**Entrust Technologies**

# Entrust Cryptographic Module 5.0

# FIPS 140-1 Validation Security Policy


Author: Marc Laroche



Document Issue: Release 1.1

Issue Date: December 1999



Abstract: This document describes the Entrust Security Kernel 5.0 (Cryptographic Module) Security Policy submitted for validation, in accordance with the FIPS publication 140-1, level 1.


# 1. Contents

## 2. Cryptographic Module Definition

This document describes the Entrust Security Kernel 5.0 (Cryptographic Module) Security Policy submitted for validation, in accordance with the FIPS publication 140-1, level 1.

The module consists of the following generic components:

- A commercially available general-purpose hardware computing platform. A generic high-level block diagram for such a platform is provided in Figure 1.
- A commercially available Operating System (OS) that runs on the above platform.
- A software component, called the Entrust Cryptographic Kernel, that runs on the above platform, under the above operating system. This component is custom designed and written by ETL 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.

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

A Dell OptiPlex Gxa Midsize Personal Computer system with:

- an Intel Pentium II 266 MHz processor,
- 128 MB system RAM (DIMM),
- 2 serial ports and 1 parallel port,
- 4.3 GB hard drive,
- 3COM 3C509 Ethernet card,
- the Windows NT 4.0 Workstation Operating System (in single user mode).

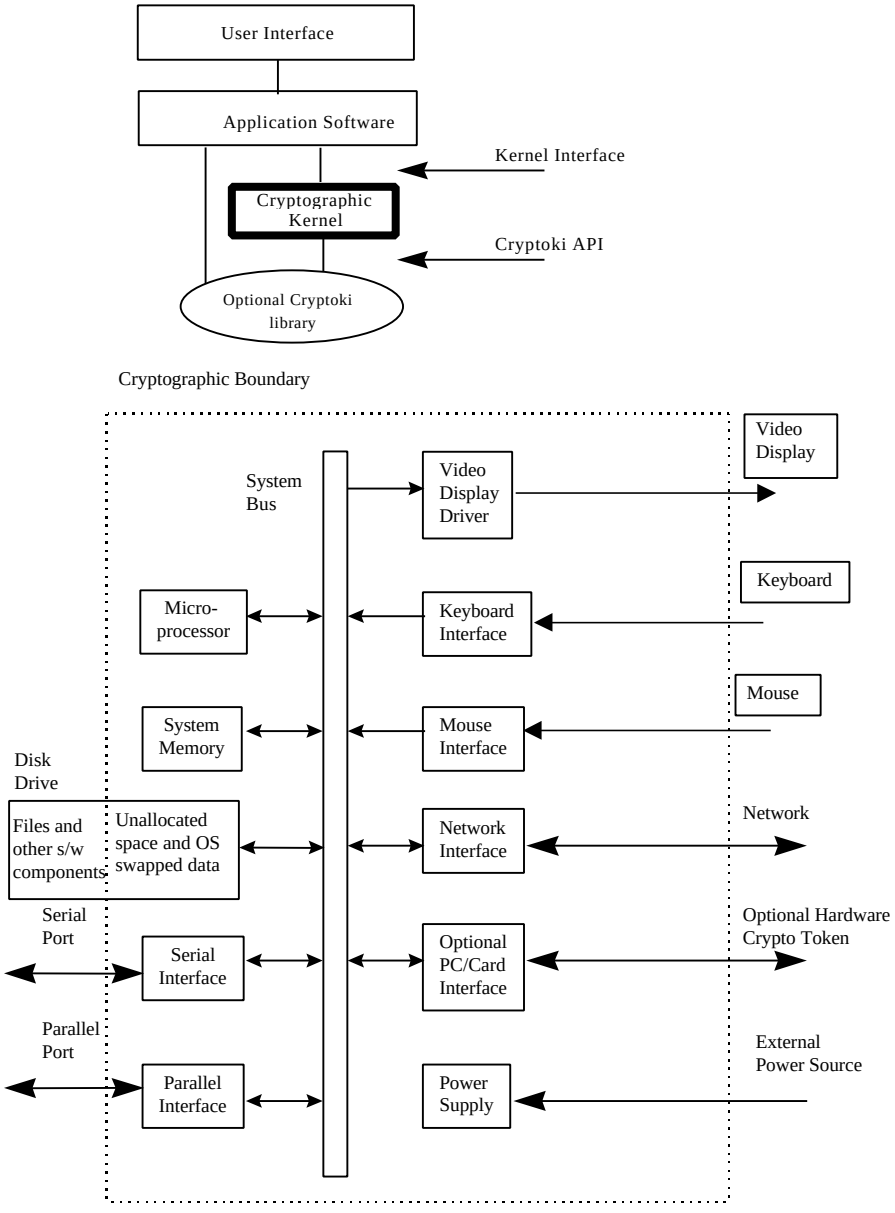
A detailed technical description of the Dell OptiPlex Gxa platform is included in [RIG].

The Entrust cryptographic kernel 5.0 has been validated on the above platform to FIPS 140-1 level 1. The implementation of the module is also suitable for FIPS 140-1 level 1 on any general purpose computers from the same or other manufacturers, based on compatible processors with equivalent or greater

system resources and equivalent or later Operating System versions, including Windows 95/98, Windows NT 3.5 and 3.51 and Windows NT 4.0 SP4, SP5, and SP6, provided that:

The general purpose computer uses the single user operating system/mode specified on the validation certificate, or another compatible single user operating system, and
The software of the cryptomodule does not require modification when ported (platform specific modifications are excluded).

**Figure 1 Cryptographic module block diagram for hardware (bottom) and software (top)**



# 3. Security Policy

This section describes the security policy for the module, as defined in FIPS PUB 140-1 and the companion Test Requirements document. The FIPS 140-1 cryptographic module is defined to be the module identified earlier in section 2 of this document.

## 3.1 Authentication Policy

The cryptographic module must perform authentication of the operator before it can deliver any cryptographic services. Authenticated operators are authorized to assume one or a set of the following supported roles: public user, private user or cryptographic officer.

Operators authenticate themselves in the public user role by presenting a valid MAC; the MAC is stored in the *entrust.ini* file and is the same for all authorized Entrust users[1]. Authentication to the user private and cryptographic officer roles is performed by presenting a valid user password; the password is unique to each individual user. The functions that allow users to login into the user private and cryptographic officer roles are only available from the user public role; an operator must be already authenticated in the user public role before he/she can authenticate in the user private and cryptographic officer roles.

## 3.2 Access Control Policy

The cryptographic module supports three roles: user public, user private and crypto-officer. An operator accesses services available from the user public role after being successfully authenticated with a valid MAC, and accesses services available from both user private and cryptographic officer roles after being successfully authenticated with a valid password. An operator performing a service within any role can read and write security-relevant data items only through the invocation of a service by means of the cryptographic module API. The type of services corresponding to each of the supported roles is described in Table 1.

[1] Under normal operations, Entrust software automatically reads the MAC form the entrust.ini file and presents it to the cryptographic module on behalf of the user. The cryptographic module will not initialize unless a valid MAC is provided.

**Table 1 Roles and Services**

| Role | Services |
|---|---|
| User Public | Authentication, symmetric key generation, key destruction, symmetric encryption/decryption, hashing, MAC generation/verification, self-test, login. |
| User Private | Key pair generation, asymmetric encryption/decryption (sign/verify), password change. |
| Cryptographic Officer | Configuration of cryptographic services (e.g. set/generate initialization vector) |

The whole set of cryptographic services is available to operators that are authenticated into the user private and cryptographic officer roles. Only those services that do not require access to an operator asymmetric private key, and services that modify the configuration of the cryptographic module, can be accessed from the public role.

The following FIPS approved basic services are provided by the cryptographic module:

1. Cryptographic data hashing using FIPS PUB 180-1 SHA-1 (and MD2, MD5, RIPEMD-160, HMAC-MD5, HMAC-SHA-1 and HMAC- RMD160)[2].

2. Bulk data encryption, decryption, and MAC calculation using FIPS PUB 46-2 DES and 3-DES) (and CAST, CAST3, CAST5, IDEA, RC2, IDEA and cipher stream RC4)[1] .

3. Signing and signature verification using FIPS PUB 186-1 DSA and RSA (and ECDSA) [1].

The Entrust cryptographic module also provides the following services:

1. Key wrapping and unwrapping using RSA.

2. Key agreement using Diffie-Hellman.

3. User authentication (as described above).

4. Random number generation using an ANSI X9.17-compliant software-based algorithm, or a hardware token-based generator.

[2] Algorithms in parenthesis have not been FIPS-approved yet; therefore, the kernel is not operating in accordance with FIPS 140-1 when these algorithms are selected.

The FIPS 140-1 related Security Relevant Data Items (SRDI) include DES keys, 3-DES keys, DSA and RSA private keys, and DSA parameters.[3] When the cryptographic module is initialized into a FIPS 140-1 compliant mode (this is done by passing TRUE to the initialization function), the following restrictions take effect:

1. During the generation of random symmetric, asymmetric, and generic keys in software, the random numbers must come from the software-based random number generator and not from any hardware token.

2. Asymmetric private, and generic keys, cannot be input or output to/from the module via the kernel API in plaintext form. They may, however, be input or output in wrapped (encrypted) or hashed form.

3. Symmetric keys (except for 3-DES keys) cannot be input to the module via the kernel API in plaintext form. Symmetric keys (including 3-DES keys) cannot be output from the module in plaintext form. They may, however, be input or output in wrapped (encrypted) or hashed form.

4. Symmetric, asymmetric private, and generic keys cannot be input or output to/from the module via the Cryptoki interface in plaintext form. They may, however, be input or output in wrapped (encrypted) form.

5. Software authentication must be performed after initialization of the module and before any cryptographic operations are attempted.

6. User authentication must be performed after initialization of the module and before any cryptographic operations are attempted, as described above in section 3.1.

7. In non-FIPS mode, software authentication and user authentication are optional.

8. Only DES can be used in the X9.17 random number generator.

### 3.3 Environment

The following assumptions are made about the operating environment of the cryptomodule:

1. Unauthorized reading, writing, or modification of the module's memory space (code and data) by an intruder (human, program or otherwise) is not feasible.

[3] IVs are either loaded externally, in which case the length is verified to be 64 bits (only CBC mode is used), or are generated internally using the internal RNG, which is FIPS approved.

2. Replacement or modification of the legitimate module code by an intruder (human, program or otherwise) is not feasible.

3. The module is initialized to the FIPS 140-1 mode of operation, as described in section 4.

4. For operation in level 2 Physical Security mode, tamper-evident seals are applied as indicated at Figure 2.

To these ends, the following operational rules must be followed by a user or integrator of the module.

1. The Entrust Cryptographic Module is being validated to be used with:

    - one or more applications, as a shared Windows DLL, or

    - single application, as a statically linked library.

2. The module is to be used by only one human operator at a time and must not be actively shared among operators at any period during its lifetime. Also, there must be only one instance of the cryptographic module loaded in RAM at any given time on a given machine.

3. All public keys entered into the module must be verified as being legitimate and belonging to the correct entity by software running on the same platform as the cryptomodule.

4. Virtual memory that exists on the platform where the cryptomodule runs must be configured to reside on a local, not a networked, drive.

5. 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. Installation Guidance

1. To operate the Entrust cryptographic module in FIPS mode, the FipsMode entry in the FIPS Mode section of the Entrust initialization (entrust.ini) file must be set to 1. For example,

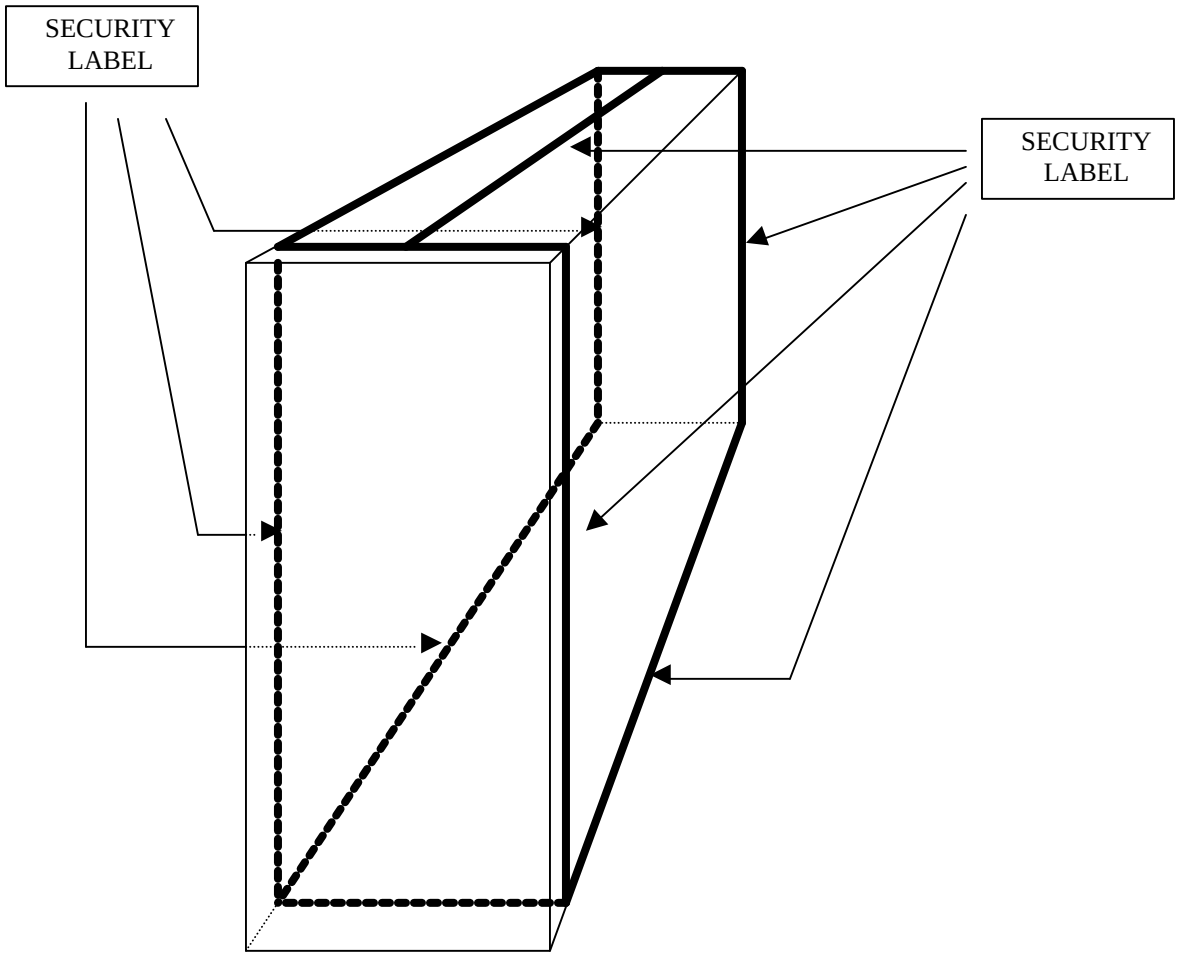
   *[FIPS Mode]*
   *FIPS=1*
   *Etfile32Name=etfile32*
   *Etfile32Auth=DES-MAC,64, F404A ...*
   *Etsesn32Name=etsesn32*
   *Etsesn32Auth=DES-MAC,64, E23B1 ...*

   Setting FipsMode to 0 (zero) prevents the module from operating in FIPS mode.

2. The operating system should be configured to operate securely and prevent remote login. Reference [4] provides guidance on securing Windows NT 4.0.

3. To operate the Entrust cryptographic module in level 2 Physical Security mode, tamper-evident labels must be applied to the computing platform so that it is not possible to open/remove any removable covers or panels without leaving detectable signs such as broken label or detection of label residue on the enclosure. Administrators or security officers should apply approved labels as indicated at Figure 2. The storage and distribution of the labels should remain under the auspices of an administrator or security officer.

**Figure 2 Location of Tamper-Evident Seals**



## 5. References

[1] FIPS PUB 140-1: Security Requirements for Cryptographic Modules. National Institute of Standards and Technology, 11 January 1994.

[2] Derived Test Requirements for FIPS PUB 140-1, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, September, 1994.

[3] PKCS #1: RSA Cryptography Specifications, Version 2.0, RSA Laboratories, September 1998.

[4] Deploying Windows NT 4.0 in a C2 Evaluated Configuration. http://www.microsoft.com/security/issues/deployingc2.asp, December 1999.