust cryptographic module.
- The above conditions must be upheld at all times in order to ensure continued system security after initial setup of the validated configuration. If the module is removed from the above environment, it is assumed to not be operational in the validated mode until such time as it has been returned to the above environment and re-initialized by the user to the validated condition.

4.5.4 Module Operator

FIPS 140-2 states that when using a software cryptographic module, the operating system shall be restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded). NIST has since provided further implementation guidance[3] regarding this matter:

“Software cryptographic modules implemented in client/server architecture are intended to be used on both the client and the server. The cryptographic module will be used to provide cryptographic functions to the client and server applications. When a crypto module is implemented in a server environment, the server application is the user of the cryptographic module. The server application makes the calls to the cryptographic module. Therefore, the server application is the single user of the cryptographic module, even when the server application is serving multiple clients.”

This indicates that for an application built on the SK cryptographic module, the application is always the single user of the cryptographic module even when multiple applications are running concurrently. This permits multiple concurrent SK based applications to be running on the same machine in a FIPS 140-2 compliant manner.

4.6 Mitigation of Other Attacks Policy

The cryptographic module is not designed to mitigate any specific attacks.

Other Attacks	Mitigation Mechanism	Specific Limitations
None	N/A	N/A

Table 6: Mitigation of Other Attacks