Entrust TruePass Applet Cryptographic Module v5.2

FIPS 140-1 Validation Security Policy

Author: Marc Laroche

Document Issue: 2.3

Issue Date: June 27, 2002

Abstract: This document describes the Entrust TruePass Applet Cryptographic Module v5.2 Security Policy submitted for validation, in accordance with the FIPS publication 140-1, level 1.

Contents

1 Cryptographic Module Definition

This document describes the Entrust TruePass Applet Cryptographic Module v5.2 Security Policy submitted for validation, in accordance with the FIPS publication 140-1, level 1. It is implemented as a multi-chip standalone cryptographic module.

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. For the purpose of this validation, the module was tested on Microsoft NT 4.0 SP3, Windows 2000 SP2 and Windows 95/98 running in single-user mode.
- A commercially available FIPS validated crypto kernel operating within a web browser configured in FIPS mode that runs on the above OS (To date, there are two web browsers that meet this requirement. They are Netscape Security Module version 1.01 that has been FIPS validated (Cert #47) and to be used in FIPS approved mode. The second is Microsoft's Base DSS Cryptographic Provider, DSS Cryptographic Provider, DSS/Diffie-Hellman Enhanced Cryptographic Provider, and Enhanced Cryptographic Provider, version 5.0.2150.1391 (Certificate #103).
- A software component, called the TruePass Applet Cryptographic Module, is compiled into an applet that runs on the above platform, OS and web browser. This component is custom designed and written by Entrust Inc. in the Java computer language and is identical, at the source code level, for all supported hardware platforms, operating systems and web browsers.

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

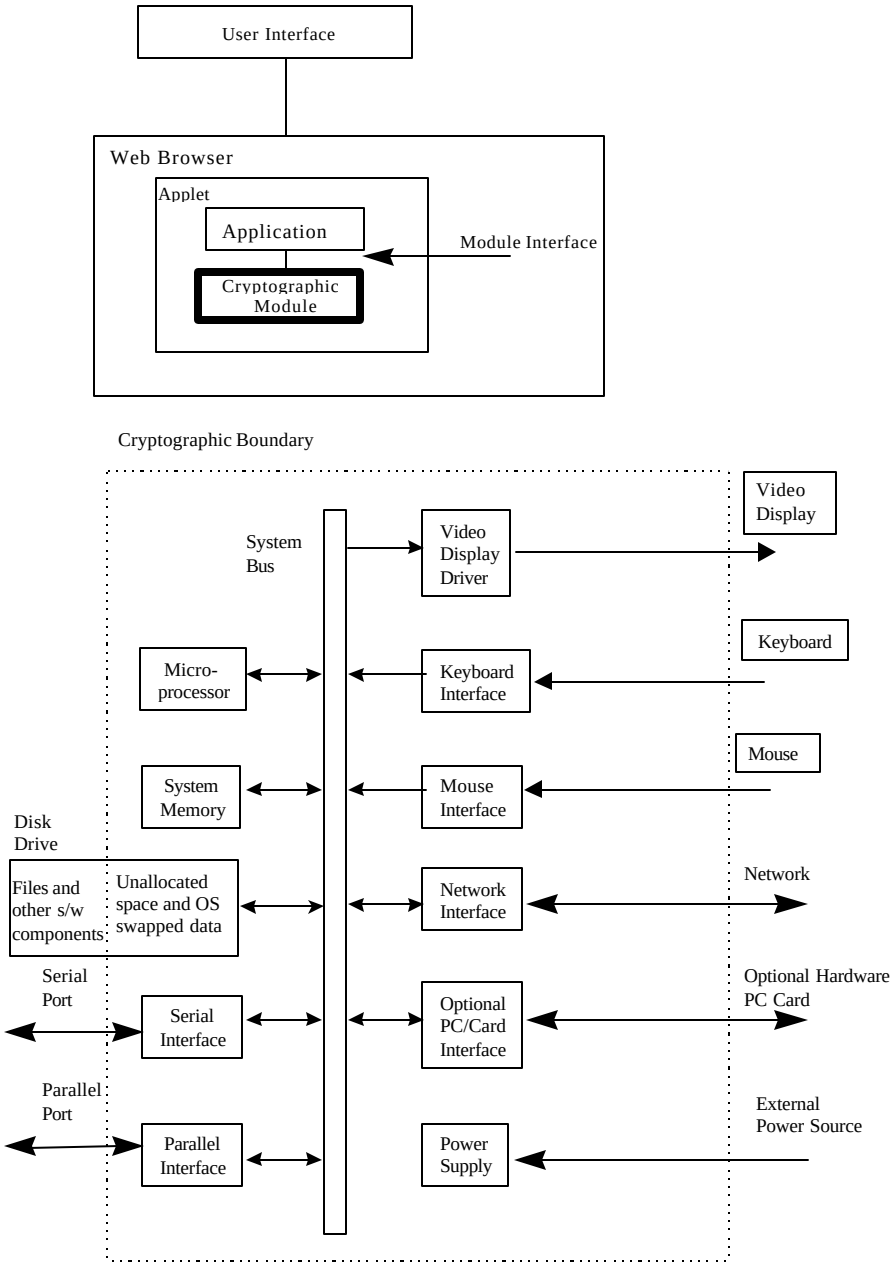
1. A Dell OptiPlex GXa Workstation with:
   - 1 Intel Pentium II 266 MHz processors,
   - 128 MB system RAM (DIMM),
   - 2 serial ports and 1 parallel port,
   - a 4.3 GB hard drive
   - PCI Ethernet card.
2. Microsoft Windows NT 4.0 service pack 3, Windows 2000 SP2 and Windows 95/98 operating systems running in single-user mode.

3. Netscape Communicator 4.7 and Microsoft Internet Explorer 5.5.

The TruePass Applet Cryptographic Module has been validated on the above platform to FIPS 140-1 level 1 and is suitable 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, provided that:

1. The general purpose computer uses the specified single user operating system/mode specified on the validation certificate, or another compatible single user operating system, and
2. The software of the cryptomodule does not require modification when ported (platform specific modifications are excluded).
3. The Browser contains a FIPS module operating in SSL and FIPS mode.

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



2 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 1 of this document.

2.1 Authentication Policy

No Authentication - Neither users nor cryptographic officers need to perform any authentication function in order to use the cryptographic module. This type is only acceptable at security level 1.

2.2 Access Control Policy

The cryptographic module supports two roles: user and crypto-officer. 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 Roles and Services.

Table 1 Roles and Services

Role	Services
User	Symmetric encryption/decryption, hash, self-test, signature generation and verification and asymmetric key generation
Cryptographic Officer	Configuration of cryptographic services (e.g. set/generate initialization vector), key entry and all services of the user role

An operator is explicitly in the user or cryptographic officer role based upon the services chosen. If any of the cryptographic officer specific services are called upon then the operator is in the cryptographic officer role otherwise the operator is in the user role.

The following FIPS approved basic services are provided by the cryptographic module (currently, there are no non-FIPS algorithms implemented):

1. Cryptographic data hashing using FIPS PUB 180-1 SHA-1.

2. Bulk data encryption, decryption using FIPS PUB 46-3 DES and 3-DES.

3. Signature generation/verification and key wrapping using PKCS#1 RSA.

The Entrust cryptographic module also provides the following services:

1. Random number generation using an ANSI X9.17-compliant software-based algorithm.

The FIPS 140-1 related Security Relevant Data Items (SRDI) include DES keys, 3-DES keys, RSA private keys, seeds for random number generator and random numbers generated.

2.3 Operational Environment

2.3.1 Level 1 Mode of Operation

2.3.1.1 Assumptions

The following assumptions are made about the operating environment of the cryptographic module in Level 1 mode of operation:

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.

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.

These assumptions are also applicable to the server on which the applet normally resides.

2.3.1.2 Policy

1. The TruePass Applet Cryptographic Module has been validated to be used by:

    - one or more applets

2. The browser must contain a FIPS140-1 validated module.

3. The browser must be configured to operate in SSL and FIPS mode.

4. 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.

5. All keys entered into the module must be verified as being legitimate and belonging to the correct entity by software (i.e. the TruePass Applet) running on the same platform as the cryptographic module.

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

7. 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.

3 Installation Guidance

3.1 Level 1 Mode of Operation

1. To operate the Entrust cryptographic module in FIPS mode, the SecurityEngine::initialize(true) must be called first before any of the cryptographic operations are called.
   - Power-up self-tests are then immediately performed upon the first invocation of SecurityEngine::initialize(true), subsequent calls will not perform self-tests again. In order to perform self-tests again, the module must be restarted and hence these power-up self-tests are also considered on-demand self-tests. The self-tests performed here are cryptographic algorithm known answer tests for the following: SHA1, DES, TripleDES and RSA. If any one of these tests fails, the module is put into an error state and no cryptographic operations performed nor sensitive data (as described in section 3.2) output with an exception to indicate this. To exit this error state, the module must be restarted.
   - There are also conditional tests that are performed as described below:
     - Pair-wise Consistency test (as described in AS11.19 of FIPS140-1) is performed every time asymmetric key pairs are generated. Upon failure of test, the keys are regenerated until such time as the test passes.
     - Continuous Random Number Generator test (as described in section AS11.22 of the FIPS140-1) is performed ever time a random number is generated. The number is regenerated until such time as the test passes.

2. The operating system should be configured to operate securely and to prevent remote login.

3. Browser must be configured to operate in SSL and FIP S mode to ensure integrity of the applet being downloaded. Refer to browser documentation below for configuration.

   - Netscape documentation:
     http://developer.netscape.com/docs/manuals/security/fips/enable.htm
     http://developer.netscape.com/docs/manuals/security/fips/server.htm
   - Microsoft documentation:
     http://support.microsoft.com/support/kb/articles/Q238/2/68.ASP

4 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.