Entrust TruePass Applet Cryptographic Module

FIPS 140-2 Validation Security Policy

Document Issue: 4.0

Issue Date: February 2006

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

Contents

1 Cryptographic Module Definition

This document describes the Entrust TruePass Applet Cryptographic Module Security Policy submitted for validation, in accordance with the FIPS publication 140-2, 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 Windows 2000 SP4 and Windows XP SP2.
- A commercially available FIPS validated cryptographic kernel operating within a web browser configured in FIPS mode that runs on the above OS.

  For example, using Microsoft Internet Explorer with a validated Cryptographic Provider, such as

  Microsoft DSS/Diffie-Hellman Enhanced Cryptographic Provider (Version 5.0.1998.1), validated on Windows NT 4.0 as described in FIPS validation certificate 60,

  Microsoft Base Cryptographic Provider, Enhanced Cryptographic Provider, Base DSS Cryptographic Provider, and DSS/Diffie-Hellman Enchanced Cryptographic Provider (Version 5.0.1877.6 and 5.0.1877.7) , validated on Windows NT 4.0 as described in FIPS validation certificate 68,

  Microsoft Base DSS Cryptographic Provider, Base Cryptographic Provider, DSS/Diffie-Hellman Enhanced Cryptographic Provider, and Enhanced Cryptographic Provider validated on Windows 95 and Windows 98 as described in FIPS validation certificate 75,

  Microsoft Base DSS Cryptographic Provider, Base Cryptographic Provider, DSS/Diffie-Hellman Enchanced Cryptographic Provider, and Enhanced Cryptographic Provider validated on Windows 2000 as described in FIPS validation certificate 76,

Microsoft Base DSS Cryptographic Provider, Base Cryptographic Provider, DSS/Diffie-Hellman Enhanced Cryptographic Provider, and Enhanced Cryptographic Provider ((Base DSS: 5.0.2150.1391 [SP1], 5.0.2195.2228 [SP2] and 5.0.2195.3665 [SP3]), (Base: 5.0.2150.1391 [SP1], 5.0.2195.2228 [SP2] and 5.0.2195.3839 [SP3]), (DSS/DH Enh: 5.0.2150.1391 [SP1], 5.0.2195.2228 [SP2] and 5.0.2195.3665 [SP3]), (Enh: 5.0.2150.1391 [SP1], 5.0.2195.2228 [SP2] and 5.0.2195.3839 [SP3])) validated Windows 2000 as described in FIPS validation certificate 103,

Microsoft Enhanced Cryptographic Provider (RSAENH) Version 5.1.2600.1029 also known as Base Cryptographic Provider (Versions 5.1.2518.0 and 5.1.2600.1029) validated on Windows XP as described in FIPS validation certificate 238,

Microsoft DSS/Diffie-Hellman Enhanced Cryptographic Provider for Windows XP (Software Version 5.1.2518.0) validated on Windows XP as described in FIPS validation certificate 240,

Microsoft Windows Server 2003 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH) (Software Version 5.2.3790.0) validated on Windows 2003 as described in FIPS validation certificate 381,

Microsoft Windows Server 2003 Enhanced Cryptographic Provider (RSAENH) (Software Version 5.2.3790.0) validated on Windows 2003 as described in FIPS validation certificate 382,

or using Netscape browser with the Netscape security module:

Netscape Security Module 1 (ID: fipscm_v1) as described in FIPS validation certificate 7,

Netscape Security Module 1.01 (ID: fipscm_v1.01) as described in FIPS validation certificate 45,

Netscape Security Module 1.01 (ID: fipscm_v1.01) as described in FIPS validation certificate 47.

- A software component, called the TruePass Applet Cryptographic Module, is compiled into an archive of class files (commonly referred to as 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:

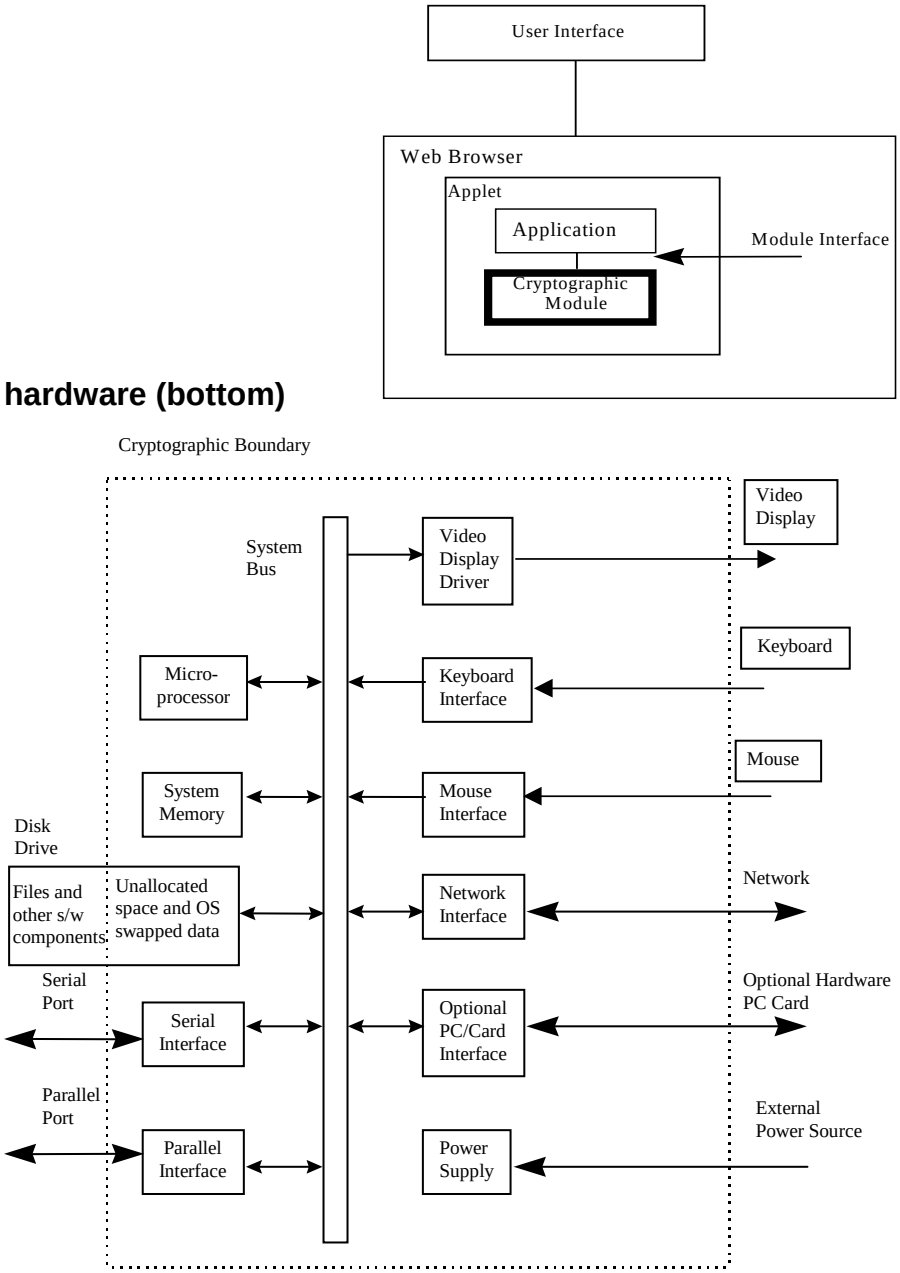
1. An IBM Netvista Workstation with:
    - 1 Intel Pentium IV 2.8 GHz MHz processor,
    - 512 MB system RAM (DIMM),
    - 2 serial ports and 1 parallel port,
    - a 20 GB hard drive and a 60 GB hard drive
    - PCI Ethernet card.
    - Windows XP (Service Pack 2)
    - Windows 2000 (Service Pack 4)

2. Netscape Navigator 7.0 and Microsoft Internet Explorer 6.0 SP1.
3. Browser support for Java: either Microsoft VM for Java 5.0.0.3810 or Sun plug-in version 1.4.1

The TruePass Applet Cryptographic Module has been validated on the above platforms to FIPS 140-1 level 1 and FIPS 140-2 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/TLS 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 140-2 and the companion Test Requirements document. The FIPS 140-2 cryptographic module is defined to be the module identified earlier in section 1 of this document.

2.1 Identification and 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.

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.

Table 1 Roles and required identification and authentication

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

Table 2 Strengths of Authentication mechanisms

Authentication Mechanism	Strength of Mechanism
None	N/A

2.2 Access Control Policy

The type of services corresponding to each of the supported roles is described in Table 3 .

Table 3 Services authorized for roles

Role	Authorized Services
User	Symmetric encryption/decryption, hashing, self-test, asymmetric key pair generation, asymmetric key wrapping
Cryptographic Officer	Installation of the server software, configuration of cryptographic services, 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. In addition, CAST-128 is implemented as a non-FIPS approved algorithm.

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

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

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

4. PKCS#1 RSA key generation using a FIPS 186-2 appendix 3.1 compliant software-based pseudo-random number generation algorithm.

The Entrust cryptographic module also provides the following services:

1. Random number generation using a FIPS 186-2 appendix 3.1 compliant software-based algorithm.

The FIPS 140-2 related Security Relevant Data Items (SRDI) include Triple DES keys, RSA private keys, seeds for random number generator and random numbers generated.

Table 4 FIPS 140-2 Approved Services Authorized for Roles

Approved Service	*Key, Algorithm or Operation*	*Certificate Number*	*Accessible Roles*	*Types of Access*
symmetric encryption/ decryption	Triple-DES	377	User	Read/Write
asymmetric key wrapping (not approved but allowed in FIPS mode)	RSA public (key wrapping, key establishment methodology provides 80-bits to 112-bits of encryption strength)	91	User	Read/Write
asymmetric key unwrapping (not approved but allowed in FIPS mode)	RSA private	91	User	Read/Write
asymmetric signature generation	RSA private	91	User	Read/Write
hash	SHA-1	379	User	N/A
asymmetric key generation	RSA public+private	91	User	Read/Write
Random number generation	FIPS 186-2 Appendix 3.1	129 (SHA-1 used)	User	N/A
self-test	None		User	N/A
Installation and configuration of FIPSMode=1	None		Cryptographic Officer	N/A
Show status	None		User	N/A

The other services that are not FIPS approved are detailed in **Table** 5 below.

Table 5: Non-FIPS approved services authorized for roles

Service	*Key, Algorithm or Operation*	*Accessible Roles*	*Types of Access*
symmetric encryption/ decryption	CAST-128	User	Read/Write

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 140-2 or 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 browser must contain a FIPS140-1 or FIPS140-2 validated module.

2. The browser must be configured to operate in SSL/TLS and FIPS mode.

3. The TruePass applet must be configured to run in FIPS mode, as described in section 4.1.

4. On the client platform the module is to be used by only one 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 client machine.

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

6. 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**.**

The Entrust cryptographic module provides the underlying functions to support FIPS 140-2 Level 1 key management.

2.4 Cryptographic Key Management

The Entrust cryptographic module provides the underlying functions to support FIPS 140-2 Level 1 key management.

2.4.1 Key Generation

The Entrust Cryptographic module provides FIPS 140-2 compliant key generation. Random number generation uses a FIPS approved method, the software-based FIPS 186-2 General Purpose RNG.

2.4.2 Key Entry and Key Output

The module does not allow the import or export of keys or other security sensitive information from outside of the physical boundary in plaintext format. For key entry and export, all Secret keys are wrapped with RSA.

2.4.3 Key Storage

The Entrust Cryptographic module does not provide key storage.

2.4.4 Key Zeroization

The Entrust TruePass Applet doesn't store any keys. When encryption keys are generated they reside in volatile memory in plaintext, they are used, exported, and discarded at session’s end. The keys, once used within the java virtual machine, are sent to the java garbage collector that immediately gets rid of any keys after the session is completed. Once the keys have been used and discarded, they cannot be retrieved.

3 Physical Security Policy

The physical security of the cryptographic module is provided by the PC that it is being used on. Physical Security requirements for FIPS 140-2 modules are not applicable. The module provides an integrity check of the software as part of the self-test procedure.

4 Installation and Initialization Guidance

4.1 Installation

The following steps are required during installation to operate the TruePass cryptographic module in FIPS mode.

1. Configure the web server to support SSL/TLS.
2. Install the signed applet on the server, as part of the TruePass install.
3. Ensure the FIPSMode setting is set to 1 in the EntrustTruePassClientConfig.js file.
4. Install a FIPS compliant browser on the client machine. No other software is required on the client machine, since the applet is downloaded during initialization. Configure the browser to use SSL/TLS and be sure to select a FIPS-approved algorithm. This will ensure integrity of the applet being downloaded. Refer to browser documentation for configuration instructions, or consult the browser vendor for applicable instructions.

4.2 Initialization

No software is needed for a client using TruePass, other than a browser. To initialize the TruePass applet, perform these steps.

1. Configure the web server to support SSL/TLS.
2. Configure the browser to use SSL/TLS and select a FIPS-approved algorithm.
3. Navigate to the web server. The SSL/TLS certificate and applet signature will be verified by the browser. The applet self-test will be performed when the applet initializes, if the FIPSMode is set during installation in step 3 of 4.1.

4.3 Self-Tests

The following self-tests are performed.

1. Power up cryptographic tests. The applet performs known answer tests for SHA1, Triple-DES, RSA, and SHA1-RNG. If any one of these tests fails, the module is put into an error state and no cryptographic operations are performed. An error message indicating that initialization has failed is written to the log. To exit this error state, the module must be restarted.
2. Conditional tests. There are also conditional tests that are performed as described below:
    a. Pair-wise Consistency test (as described in AS11.19 of FIPS140-2) is performed every time asymmetric key pairs are generated. Upon failure of test, the keys are regenerated until such time as the test passes.
    b. Continuous Random Number Generator test (as described in section AS11.22 of the FIPS140-2) is performed every time a

random number is generated. The number is regenerated until such time as the test passes.

5 Mitigation of other attacks policy

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

Table 5 Mitigation of other attacks

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

6 References

[1] FIPS PUB 140-2: Security Requirements for Cryptographic Modules. National Institute of Standards and Technology, May 2001.

[2] Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, November 2001.

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