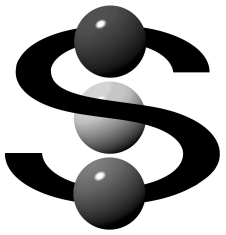


3S Group

T2CSS User's Manual

Product Name: Type 2 Cryptographic Support Server
FCC ID: P2JT2CSS

FCC Compliance Statement

This device complies with Part 15 of the FCC Rules for Class B digital devices. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Notice

NOTE: This equipment has been tested and found to comply with the limits for a
Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are
designed to provide reasonable protection against harmful interference in a
residential installation. This equipment generates electromagnetic energy and, if not installed and used in accordance with the instructions, may cause harmful interference with other electronic components. If, when installed within a host personal computer (PC), this equipment does cause harmful interference, which can be determined by turning the host computer off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Verify that the cover of the host computer chassis is properly closed.
- Increase the separation between the equipment and host computer
- Connect the equipment into an outlet on a circuit different from that to which

the host computer is connected.

Table of Contents

Introduction

The Type 2 Cryptographic Support Server (T2CSS) User's Manual includes an overview of the T2CSS system and instructions for installing, administering and operating the T2CSS through the Administrator's interface.

The intended audience for this manual is the Administrator who has been delegated as the System/Security Administrator for the domain in which use of the T2CSS is intended.

The instructions in this document assume the reader has some knowledge of Windows NT administration and the available tools. The administrator should have a basic understanding of the operating system, directory structure, and typical Windows NT commands, as well as familiarity with the Graphical User Interface (GUI). Basic knowledge of the FORTEZZA card, its API, and its and library would be helpful; the documentation at

http://www.armadillo.huntsville.al.us/Fortezza_docs/index.html

is highly recommended. The hardware information in this manual applies to the Peripheral Component Interconnect (PCI) bus architecture supported by the Windows NT operating system.

Overview

This section gives a basic overview of the T2CSS system and discusses the operating environment, use and problem reporting capabilities.

2.1 Operating Environment

The T2CSS consists of a PCI board and host software designed to work on a Personal Computer (PC) platform. The system characteristics, operating system and T2CSS configuration related parameters are described below.

System Characteristics:
The following minimum requirements are recommended:

Pentium II, 266 MHz or better
96MB RAM
4 GB hard drive
SVGA graphics display controller
Monitor
Keyboard
33 MHz PCI slot (one per T2CSS board)

Operating System:

Windows NT 4.0 Server or Enterprise Server with service pack 3 or greater

T2CSS Configuration Requirements:
Primary memory

128KB (minimum) for the Windows NT driver
2-3 MB for T2CSS Application

Hard Drive

18MB for T2CSS install image (not including Windows NT memory management)
144KB (maximum) per Virtual FORTEZZA Card containing 48 certificates (approximately 3KB per certificate); times the anticipated number of VFCs in the T2CSS
10MB (minimum) audit log file

Note:
1. The total number of VFCs are dependent upon the user organization.
2. The size of the audit log file is dependent upon the audit settings and the number of errors occurring. If one or a few events are being monitored, the size of the audit log file will be smaller than if all events are being monitored.

The audit log file will inevitably grow if the audit function is enabled because the T2CSS will typically operate continuously. So it is highly recommended that the Administrator review, archive (off the system) or purge audit log files regularly. Otherwise, the system performance will suffer, especially when Windows NT has contention for disk space.

2.2 System Use

The T2CSS provides security services appropriate for protecting Sensitive But Unclassified (SBU) data. The Virtual FORTEZZA Card and the T2CSS board are the operational elements used to perform the security processing. The T2CSS board is an intelligent PCI board that mounts directly into a 32-bit 33 MHz host bus expansion slot. The T2CSS PCI board contains eight cryptographic processors and a control processor. The control processor distributes the data between the host and the cryptographic processors.

The T2CSS provides confidentiality, data integrity, digital signature, key management, and auditing. The encryption, hashing and signature algorithms supported by the T2CSS are based on the Federal Information Processing Standards (FIPS) established by the National Institute of Standards and Technology (NIST). The T2CSS ensures confidentiality by using the Skipjack Encryption standard, FIPS 185. The T2CSS ensures data integrity by using the Secure Hash Algorithm (SHA-1), FIPS 180-1. The T2CSS supports authentication and non-repudiation services by using the Digital Signature Standard (DSS), FIPS 186. The T2CSS allows exchange of cryptographic key information by using the Key Exchange Algorithm (KEA).

The T2CSS is application protocol independent. This means that the T2CSS can easily be integrated into a variety of software applications and hardware platforms that support the Windows NT operating system. A standard PCI bus configuration is necessary to accommodate the T2CSS boards. The T2CSS has a standardized set of cryptographic commands and a set of drivers that can interface with most software applications.

2.3 System Overview

This section discusses the components of the T2CSS system, performance benefits of the T2CSS, supervisory controls related to the T2CSS system, and gives an overview of operations for the T2CSS Administrator.

2.3.1 T2CSS System Components

The T2CSS consists of both hardware and software components. It resides on a server platform to provide security services to high throughput server-based applications.

Installation

This section of the manual describes the steps for installing the hardware and software components of the T2CSS.

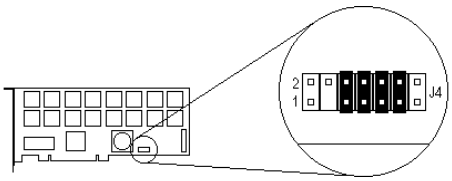
3.1 Hardware

To install the T2CSS PCI bus card, first shut down the Windows NT operating system and power down the computer. Make sure the computer is unplugged from the power source before removing the computer cover.

Be sure to use proper grounding equipment (e.g., wrist strap provided) during installation to avoid damaging the board.

Verify the jumper settings as below:
4 Jumpers are required for proper operation.
Remove the computer's cover to gain access to the expansion slots. (The computer manufacturer's documentation should explain this in detail.) There may be slots of different lengths and even of different types. Select an available PCI slot and install the T2CSS board. The T2CSS board is a standard PCI plug-and-play device. The Windows NT system will recognize the card and send the appropriate information to the board driver.

After inserting the T2CSS board into an available PCI slot, screw the mounting bracket into the computer. Replace the computer cover, reconnect the power supply, and turn on the computer.



#1 PIN 3-4
#2 PIN 5-6
#3 PIN 7-8
#4 PIN 9-10