Sentinel Model III Computer Security System

Security Target

VERSION 5.6

June 2002

Prepared by:

Delta Security Technologies
205 S Whiting Street
Alexandria, VA 22304

TABLE OF CONTENTS

Chapter/ Paragraph	Title	Page
CHAPTER 1.	Security Target Introduction	1
1.0	Introduction	1
1.1	Security Target Identification	1
1.2	ST Overview	2
1.3	Common Criteria Conformance Claim	10
1.4	Conventions	11
1.5	Terms	11
CHAPTER 2.	Target of Evaluation Description	15
2.0	Introduction	15
2.1	Applicability of ST	15
2.2	Sentinel Implementation	15
2.2.1	Concept of Operations	16
2.2.2	Sentinel TOE Subsystems	20
2.2.3	Sentinel Kit Add-On Components	29
2.3	TOE Functional Description	34
2.3.1	Security Functions	35
2.3.2	Sentinel TSF Interfaces/TOE Boundary	48

CHAPTER 3. Target of Evaluation Security Environment 50
3.0 Introduction..... 50
3.1 Intended Usage of TOE..... 50
3.2 Facility Characteristics..... 51
3.3 User Characteristics..... 51
3.4 Operator Roles..... 52
3.5 Protected Assets 52
3.6 Threats..... 52
3.6.1 Threat Agents……...53
3.6.2 Threats to TOE…….53
3.7 Assumptions…….54
3.7.1 Physical Assumptions…….54
3.7.2 Personnel Assumptions……...54
3.7.3 Connectivity Assumptions……..54
CHAPTER 4. Security Objectives..... 56
4.0 Introduction..... 56
4.1 TOE Security Objectives..... 56
4.2 Security Objectives for the Environment..... 57
4.3 Security Objectives Rationale 58
4.3.1 Threat v Security Objectives for TOE....……...……58

4.3.1.1 [T.ACCESS_SECRETS] v Security Objectives for TOE……..…...59

4.3.1.2 [T.ACCESS_INFO] v Security Objectives for TOE…..…..……..59

4.3.1.3 [T.PROCESS_INFO] v Security Objectives for TOE……...…...59

4.3.1.4 [T.DISABLE_TOE] v Security Objectives for TOE…….…...60

4.3.1.5 [T.ADMIN_RIGHTS] v Security Objectives for TOE…….…...60

4.3.2 Threat v Security Objectives for Environment……..…….....60

4.3.2.1[T.ACCESS_SECRETS] v Security Objectives for Environment….61

4.3.2.2 [T.DISABLE_TOE] v Security Objectives for Environment……....61

4.3.3 Assumptions v Security Objectives for Environment……..61

4.3.3.1 [A.LOCATE] v Security Objectives for Environment…….62

4.3.3.2 [A.PROTECT] v Security Objectives for Environment……..…….62

4.3.3.3 [A.ROLES] v Security Objectives for Environment……...…….62

4.3.3.4 [A.CONNECT] v Security Objectives for Environment…….…….62

CHAPTER 5. Information Technology Security Requirements..... 63

5.0 Introduction……..63

5.1 TOE Security Functional Requirements 65

5.1.1 Security Audit Data Generation Requirements……..……65

5.1.1.1 FAU_GEN.1 Audit Data Generation..... 65

5.1.1.2 FAU_GEN.2 User Identity Association..... 67

5.1.2 Security Audit Review Requirements..... 67

5.1.2.1 FAU_SAR.1 Audit Review..... 68

5.1.2.2 FAU_SAR.2 Restricted Audit Review..... 68

5.1.3 Security Audit Event Storage Requirements..... 68

5.1.3.1 FAU_STG.1 Protected audit data storage..... 69

5.1.3.2 FAU_STG.4 Prevention of Audit Data Loss..... 69

5.1.4 Access Control Policy Requirements..... 69

5.1.4.1 FDP_ACC.2 Complete Access Control..... 70

5.1.5 Access Control Functions..... 70

5.1.5.1 FDP_ACF.1 Security Attribute Based Access Control..... 70

5.1.6 Residual Information Protection Requirements..... 72

5.1.6.1 FDP_RIP.1 Residual Information Protection Requirements..... 73

5.1.7 Authentication Failures Requirements..... 73

5.1.7.1 FIA_AFL Authentication Failure Handling……..……..73

5.1.8 User Attribute Definition Requirements..... 74

5.1.8.1 FIA_ATD.1 User Attribute Definition..... 74

5.1.9 Specification of Secrets Requirements..... 74

5.1.9.1 FIA_SOS.1 Verification of Secrets..... .75

5.1.10 User Authentication Requirements..... 75

5.1.10.1 FIA_UAU.2 User Authentication Before Any Action..... 75

5.1.10.2 FIA_UAU.7 Protected Authentication Feedback..... 76

5.1.11 User Identification Requirements..... 76

5.1.11.1 FIA_UID.2 User Identification Before Any Action..... 76

5.1.12 User-Subject Binding Requirements..... 76

5.1.12.1 FIA_USB.1 User-Subject Binding..... 77

5.1.13 Management of Security Attributes Requirements..... 77

5.1.13.1 FMT_MSA.1 Management of Security Attributes 77

5.1.13.2 FMT_MSA.2 Secure Security Attributes..... 78

5.1.13.3 FMT_MSA.3 Static Attribute Initialisation…….78

5.1.14 Management of TSF Data Requirements..... 78

5.1.14.1 FMT_MTD.1 Management of TSF Data 79

5.1.15 Revocation Requirements 79

5.1.15.1 FMT_REV.1 Revocation..... 79

5.1.16 Security Management Roles Requirement..... 79

5.1.16.1 FMT_SMR.2 Restrictions on Security Roles..... 80

5.1.17 Fail Secure Requirements……..81

5.1.17.1 FPT_FLS.1 Failure with Preservation of Secure State 81

5.1.18 TSF Physical Protection Requirements……..81

5.1.18.1 FPT_PHP.3 Resistance to Physical Attack..... 81

5.1.19 FPT_RVM.1 Reference Mediation Requirements…….…….82

5.1.19.1 FPT_RVM.1 Non-bypassability of the TSP 82

5.1.20 Domain Separation Requirements……..82

5.1.20.1 FPT_SEP.1 TSF Domain Separation..... 83

5.1.21 Time Stamps Requirements……83

5.1.21.1 FPT_STM.1 Reliable Time Stamps 83

5.1.22 Limitation on Scope of Selectable Attributes Requirement……..…83

5.1.22.1 FTA_LSA.1 Limitation on Scope of Selectable Attributes 84

5.1.23 TOE Session Establishment Requirement……..84

5.1.23.1 FTA_TSE.1 TOE Session Establishment..... 84

5.2 TOE Security Assurance Requirements..... 85

5.3 Security Requirements Rationale..... 85

5.3.1 [O.IDENTIFICATION] v TOE Security Requirements……...……86

5.3.2 [O.AUTHENTICATION] v TOE Security Requirements……...……87

5.3.3 [O.HBAC] v TOE Security Requirements……...……87

5.3.4 [O.RESIDUAL_INFO] v TOE Security Requirements……...……88

5.3.5 [O.AUDIT] v TOE Security Requirements……...…...……88

5.3.6 [O.ENFORCEMENT] v TOE Security Requirements……....……88

5.3.7 [O.TOE_PROTECT] v TOE Security Requirements…….……..88

5.3.8 [O.FAILSAFE] v TOE Security Requirements…..……..……89

5.3.9 [O.SEPARATION] v TOE Security Requirements…..…….…...……89

5.4 Security Requirements Dependencies…….…….89

CHAPTER 6 TOE Summary Specifications……..…91

6.0 Introduction..... 91

6.1 TOE Security Fuctions……..…..91

6.1.1 FAU_GEN.1 Audit Data Generation..... 91

6.1.2 FAU_GEN.2 User Identity Association…….……..93

6.1.3 FAU_SAR.1 Audit Review……..93

6.1.4 FAU_SAR.2 Restricted Audit Review……...…..94

6.1.5 FAU_STG.1 Guarantees of Audit Data……..…..94

6.1.6 FAU_STG.4 Prevention of Audit Data Loss ..... .94

6.1.7 FDP_ACC.2 Complete Access Control..... 95

6.1.8 FDP_ACF.1 Security Attribute Based Access Control..... 97

6.1.9 FDP_RIP.1 Full Residual Information Protection..... 98

6.1.10 FIA_AFL.1 Authentication Failures 99

6.1.11 FIA_ATD.1 User Attribute Definition ……..…….100

6.1.12 FIA_SOS.1 Strength of Authentication Data..... 101

6.1.13 FIA_UAU.2 User Authentication Before Any Action..... 101

6.1.14 FIA_UAU.7 Protected Authentication Feedback..... 102

6.1.15 FIA_UID.2 User Identification Before Any Action..... 102

6.1.16 FIA_USB.1 User-Subject Binding..... 103

6.1.17 FMT_MSA.1 Management of Security Attributes 103

6.1.18 FMT_MSA.2 Secure Security Attributes…….....104

6.1.19 FMT_MSA.3 Static Attribute Initialisation……..…..……..104

6.1.20 FMT_MTD.1 Management of TSF Data 104

6.1.21 FMT_REV.1 Revocation of User Attributes..... 105

6.1.22 FMT_SMR.2 Restrictions on Security Roles..... 105

6.1.23 FPT_FLS.1 Failure with Preservation of Secure State 106

6.1.24 FPT_PHP.3 Resistance to Physical Attack 107

6.1.25 FPT_RVM.1 Non-bypassability of the TSP 107

6.1.26 FPT_SEP.1 Domain Separation..... 108

6.1.27 FPT_STM.1 Reliable Time Stamps 110

6.1.28 FTA_LSA.1 Limit on Scope of Selectable Attributes 110

6.1.29 FTA_TSE.1 TOE Session Establishment..... 111

6.2 Assurance Measures……..……111

6.2.1 ACM_CAP.3 Authorization Controls..... 111

6.2.2 ACM_SCP.1 TOE CM Coverage 112

6.2.3 ADO_DEL.1 Delivery Procedures..... 112

6.2.4 ADO_IGS.1 Installation, Generation, and Start-up Procedures..... 112

6.2.5 ADV_FSP.1 Informal Functional Specification..... 112

6.2.6 ADV_HLD.2 Security Enforcing High-Level Design..... 112

6.2.7 ADV_RCR.1 Informal Correspondence Demonstration..... 113

6.2.8 AGD_ADM.1 Administrator Guidance..... 113

6.2.9 AGD_USR.1 User Guidance..... 113

6.2.10 ALC_DVS.1 Identification of Security Measures..... 113

6.2.11 ATE_COV.2 Analysis of Coverage..... 114

6.2.12 ATE_DPT.1 Testing: High-Level Design..... 114

6.2.13 ATE_FUN.1 Functional Testing..... 114

6.2.14 ATE_IND.2 Independent Testing – Sample..... 114

6.2.15 AVA_MSU.1 Examination of Guidance..... 114

6.2.16 AVA_SOF.1 Strength of TOE Security Function Evaluation..... 114

6.2.17 AVA_VLA.1 Developer Vulnerability Analysis..... 115

6.2.18 ACM_AUT.1 Partial Configuration Management Automation..... 115

6.2.19 ACM_CAP.4 Generation Support and Acceptance Procedures..... 115

6.2.20 ACM_SCP.2 Problem Tracking CM Coverage..... 115

6.2.21 ADO_DEL.2 Detection of Modification..... 115

6.2.22 ADV_FSP.2 Fully Defined External Interfaces..... 116

6.2.23 ADV_IMP.1 Subset of the Implementation of the TSF..... 116

6.2.24 ADV_LLD.1 Descriptive Low-Level Design..... 116

6.2.25 ADV_SPM.1 Informal TOE Security Policy Model..... 116

6.2.26 ALC_LCD.1 Developer Defined Life-Cycle Model..... 117

6.2.27 ALC_TAT.1 Well-Defined Development Tools 117

6.2.28 AVA_MSU.2 Validation of Analysis 117

6.2.29 AVA_VLA.2 Independent Vulnerability Analysis..... 117

6.3 Summary Specification Rationale…….117

LIST OF TABLES

Table No.	Title	Page
2.1	ST Functional Requirements as Enabled in TOE	49
4.1	Threats v Security Objectives for TOE	58
4.2	Threat v Security Objectives for the Environment	60
4.3	Assumptions v Security Objectives for Environment	61
5.1	Sentinel Security Functional Requirements	64
5.2	Auditable Events	66
5.3	Sentinel Security Assurance Requirements	85
5.4	Security Requirements Rational	86
5.5	Functional Requirements Dependencies	90
6.1	Implementation of Audit Data Requirements	92
6.2	Implementation of Access Control Requirements	97

LIST OF FIGURES

Figure No.	Title	Page
1.	Sentinel Kit Installed in Computer	21
2.	Security Module	22

CHAPTER 1. Security Target Introduction

1.0 Introduction

This chapter contains document management and overview information necessary to describe a Security Target (ST). The ST identification provides the descriptive information necessary to identify, catalogue, and cross-reference an ST. The ST overview summarizes the target in narrative form and provides sufficient information for a potential user to determine whether the ST is of interest. The conventions section provides an explanation of how this document is organized and the terms section gives a basic definition of terms that are specific to this ST.

1.1 Security Target Identification

Title: Sentinel Model III Computer Security System Security Target
Version: 5.6, June 2002
Developer: Delta Security Technologies, 205 S. Whiting Street, Alexandria, VA 22304
Target of Evaluation (TOE): Sentinel Computer Security System

This Security Target (ST) has been prepared by Delta Security Technologies, 205 S. Whiting Street, Alexandria, VA 22304. This ST supports the Target of Evaluation (TOE) as implemented within the Sentinel Computer Security System. The ST has been developed to the extent feasible against the following specifications:

1. Common Evaluation Methodology for Information Technology Security, Part 1: Introduction and General Model, Draft Version 0.6, January 11, 1997

2. Common Evaluation Methodology for Information Technology Security, Part 2: Evaluation Methodology, Version 1.0 August 1999

3. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 2.1 August 1999

4. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Version 2.1, August 1999

5. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 2.1, August 1999

6. Glossary of Computer Security Terms, NCSC-TG-004-88, October 21, 1988

1.2 ST Overview

The Sentinel Security Target, hereafter called the ST, was designed against the objectives necessary to address security for computers and workstations in a Government and Industry environment that are used to process multiple levels of restricted data. It is assumed that the threat environment consist of organizational insiders such as employees, consultants, and any individuals that have apparent authorized access to the facility where restricted data is processed and have IT skills that range from that of the average PC user to highly trained IT specialists. The threat must also be assumed to have a superior knowledge of the IT environment that includes knowledge of where assets are located and how they are being protected. Finally it must also be assumed that threat is anonymous, motivated, and has access to those areas in the facility where restricted data and information is stored and processed.

The characteristics of the threat environment will require the Sentinel Target of Evaluation (TOE) to incorporate counter-measures in which few, if any, assumptions can be made about a computer user's level of trust. This will certainly require the TOE to have: very strong Identification and Authentication (I&A); access control that is non-discretionary to users and based on verifiable security attributes; a protected security audit capability; a capability to protect restricted data during and after the completion of user sessions; a limitation of access to the minimum number of users based on their assigned role or job; and a design that is capable of withstanding attacks from an adversary with some direct access to the computer. These requirements, when translated into Common Criteria Functional and Assurance Requirements, will define a set of TOE Security Functions (TSFs) capable of meeting an Evaluation Assurance Level (EAL) of 4 for selected CC components in the following classes of functional requirements: Class FAU- Security Audit; Class FDP – User Data Protection; Class FIA –

Identification and Authentication; Class FMT – Security Management; Class FPT – Protection of the TSF; and Class FTA – TOE Access.

Conformance of the TSFs will be based on the functional requirements defined for each component and the TOE's scope of control (TSC). Since the Sentinel TOE is a hardware based security system its TSC will be defined by the range and strength of security functions capable of being performed in Hardware and Firmware. The benefit of implementing a TSF within the Sentinel hardware is that it is totally isolated from the computer/workstation processes and, therefore, less susceptible to the software based threats associated with attacks from hackers and viruses. The tradeoff is that the isolation from computer/workstation processes limits the granularity of hardware based TSFs when compared to software based TSFs. This tradeoff is reasonable when considering that the software that runs within the computer or workstation protected by the Sentinel TOE is essentially protected by the TOE and can provide the additional granularity in a security hardened environment.

In essence the Sentinel has been designed as a very strong hardware based shield that is isolated from software based threats thereby providing a high level of protection to the processes and operations performed on restricted data at different security levels within the host computer or workstation. It should also be noted that TSFs must be evaluated within the TSF Scope of Control (TSC) which is the "set of interactions that can occur with or within a TOE and are subject to the rules of the 'TSP" or TOE Security Policy. Traditional notions of a TSF based on software based TOEs and TSCs are not relevant to the Sentinel TOE and its hardware based TSC.

This ST provides for a level of protection that is appropriate for a well-managed user community requiring protection against insider threats. The TOE is essentially intended to counter attacks by organizational insiders of average to superior technical competence in IT within a controlled and secure facility. This ST also is designed to attenuate and limit the threats posed by malicious administrative personnel by controlling and limiting their access to restricted data in the computers/workstations that they administer. The Sentinel has also been designed as a product that is suitable for use in both commercial and government environments. Since the Sentinel has been designed to protect against hostile attacks from insiders including some

Security Administrators, the ST has been set to an EAL 4 level of assurance. The Sentinel has also been primarily targeted for an environment in which the host computer is usually assigned to a single user and owner of the data stored on their machine. Sharing of computers or workstations is still possible within the Sentinel TOE since each user of a host computer or workstation can have different access rights with respect to the information and operations available within restricted security domains. The Sentinel TOE, however, does not allow simultaneous sharing of a domain and/or a session.

The Sentinel TOE consists of the hardware, software, and firmware necessary to create, maintain, protect, administer, and control access to as many as two restricted security domains within a host desktop personal computer (PC) or workstation. Each restricted security domain is defined by computer processing components consisting of a single Removable Hard Disk Drive (RHDD), Network Interface Card (NIC), modem, and two USB ports. The processing within the domain is implemented using the host computer's CPU which operates through the operating system and applications software within the domains RHDD. A Security Module, described in detail in Chapter 2, is responsible for implementing the TOE Security Functions (TSFs) consisting of: the Identification and Authentication (I&A) of authorized users; User Data Protection; Security Audit; Security Management; Protection of TSFs; and functions relating to TOE Access. The Security Module includes a Smart Card Reader; LCD Module Interface (RS 232); LED Domain Status Indicators, and a Secure Microcontroller that is mounted on the Asset Status Sensor and Controller Printed Circuit Board. In essence, the Secure Microcontroller, is the TOE central processor that implements the firmware based TOE Security Policy (TSP). All the other TOE components interface with the Secure Microcontroller through the hardware interface provided by the Asset Status Sensor and Controller Board.

In addition to the restricted domains, the TOE establishes the host computer with all its original components including internal hard disk drive, NIC, modem, USB ports, Floppy Disk Drive (FDD), Compact Disk (CD) Drive, Digital Video Disk (DVD) Drive as an unrestricted domain that can be accessed by an user. This domain can also be enabled as the default domain for user's who fail to gain access to a restricted domain after several attempts for any reason. When operating in a restricted domain user's will not have access to any Read/Write (R/W) Drive that uses portable media including the FDD, Zip Drive, and any R/W CD Drive. Nor will

users operating in a restricted domain, be able to write data to any Non-Volatile Memories that are shared between domains. Read Only Drives such as CD and DVD drives are enabled in the restricted domain. It should be noted that the Security Module will only permit one user to be logged into the TOE and one domain at any given time by only enabling a single domain during a user session. All other domains are deactivated by removing power from the hardware components that define the domain. This essentially implements a periods processing technique for domain separation that prevents the data from one domain from being available in another domain. It also makes residual data that might be retained in the host computer's RAM unavailable during the next user session since the host computer is powered off by the operating system within an active domain at the end of each session.

Access to each domain is based on a user identifying and authenticating themselves as an authorized user and then initiating a Hardware Based Access Control (HBAC) process in which the sensitivity level of the domain using hardware based labels and the clearance of the user are compared to determine if the user can be given access. Both the I&A and Access Control process are implemented by the Security Module using user security attribute data entered from the keyboard and read from a user's Smart Card. A user's security clearance, access rights to an operation, and encrypted PIN are stored on their Smart Card which is read and processed by the Secure Microcontroller via the Security Module's Smart Card Reader. The encrypted PIN is compared with a PIN that is entered through the keyboard and encrypted by the Secure Microcontroller. If the PIN is accepted, the password data entered from the keyboard will be compared with a password stored in the Secure Microcontroller to determine if the identified user is authenticated and is allowed to proceed with access control as an authorized user. Any failure of the I&A process will result in a user being relegated to a default state which could be the unrestricted domain or a power off of the host computer depending on what policy the organization wants. The I&A process will only be initiated if the user's Smart Card is identified as valid by the Security Module by comparing the card's Machine Authorization Code against a code stored in the Secure Microcontroller. Failure to validate the Smart Card will be treated as if there is no card present and the Security Module will activate the unrestricted domain.

The Security Module implements the HBAC process that controls the enabling of the hardware based components that define a domain. This is implemented by reading the user's security clearance from their Smart Card and then displaying the available restricted domains based on the domain's sensitivity level being within the security clearance. The selection of a domain will cause the Security Module to read the user's Smart Card a second time to determine the operations that the user is allowed to perform within the domain. These operations can include networking and/or telecommunications and/or Input/Output (I/O). The selection of any, all, or none of these operations will cause the Security Module to determine if the selected domain is available by reading a label from the RHDD installed within the host computer to determine if it matches the sensitivity level of the selected domain. If the sensitivity labels don't match the Security Module will initiate the default state described previously. Even if the sensitivity levels do match, the selected domain will not be enabled unless the ID part of the RHDD label is identical to the ID in the Secure Microcontroller. This ensures that the correct drive with the correct information including operating system, applications software, and restricted data is being made available to the domain user. It should be noted that the ID label is compared in both Security Module and in the RHDD and that if either comparison fails, access to the RHDD is denied. This mechanism also prevents the RHDD from being accessed in any other computer or workstation with a compatible drive bay regardless of whether it has an installed Sentinel Computer Security System. The interface also has some special communications protocol requirements that will prevent it from being easily spoofed.

During the entire I&A and access control process there is no operating system that is active within the computer. This eliminates any possibility of operations being performed within a domain until the user is authorized and their access rights determined. In addition, all information entered from the keyboard and read from the Smart Card is processed by the Secure Microcontroller in the Security Module through the direct hardware interface provided by the Asset Status Sensor and Controller Board. There is absolutely no software or hardware based communications between the TOE and the host computer. This essentially isolates the Security Module and its Secure Microcontroller from attack or interference. In addition, to the isolation of the Security Module and its TSP, the Secure Microcontroller uses encryption, dummy instructions, and tamper proofing to counter any direct attacks against it.

The initiation and setup of a domain by the Secure Microcontroller is implemented so that each active domain and the processes performed therein is isolated from any other domain by controlling the application of power to the hardware components that define the domain. This is done through the design of the Asset Status Sensor and Controller Board within the Security Module, which automatically and simultaneously disables power to the components in the inactive domains when it enables power to the selected active domain. The design ensures that it is physically and electrically impossible to have more than one domain active at any time.

The Security Module also implements an audit capability to record all user I&A and access control operations against the user ID and Time/Date Stamp provided by the Secure Microcontroller's Real Time Clock. This information is stored in an encrypted state within the Secure Microcontroller. The Security Module prevents any authorized user from accessing the audit data but does allow an authorized administrator to download the data in a format that allows it to be easily read and processed outside the TOE. Authorized administrator's are identified from their PIN and their role attribute stored on their Smart Card in the same manner as an authorized user. In addition to downloading audit data, an administrator is also allowed to change or delete the user's PIN from the Security Module. All password modifications, however, are only allowed to be performed by an authorized user after they have been authenticated.

As a hardware based security system that is intentionally isolated from the operations of the computer and its software, it is clear that the Sentinel TOE provides no direct capability to control access to software based operations on specific data at a security level. However, this does not mean that access control to these operations is not being implemented within the TOE. The mechanism for implementing access control to operations such as networking, telecommunications, or I/O within a domain is via the control implemented by the security module over the specific hardware in the domain (RHDD, NIC, Modem, and USB port) that is needed to perform these operations.

The security provided by the HBAC is extremely strong since its isolation from the computer prevents it from being disabled by computer users via their normal user access to the computer and its resources. In general, the closer a security system works to the hardware level

of a network or a computer system the less vulnerable it is to attack. The TOE does not provide access control over all operations within a domain since those operations that can be implemented using the programs and data within an RHDD are allowed if a user has access to the domain. High risk operations such as networking, telecommunications, and I/O in which restricted data within the RHDD could be accessed from or sent to other computers or workstation are controlled to prevent subversion by external threats. A Security Administrator will decide whether these operations are allowed based on the threat environment and the availability of external resources such as SIPRNET or NIPRNET network interfaces, encryption systems, or protected peripheral systems that will allow these operations to be performed at an acceptable level of risk. It should be understood that in most cases the TOE provides no protection outside the computer itself. The one exception is the capability of the TOE to utilize special Fortezza PCMCIA based modem and media encryption systems.

The Sentinel TOE has a physical configuration that essentially consists of a kit or set of hardware components that can be installed into virtually any modern personal computer or workstation in less than two hours. These components consist of the Security Module that is usually installed in an available 5 ¼ inch bay; a removable hard disk drive frame that is installed in a second 5 ¼ inch bay; as many as six (6) Sensor/Controller (S/C) Cards that are installed as interface cards that control the distribution of power from the PCI and ISA slots in the PC motherboard; an I/O controller Board for controlling power to individual USB I/O ports; an LCD Module for displaying security system status data; one or more Non-Volatile Memory (NVM) Control Interfaces for disabling the writing of data to all NVMs embedded in the computer or workstation circuitry that could be shared between security levels; and a Back Panel Assembly for providing USB ports and cable locks. It should be noted that the S/C cards and the I/O Controller board are directly connected via cables to the Security Module which controls their operation with respect to whether they enable or disable power transmission to the devices with which they interface. The S/C Cards are specially designed to operate in a manner similar to an extender card in that they are installed in a PCI or ISA slot in the motherboard and provide a power controlled slot for devices such as NICs, Modems, and PCMCIA Card Readers that would normally be installed directly in the motherboard PCI or ISA slot. The devices that are inserted in the S/C cards are not a part of the TOE but must be installed correctly in the proper configuration for the TOE to correctly implement its TSP. Most of the installed devices have no

specific security capabilities. The one exception is the optional Palladium Secure Modem that is itself an evaluated encryption product that uses the PCMCIA based Fortezza encryption module to encrypt and decrypt modem communications.

The Sentinel Security System has several optional configurations that must be specified by an organization before the system can be installed. These options define the configuration of the firmware in the Secure Microcontroller as well as the number and configuration of operational components such as NICs and modems that need to be included in the kit. One of the options that needs to be defined is whether the default state implemented by the TSP during I&A and Access Control is a power off condition or the unrestricted domain. Another option is a definition as to whether the domains will have specific NICs and modems for each domain or whether these components will be shared by some or all of the domains. For example, if each domain is to have its own dedicated network connection, three NICs will be required and the Secure Microcontroller firmware will need to ensure that only the NIC in the active domain is powered. If each domain will use a single network connection than only one NIC is required and it will be activated when each domain is activated. This configuration assumes that outside the TOE, the external network is running in a system high mode or there is an MLS Network Security System that can apply the required encryption and label processing to the transmitted and received data. These same considerations also apply to the utilization of Modems by the TOE. The USB port configuration is not optional since the TOE provides its own USB ports that are part of the TOE and replace the host computer's I/O ports which become unavailable when the Back Panel Assembly is installed.

It should be noted that the Sentinel TOE has been designed to interface with and utilize kit add-on components that are outside of the TOE but still perform important security related functions. For example, the TOE can interface with and utilize biometrics to further enhance the Identification and Authentication, Access Control, Object Reuse, and Audit processes. The TOE could possibly rely on biometrics for authenticating multiple users who share a single RHDD that is setup for use on multiple computers or workstations. The Biometrics that are currently available for operation with the TOE will consist of fingerprint scanning that is implemented via a fingerprint scanner and the processing software on the users RHDDs. The Sentinel will also

utilize media encryption systems that meet NSA and NIST requirements for the protection of the restricted data stored on the RHDDs. In the case of a classified RHDD the media encryption will consist of the RASP Media Encryption System approved by NSA and based on the use of the Fortezza Card, which will be installed in an optional PCMCIA Card Reader that is installed in an ISA slot and is under the control of the Security Module. Other optional components outside the TOE include the utilization of tamper proof screws to secure the computer case and an external alarm system to deter the unauthorized removal or tampering with the computer and the Sentinel Security System.

Most of the security features of the Sentinel are transparent to the user. In fact, they have been specifically designed to prevent user operations errors that could create security vulnerabilities. For example, mistakes in PIN or Password entry or in the selection of the security level will result in the selection of a default state, which can be either power off or the unrestricted domain. There is also no requirement for the user to learn new programs or operating systems. A computer user can continue to utilize the operating system they are familiar with and all their applications programs in all modes of operation. In fact, any operating system and application program capable of being run on a personal computer can be run on the same computer after the TOE is installed. In some instances use of certain security applications outside the TOE such as RASP may restrict the user to a specific operating system such as Windows NT. This is not a restriction that is based on the Sentinel TOE, however.

1.3 Common Criteria Conformance Claim

This ST conforms to the Common Criteria (CC), Parts 1,2,and 3 and the TSFs included in the ST. The ST is targeted at a generalized but controlled environment with a moderate to high level of risk to the assets. All ST assurance requirements and the minimum strength of function were chosen to be consistent with that level of risk. The assurance level supported by the ST is EAL 4 for the assurance requirements addressed in Chapter 5 and supporting documentation. The minimum strength of function is SOF-medium.

1.4 Conventions

This document is organized based on Annex C of Part 1 of the Common Criteria (see paragraph 1.1, item 4.).

1.5 Terms

This ST uses various terms that are described in this section to aid in the application of the security requirements. It should be noted that to the degree that a definition is available within the Common Criteria it will be utilized. In those cases where no definition for a term is provided in the Common Criteria the author will define the term as it is used within the ST. The substitution of definitions from other documents and security standards such as DoD Directive (DoDD) 5200.28-STD is not allowed if these terms are used to define Security Functional Requirements within Part 2 of the Common Criteria. Such use could and in many cases result in anomalous interpretations of the Security Functional Requirements. An example of this is seen in the definitions for object, subject, and user which are defined differently in the CC and DoDD 5200.28-STD. Where relevant these differences will be identified in the definitions provided for the following terms:

- User
- Authorized User
- Authorized Administrator
- Object
- Subject
- Controlled Object
- Controlled Subject
- TOE Security Function (TSF)
- TOE Security Policy (TSP)
- TSF Scope of Control (TSC)
- Hardware Based Access Control Policy

A *user* is any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

An *authorized user* is a user who may, in accordance with the TSP, perform an operation.

An *authorized administrator* is an authorized individual who has been granted the authority to manage the TOE with respect to controlling audit data and user security attributes but not performing operations. These individuals are expected to use this authority only in the manner prescribed by the guidance given them.

An *object* is an entity within the TSC that contains or receives information and upon which subjects perform operations. Within the context of the TOE, this includes the RHDD, NIC, Modem, I/O ports, CD-ROM, or DVD. All R/W drives with portable media such as an FDD, Zip Drive, R/W CD Drive, R/W DVD Drive are also objects but they are disabled by the TSC during operations in a restricted domain.

A *controlled object* is any object within the TSC that is under the control of the TSP's HBAC TSF. This includes all the objects described above.

A *subject* is an entity within the TSC that causes operations to be performed. Within the context of access control as described in Annex F.1 of CC Part 2, Version 2.1, a *subject* is the 'accessor'. The accessor, as described in this ST consists of an authorized user of the system, as determined from their PIN and Password, in combination with their Smart Card with its stored security attributes that are utilized by the TOE to control an authorized user's access to objects.

A *controlled subject* is any subject within the TSC that is under the control of the TSP's HBAC TSF. Only those users that have been authorized and have been granted access to a restricted domain based on a selected and available set of attributes are controlled *subjects.* A controlled subject assumes the subset of attributes that are available from their Smart Card and are active during a user session. The active attributes are those that are either selected by the user for the duration of the session such as sensitivity level or access rights or those attributes that are invoked due to some external event such as Time of Day.

The *TOE Security Functions (TSF)* are a set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

The *TOE Security Policy (TSP)* is a set of rules that regulate how assets are managed, protected and distributed within a TOE.

The *TSF Scope of Control (TSC)* is the set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

The *Hardware Based Access Control* Policy, also referred to as *HBAC*, is the basic access control policy within the TSP that this TOE enforces over *subjects* and *objects* under its control.

The *HBAC Policy* is the set of rules used to control access to *controlled objects* by *controlled subjects* within a domain at a restricted level of sensitivity based on the subject*'s* active security attributes. Within the context of HBAC as implemented within the TOE all objects within the TSC are hardware based *controlled object*s that are either used to store data or implement data communications via a network, modem, or I/O link. A *controlled subject* is any Authorized User or Authorized Administrator that has a valid Smart Card and has completed the Identification and Authentication process controlled by the TOE. The Authorized Administrator has exclusive access to PIN and Audit Data stored within the Secure Microcontroller but has no access to restricted domains. An Authorized User has no access to PIN and Audit data but is granted access to a restricted domain based on their selected or invoked active security attributes as verified by the HBAC TSF. The controls implemented by the TOE on controlled objects consists of five separate groups that are all under the control of the TOE security functions.

In the first group are data storage and data communications objects that can be accessed by all users in the unrestricted domain. These include the unrestricted Hard Drive, floppy drive, zip type drives DVD, CD, R/W CD, and unrestricted data communications objects such as unclassified modems and NICs.

In the second group are controlled objects consisting of the RHDD data storage object and the NIC, Modem, and USB port data communications objects that are available to authorized users based on their security attributes and the security attributes of the objects. Access to these objects is based on rules that compare the active security attributes of the controlled subject (authorized user) against the security attributes of the controlled object and then grant or deny access in accordance with the results of the comparison. The security attributes associated with the controlled subjects includes: security clearance, object access rights, role, and time of day.

Security attributes associated with controlled objects includes: sensitivity level, access rights, time of day, and in the case of the RHDD the ID code.

In the third group are the controlled objects consisting of all objects that utilize portable R/W media for the reading and writing of stored data. These objects include the floppy disk drive, R/W CD Drive, R/W DVD Drive, and any Zip type drives. All of these drives are disabled by the TSF for all authorized user's of a restricted domain.

In the fourth group are controlled objects consisting of all objects that utilize portable Read-Only media such as the CD or DVD Drives for reading stored data. All of these drives are enabled by the TSF for all authorized users in a restricted or unrestricted domain.

In the fifth group is the Secure Microcontroller that stores User PIN and Audit Data and can only be accessed by an Authorized Administrator.

The HBAC policy implements role based access to the TOE by controlling the security functions that are available to Authorized Administrators as opposed to Authorized Users. A user of the TOE is either recognized as an Authorized User or Authorized Administrator based on the profile on their Smart Card. An Authorized Administrator will not be allowed to gain access to any restricted domain. They will be restricted to selectable functions that include changing or deleting user PINs within the TOE or downloading audit data from the Security Module's Secure Microcontroller.

An Authorized Administrator is also responsible for setting a user's Smart Card PIN and their Security Profile Label through the Audit X Security Administration Tool. This tool is not part of the TOE but is used to support TOE functions. The Audit X Tool is also used to evaluate audit data on the Security Administrator's workstation. This includes the performance of sorts and searches on audit data.

CHAPTER 2. Target of Evaluation Description

2.0 Introduction

This Chapter will provide a complete description of the Sentinel Computer Security System as the TOE. It will include a description of the various subsystems that comprise the Sentinel as well as all of the security functions implemented by these subsystems. The description will be sufficient to support the CC TSFs described in Chapters 4, 5, and 6.

2.1 Applicability of ST

The ST defines a set of security requirements that implement CC based TSFs applicable to countering the threats posed by attacks from organizational insiders in a Government or Industry facility as described in paragraph 1.2.

2.2 Sentinel Implementation

This section presents a comprehensive description of the Sentinel Computer Security System from the implementation perspective. It should be understood that the Sentinel TOE includes a set of kit components needed to implement the TSFs within the TSC and these include the following:

1. Security Module
2. Sensor/Controller Cards
3. I/O Controller Board
4. RHDD Drive Frame
5. LCD Module
6. Back Panel Assembly
7. Tamper Proof Secure Microcontroller
8. NVM Control Interface (as needed)
9. PCMCIA Card Reader (Optional)

2.2.1 Concept of Operations

The Sentinel TOE is a computer security system that uses the principles of HBAC to control access to multiple domains and the controlled objects and controlled subject that perform operations within the domains in a single stand-alone computer or workstation. Each domain is defined by the access controls that are applied by the TSF to the controlled subject (authorized user) and the controlled objects. Controlled objects are comprised of selected computer hardware components that can include hard disk drives, network cards, modems, USB ports, CD Drives, DVD Drives, etc. There are as many as three operational domains, two of which are allocated to the processing of restricted data. A domain is physically isolated from the other domains by means of a periods processing technique that is implemented by a unique domain enabling process that ensures only one domain can possibly be active at any given time. Physical isolation of a domain is achieved by controlling power to the computer components within the domain and disabling the write command for all embedded NVMs shared between domains via the implementation of the TSP.

An authorized user's selection of a domain is limited by that user's security profile as programmed on their Smart Card. This profile defines the allowed security level(s) for the user and the controlled objects used for data communications including the NIC, Modem, and USB ports, that can be accessed at each restricted security level. Some objects such as the DVD or CD Drives are considered to be a low security risk since they can only be used to read data and, therefore, are available to all authorized users within a restricted domain. Other objects such as the FDD, R/W DVD, R/W CD, or any other R/W drives with portable media are considered to present such a high level of risk that the TSF disables these objects for all authorized users in any restricted domain. In addition, any embedded NVM that is shared between domains is prevented from being written to by having its write command disabled in the restricted domains and enabled only in the unrestricted domain by administrator action.

The RHDD is also a R/W drive, but it has some built-in security protection that makes it a much lesser risk than other portable media. In addition, the RHDD is essential to operations in a restricted domain since it stores the operating system, restricted data, and all applications programs that would be needed by an authorized user to perform operations within the domain.

The RHDD is, therefore, available to authorized users of the domain based on rules enforced by the TSP that relate to the security attributes of both the user and the RHDD. These conditions include the following:

1. The user must a clearance equal to the sensitivity level of the RHDD as determined from the clearance attribute on their Smart Card and the electronic sensitivity label within the RHDD.
2. The user must be initiating access to a domain during a time of day when the required clearance is in effect, as defined by the Time of Day attribute.
3. The user must be designated as an authorized user as opposed to an administrator based on the Role Attribute on their Smart Card.
4. The RHDD must have an ID that is accepted by the Secure Microcontroller as being valid.

The other objects that are potentially accessible in a restricted domain are the NIC, Modem, and USB ports. Access to these objects is dependent on first gaining access to the RHDD for the selected domain since the RHDD contains the minimal functionality needed to perform operations within the domain. The user's capability to access the NIC, Modem, and USB ports in a restricted domain is based on the access rights to each object at the sensitivity level of the RHDD. This is determined from the user's access rights for each object as defined by the NIC, Modem, and USB access rights attribute on their Smart Card. These access rights can also be time dependent. This feature allows the user's Smart Card to be programmed with a separate Time of Day attribute for each object such that access to the NIC, Modem, and USB ports can each be based on individual Time of Day settings.

The Time of Day attribute operates the same for controlling access to the RHDD, NIC, Modem, and USB port objects. If a user session is initiated during a time when the RHDD is accessible based on user clearance, it remains accessible for the length of the session even if it goes beyond the allowed time interval. Similarly, the NIC, Modem, and USB port objects can also be accessed for the duration of the session as long as the user's access rights allowed access at the beginning of the session. The time check itself is actually performed immediately prior to enabling the objects which occurs immediately after the selection of the security level and the NIC, Modem, and/or USB options for the selected level. This is known as the time of logon and

is used for comparison with the time of day as established from the Secure Microcontroller's Real Time Clock.

The portion of the security profile that defines the allowed security level(s) of the user is read by the Secure Microcontroller via the Sentinel Smart Card Reader, both of which are located in the Security Module. This occurs after the Smart Card has been validated for operation with the Security Module and the user has been identified and authorized via their PIN and Password. All the allowed levels are then displayed on the LCD module so that the user can select the desired level for that session. When the selection is made, the LCD Module provides the data on the selected level to the Secure Microcontroller which then outputs a discrete signal representative of the selected level to the RHDD via the Asset Status Sensor and Controller Board located in the Security Module. The RHDD then returns a signal to the Secure Microcontroller via the Asset Status Sensor and Controller Board that is representative of its security level. If the returned signal is correct for the level selected the Secure Microcontroller will then proceed to read the ID portion of the security profile label that defines the unique identity of the RHDD. If the ID is found to be valid the Security Module will read the attributes from the Smart Card that define the user's allowed data communications objects at the selected level. The Secure Microcontroller will then generate control signals to activate the RHDD and the allowed data communications objects. These control signals transfer power to the RHDD and the allowed objects for the selected level via the Asset Status Sensor and Controller Board.

In essence, the Sentinel provides one unrestricted computing domain and two separate and physically isolated restricted computing domains that provide the user with the capability to perform the normal desktop operations associated with data processing, networking, and telecommunications at three security levels. The key element is that users can only access one computing domain at a security level at any given time. For example, when in an unrestricted domain the user cannot access any of the computer components or data in the restricted domains. In addition, within each restricted computing domain, a user's access to specific components, other than the hard drive, such as the NICs, modem, or I/O ports are also independently controlled by a profile stored on their Smart Card.

The actual isolation of domains is done through the design of the Asset Status Sensor and controller board which links components assigned to a security level to a common parallel power grid via a series of Normally Closed Relays. In default mode with no relay activation signals power is only available to the unrestricted domain, which includes all the components of the normal PC or workstation. Access to either restricted domain will require the relay connecting power to the unclassified domain to be activated so that power is applied to the selected restricted domain. The restricted domains are connected to power via a common relay so that only one domain can be activated when the relay is in a closed or open position. Within each domain selected components are activated based on the output from relays that are controlled by the Secure Microcontroller. Since the selection of a restricted domain is based on the correct RHDD being available, a domain can consist of only the RHDD and any available Read-Only CD/DVD objects if the other data communications objects in the grid (NIC, Modem, I/O) are not activated. It is clear that the selection of a security level by the user from the security profile on their Smart Card also selects the security level of all controlled objects allowed by the user's security profile. The TSP that is enabled by the operation of the Security Module implements both HBAC and implements isolation between the domains.

The minimum authorized restricted domain for any user is defined by allowing access to only one of the available RHDDs and the available CD/DVD Drives. Each RHDD is set to enable a domain at a specific security level and interfaces with a removable hard disk drive frame that is installed in a 5 ¼ inch bay. When the RHDD is installed into the computer and accessed, signals are generated indicating the security level of the removable drive bay that has been installed. These signals are utilized by the TOE to verify that the security level selected and authorized by the Secure Microcontroller is actually available to the user. If the user has selected and been authorized access to a restricted domain but the required RHDD is not installed, the Secure Microcontroller will implement a default security state. Depending on how the Secure Microcontroller is programmed, the default state will either be the unrestricted domain or a power off condition. In addition, to defining the security level of the RHDD , each removable drive can be electronically keyed to the drive bay and Security Module so that it cannot be installed in any other computer with a compatible drive frame including another Sentinel. This is a useful feature for drives that are to be used by a single or multiple users on one dedicated

computer. In such cases, Biometrics are not needed to control access to the drive since this can be done via the user's Smart Card.

The Security Module is the component of the Sentinel that is primarily responsible for implementing the overall security policy as defined in the ST TSFs. Access to the restricted computing domains is under the control of the Security Module through its implementation of the HBAC Security Policy as programmed in the firmware of the internal Secure Microcontroller. The design of the Security Module has been implemented with the goal of isolating all interfaces to the Security module from the computer operating system and any software. Interfaces with computer components are primarily power controls that are implemented by the internal Secure Microcontroller and transmitted via the Security Module Asset Status Sensor and Controller Board and the cables, S/C Cards, and I/O Controller Board that connect with the hardware based objects to be controlled in each domain. One exception is the NVM Control Interface that disables Write Commands to all NVMs embedded in the host computer or workstation circuitry that is shared between security levels. Updating of the NVM can only be enabled by administrator action in the unrestricted domain. The Security Module, however, has no communications bus or software interfaces with the host computer's CPU, RAM, read/write (R/W) data storage, encryption modules, and network resources. This creates a secure shell that isolates the security module and the overall Sentinel TOE from the characteristic vulnerabilities of software-based security systems.

2.2.2 Sentinel TOE Subsystems

The Sentinel TOE consists of the subsystems, which are described, in detail in the paragraphs below. Figure 1 provides a detailed diagram of the Sentinel installation kit and its component parts while Figure 2 shows the Security Module and its component parts.

A. Security Module

The Security Module as discussed in paragraph 2.1.1 and shown in Figure 2 consists of the Asset Status Sensor and Controller Board, Smart Card Reader, and Security Module Chassis and Front Panel, which includes the LEDs. The Asset Status Sensor and Controller Board, which

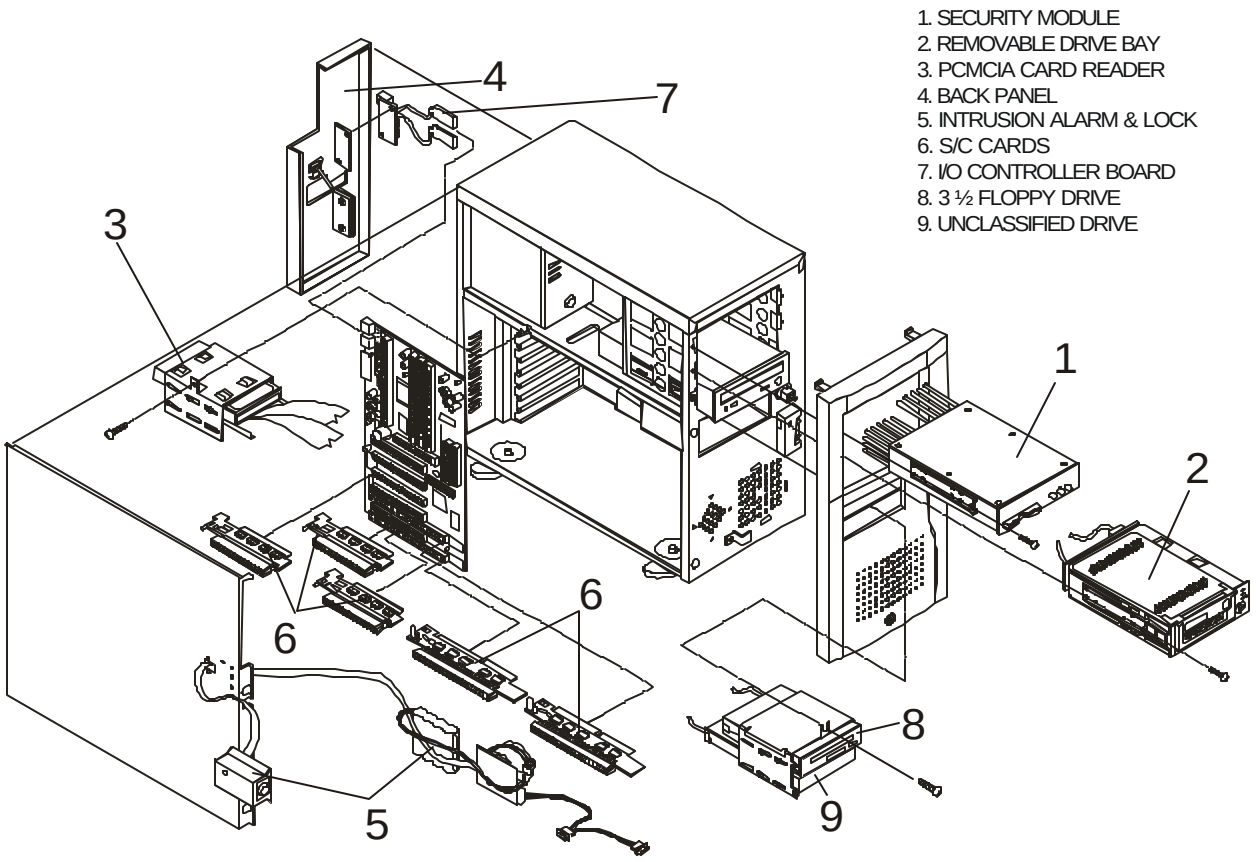
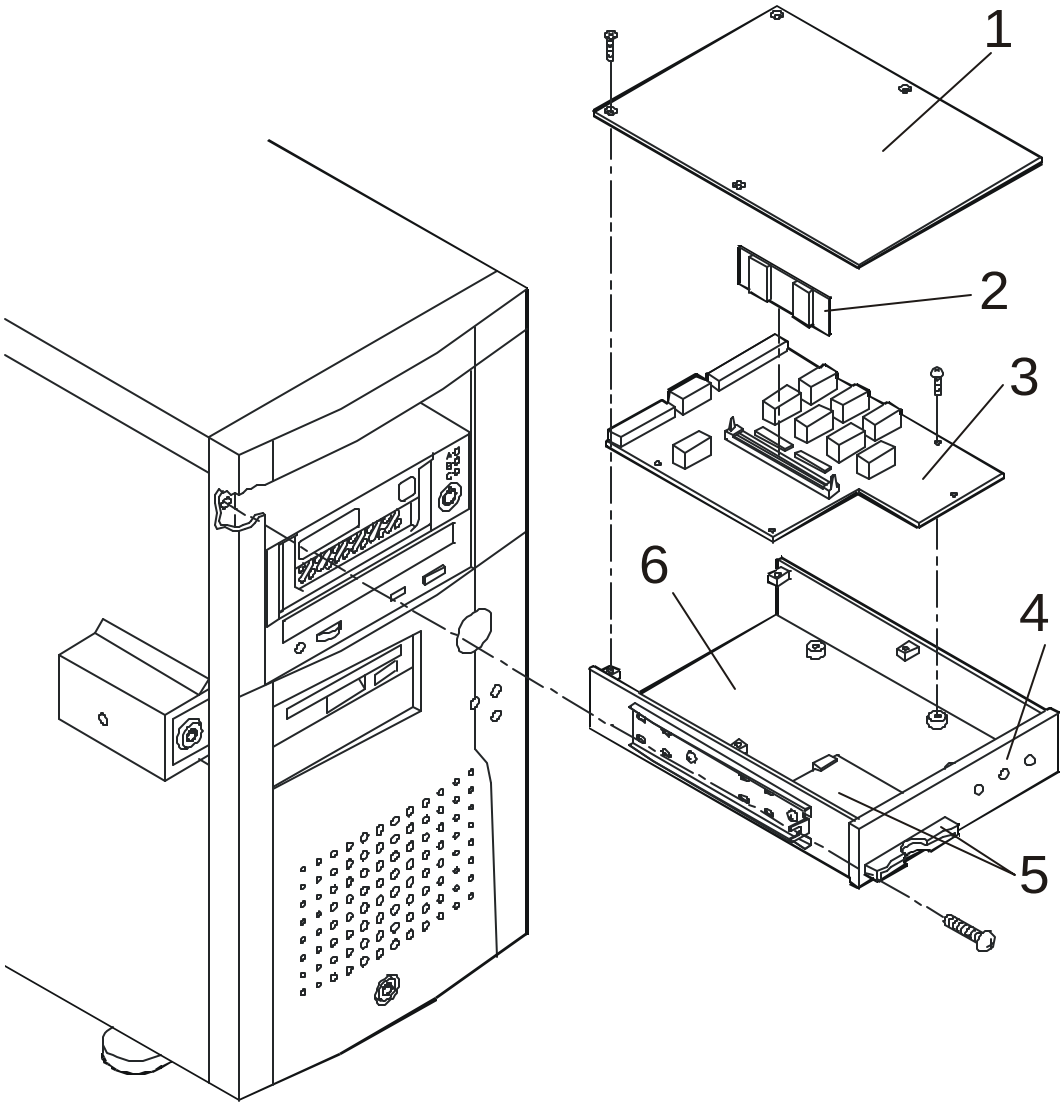


Figure 1 Sentinel Kit Installed in Computer



1. COVER
2. MICRO CONTROLLER
3. ASSET STATUS SENSOR
4. LEDS
5. SMART CARD READER
6. CHASSIS AND FRONT PANEL

Figure 2 Security Module

includes the Secure Microcontroller, is responsible for the activation and control of the hardware based objects that are required for the unrestricted and restricted domains. This circuit board provides the gating via electronic relays, as determined by the Secure Microcontroller generated signals, which allows power to the various computer components that comprise that controlled objects within a domain. At start up, the Asset Status Sensor and Controller Board holds the computer mother board in a reset state thereby restricting access to other computer components while providing the isolation necessary for the I&A and access control processes to be completed. The keyboard and Smart Card Reader interfaces used to enter user profile information and the data and commands used during I&A and access control are connected to the Asset Status Sensor and Controller Board during the entire I&A and access control process. The status data and selection choices needed by the user during I&A and access control are displayed on the LCD Module. Upon successful completion of the I&A and access control process, power is gated to the required hardware based objects for the selected authorized domain in accordance with the security profile programmed on the Smart Card. In addition, the Secure Microcontroller releases the reset allowing the operating system and any application software on the selected hard drive to initialize. The Secure Microcontroller also switches the keyboard and Smart Card Reader bus interfaces from the Asset Status Sensor and Controller Board to the motherboard so that they can be accessed by the operating system and the appropriate applications programs after completion of the I&A and access control processing.

When the computer is first powered on, the Asset Status Sensor and Controller Board allows power to only the Smart Card Reader, LCD Module, LEDs, and keyboard and directly latches them to the Secure Microcontroller. The Secure Microcontroller uses a direct interface to receive and transmit data directly with the Smart Card Reader, LCD Module, and LEDs. All the functions for I&A and access control are then performed by the Secure Microcontroller before allowing power to any assets. The Smart Card Reader, LCD Module, LEDs and keyboard are, thereafter, accessed as needed during the I&A and access control operations.

During initial computer power up, the first action initiated by the Secure Microcontroller is checking the Smart Card Reader for insertion of a valid Smart Card. Each Sentinel Secure Microcontroller is programmed with a set of codes called Machine Authorization Codes that

must match the codes programmed on a Smart Card for it to be recognized as valid. A user's card will usually have a single Machine Authorization Code that represents the computer that has been assigned to them. All codes stored in the Secure Microcontroller are stored in an encrypted format. The Secure Microcontroller also detects the status of the removable drive bay to determine the security level of the installed RHDD. A RHDD at a restricted level has an electronic label that will only recognize and enable signals from the Secure Microcontroller that select the domain for that same restricted level. Any other signals, such as those for enabling a different domain, will be disabled by the label. If the security level selection signal from the Secure Microcontroller is not enabled by the RHDD that is present, the computer will either default to the unrestricted domain or power off depending on the option selected by the customer. The RHDD is also interrogated by the Secure Microcontroller to determine if the ID within the RHDD is valid with respect to the RHDD IDs stored in the Secure Microcontroller. An invalid ID will prevent the RHDD from being recognized and the default state will be initiated.

In addition to the user's PIN, the codes programmed on the Smart Card consist of the user security profiles and the Machine Authorization Code. A user security profile consists of the users authorized security level and the computer components (NIC, Modem, USB Ports) that are available to the authorized user as data communications objects at that level. An initial password is also programmed into the Secure Microcontroller of all new Sentinels and this password is also issued to new users. During initial setup of a machine for a user, the Security Administrator will assign and link the user's PIN to the password in the Secure Microcontroller. After the new user initializes his Smart Card with the first use, they will be prompted by the LCD Module to change their password. This changed value is then stored in the Secure Microcontroller in an encrypted format, time stamped, and used for future comparisons.

The Secure Microcontroller first compares the Smart Card Machine Authorization Code to the Machine Authorization Code stored in the Secure Microcontroller memory to ensure that the inserted card is valid for the machine chosen. A user validates his PIN, password, and security profile by entering them on the keyboard when prompted by the LCD module. The Secure Microcontroller compares the entered password and PIN values with the password value stored in its memory and the PIN value stored on the Smart Card. When all values are verified,

the Secure Microcontroller sends the proper signals to the Asset Status Sensor and Controller Board components for enabling signals to the selected hardware based objects that define the domain. If a failure (either by incorrect user keyboard entries or card removal) occurs during the I&A and access control the Asset Status Sensor and Controller Board will not allow a power–up of any computer components and will enable the defined default state.

The Secure Microcontroller continues to poll the Smart Card and perform comparisons intermittently throughout the time that the card is inserted in the machine to ensure that the card is not removed and another card inserted. After the I&A and access control procedures are completed, and the selected system has booted up, the operating system of the associated drive may continue to interact with the Smart Card if the Smart Card Reader is setup as a recognized device for the operating system. In any case the Secure Microcontroller will continue to monitor the presence of the card and will initiate a system reset if the card is removed.

If upon power up, there is no Smart Card detected in the reader, the Secure Microcontroller will enable the Asset Status Sensor and Controller Board to allow only unrestricted operations. The Asset Status Sensor and Controller Board will gate signals to those unrestricted components determined to be available (such as the computer internal hard drive, R/W drives, unrestricted NIC, and I/O ports) for unrestricted operations. Power will also be supplied to the green LED on the Security Module for indication of unrestricted operations.

As stated previously, If the security level selection signal generated by the Secure Microcontroller in response to the profile on the Smart Card is not enabled by the removable drive that is present, the computer will either default to unrestricted operation or power off depending on the option selected by the customer. This condition will also be indicated by the fact that the green LED will be illuminated, the LCD will display the selected security level, and the computer will power off or default to an unrestricted state.

In addition to controlling the selection and implementation of security profiles the Security Module also stores and controls access to all security event audit data. The Security Administrator’s Smart Card will be programmed with a role attribute that allows for retrieval of the audit data stored within the Secure Microcontroller memory. This data is stored in an

encrypted format. When the audit data capacity reaches a preprogrammed limit, the Secure Microcontroller will issue a warning message for display on the LCD Module that will request the user to notify the Security Administrator so that the data can be downloaded and the memory cleared. The Security Administrator's Smart Card will be used to receive and store the downloaded audit data.

After Smart Card I&A, the Security Administrator will select the Download Audit Data option as displayed on the LCD Module. The Secure Microcontroller will then send a signal to the Asset Status Sensor and Controller Board, which will latch the internal Smart Card Reader directly to the Secure Microcontroller. The Secure Microcontroller then downloads the stored audit data. Upon completion of the download, the Secure Microcontroller audit data memory space is initialized and new audit data can now be captured.

B. Removable 5 ¼ Inch Drive Bays

Although an RHDD can be setup in either of two restricted security levels, the construction of both is essentially the same. The RHDDs consist of a drive bay frame and tray that house a 3.5 inch hard drive. This drive stores the data at a restricted security level; the operating system to be used at that level; and all applications software. A security level detection system in the RHDD replicates the security level detection signal from the Secure Microcontroller and returns it for comparison if the RHDD is at the security level selected by the user. The returned signal must be present and identical to the signal that was sent for the selected security level to be enabled. If no signal or the wrong signal is returned, the Secure Microcontroller will enable the default state, which is either the unrestricted domain or a power off condition.

In addition to the drive's security level, each RHDD can be electronically keyed to a drive bay and the Security Module within a computer so that the drive cannot be used in any other drive bay. The keying is enabled by a microcontroller in the RHDD that outputs a unique ID word to the Secure Microcontroller in the Security Module. If the transmitted ID word is identical to an ID word stored in the Secure Microcontroller the RHDD is recognized as being valid and is enabled, otherwise it is disabled. This keying mechanism is primarily useful in dedicating a specific RHDD to a user or group of users for operations at a specific security level

in a specific computer. This absolutely prevents the drive from being used in any other computer where it could be accessed by other users. Additional protection is provided against gaining the ID by using a special communications protocol that must be duplicated exactly for the ID word to be recognized.

The RHDD can only be installed in a computer by inserting the drive in the drive bay and locking it in place with the mechanical drive bay lock. If at any time during operations, the RHDD is unlocked with the drive bay key, the hard drive will dismount and the system will lock up. If the RHDD utilizes media encryption to provide additional protection for the restricted data on the drive, the sudden lockup could prevent some of the data from being encrypted. In such cases the system must be powered off, the drive must be locked, the computer restarted and all I&A and Access Control procedures performed again in order to resume operations.

C. Sensor/Controller and I/O Controller Cards

This subsystem can consist of one or more or a mix of PCI Sensor/Controller (S/C) Cards, ISA Sensor/Controller (S/C) Cards and the I/O Controller Card used to control access to various hardware components that comprise controlled objects. These cards allow the Security Module to control the hardware based controlled objects interfaced with these cards which include NICs, Modems, USB ports, and the optional PCMCIA Card Readers. The PCI and ISA S/C Cards are mounted on the motherboard of the personal computer and interface the Asset Status Sensor and Controller Board with the computer NICs, modem, and the optional PCMCIA Card Reader. The I/O Controller Card is mounted to the Rear Panel Cable Lock Shield and interfaces the Asset Status Sensor and Controller Board with any equipment attached at the USB ports. When the security profile indicated by the inserted Smart Card enables a domain that requires those hardware based objects interfaced to the PCI and ISA S/C Cards or I/O Controller Card, the Asset Status Sensor and Controller Board gates power on signals to these components as directed by the Secure Microcontroller. The PCI and ISA S/C Cards and I/O controller Cards route these signals allowing their interfaced components to power up and begin operations. It should be noted, that in some instances a modem or other controlled device such as a NIC may

be in a PCMCIA card configuration which will require the use of a controlled PCMCIA Card Reader. It is for this reason that the PCMCIA Card Reader is optional within the TOE.

D. LCD Module

The LCD Module consists of a display module with an internal LCD and a microcontroller, which reads and converts keyboard inputs to hexadecimal codes. These hexadecimal codes are sent to the Secure Microcontroller which interprets them as PIN, password, or security profile selection codes used during the I&A and access control processes. The microcontroller in the LCD module also accepts response data from the Secure Microcontroller and displays it on the internal LCD to support the user interface during the I&A, access control, and audit processes.

E. Back Panel Assembly

The Back Panel Assembly is mounted over the original PC or Workstation I/O Panel. It incorporates two USB ports and a Cable Lock Shield that makes it virtually impossible to switch cables or attach unauthorized cables to the USB I/O ports and NIC interfaces. This is accomplished by installing the shield over the connections of the rear panel of the computer. The shield is secured to the case with intrusion proof screws that are installed from inside the case.

F. NVM Control Interface

The NVM Control Interface consists of a standard Integrated Circuit IC Test Clip that is attached to any Non-Volatile Memory (NVM) that must have its Write Command disabled when a user is operating in a restricted or unrestricted domain. All pins on the IC that disable the Write Command are connected via a set of wires or cable from the IC Test Clip to the Security Module. The Security Module generates the signals to disable the Write Command in all domains for each NVM that is accessible to multiple security levels. This would generally include any NVMs embedded in the host computer or workstation BIOS, Video, or Audio Circuitry. NVMs that are already controlled by the Security Module such as those on a NIC or Modem are not connected to this interface. The NVMs can only be enabled for write updates by the action of the Security Administrator who can select the BIOS Update option after login with their Administrator Smart Card. This option will enable the NVM write capability for as long as the Administrator’s Smart

Card is in the Security Module Card Reader. This allows for the updating of NVMs as necessary by the Security Administrator. Removal of the Smart Card will cause the NVM write Update to be disabled.

G. Tamper Protection

Tamper proofing for elements of the Sentinel within the TOE includes the use of tamper proof screws for securing the Back Panel Assembly to the PC or Workstation casing. The Secure Microcontroller has some special tamper proofing that will erase the program and all stored data if any attempts are made to strip its casing. In addition, the Secure Microcontroller also encrypts its program and data when it is powered off. During operation, the Secure Microcontroller adds dummy instructions while it is implementing its program so that there is no way to monitor the actual instruction sequence.

2.2.3 Sentinel Kit Add-On Components

Sentinel kit add-on components include those components that are outside the TOE but provide some capability or function that is either acted on by the TOE; supports the management of the TOE; or enhances the operation of the TOE. These components are described in the paragraphs below.

A. PCMCIA Card Reader Assembly

The PCMCIA Card Reader Assembly is primarily utilized for housing and interfacing with the PCMCIA based encryption or secure modem PCMCIA based modules such as Fortezza Card or the Palladium Secure Modem Card, respectively. Encryption of restricted media at the classified level requires the use of the RASP system, which has been certified by NSA and requires the utilization of the Fortezza Card. The Palladium Secure Modem Card is based on the use of Fortezza to restricted level telecommunications.

Power is provided to the PCMCIA Card Reader via the Asset Status Sensor and Controller Board after the security profile selection for the enabling of a restricted domain is confirmed by the Secure Microcontroller. The power to support the reader is routed from the

associated circuitry and components controlled by the enabled security level detection signal and the other signals generated by the Secure Microcontroller to enable the components defined within the selected restricted domain. An ISA based S/C Card is used to control power to the reader at the host PC/Workstations motherboard.

B. PCI or ISA Based NIC and Modem Cards

Both the Modem used for unrestricted communications and the NIC cards are PCI or ISA based commercial products that are installed in PCI or ISA S/C cards so that they can be controlled by the Security Module. There is generally no restriction on the type of NIC or Modem Card that can be used as long as it can be installed in a typical PC/Workstation 32 bit PCI slot or 16 bit ISA slot. While these cards are not part of the TOE, they perform networking and telecommunications functions under the control of the TOE. In normal operation each NIC is assigned to a specific domain with two of the NICs being dedicated to the restricted domains and the other being assigned to the unrestricted domain. During installation the NICs are assigned to those three S/Cs that are pre-assigned for NICs. The only differences in the NICs would be those required for proper operation with the external network used to support each domain. For example, the configuration (Ethernet, ATM, Token Ring) and speed of the external networks could require differences in the type of NIC used.

The Modem Card is installed for telecommunications in the unrestricted domain and is installed in an S/C Card that is controlled by the Security Module so that it can only be activated during operations in that domain. Again, the Modem Card can be virtually any commercially available modem that is compatible with a 16 bit ISA slot or a 32 bit PCI slot. It should be noted that during setup the cable interface between the S/C cards and the Security Module is tagged so that the proper components are installed with each S/C Card and cable. This is also checked after installation to ensure that there is no mistake. In addition, the external interfaces for the NICs and Modems are color coded so that the external connections are correct. In addition, the current PCI S/C Cards are setup for 32 bit PCI since this is the PCI slot used in virtually all commercially available motherboards. However, a 64 bit PCI based S/C Card has already been designed and will be available when the 64 bit PCI slots are introduced.

C. Computer Disk Drives

All Disk Drives within the computer including the internal computer HDD, RHDDs, CDs, DVDs, FDD, and Zip type drives are controlled objects that are outside the TOE but are controlled by the TOE. The Security Module implements control over user access to these objects through its control over the power circuits that enable these devices. Operations within a restricted domain will cause all R/W disk drives, with the exception of the RHDD designated for the selected domain, to be disabled. The computer CD and DVD drives that are of a Read-Only Configuration will generally be enabled for all domains including the restricted domain. This can be changed, however, if an organization's security policy requires such drives to be disabled when operating in either or both restricted domains. In such cases, the drive is connected to a power circuit controlled by the security module and the firmware within the Secure Microcontroller is written such that power is controlled based on the access rules that the organization requires. If an object such as a Read-Only CD or DVD is determined to be accessible in all domains it will not be connected to the Security Module.

D. Audit X Administration Tool

The Security Administration requirements for the Sentinel are for the most part outside the TOE but are necessary to support TOE functions such as Audit, Identification &Authentication (I&A), and Access Control. Certain functions such as changing or removing a user PIN or downloading audit data are within the TOE and are described in Section 2.2. Those administrative functions that are outside the TOE include programming user Smart Cards with their initial PIN and their Security Profiles; updating PINs and profiles on the Smart Cards when necessary; and evaluating all audit data recorded by the Security Module. These functions can be supported using the Audit-X Administration Tool developed to specifically support the Sentinel TOE.

The Sentinel Audit-X is a Windows based application that can be loaded on virtually any PC/Workstation via the CD/DVD Drive. Audit X allows the Security Administrator to reprogram user Smart Card data including their PIN and Security Profiles in seconds from their PC or workstation. The program itself has a Graphic User Interface that is easy to use and interactive to

allow the user to easily select and perform the desired operations with minimal training. After selecting the PIN and/or security profile data to be stored on the card the Security Administrator will insert the Smart Card into a Smart Card Reader/Writer connected to their PC/Workstation and will initiate the programming sequence. The card will then be updated and the success or failure of the operation is indicated. Active Smart Cards can also be scanned to verify that the programmed data is correct.

The Audit-X Tool can also be used to load the audit data from a Sentinel via the Security Administrator's Smart Card and then evaluate the data to identify and analyze the recorded events. Loading the audit data is done via the Smart Card Reader/Writer which inputs the data, which is in a CSV file format into a database via a script within the Audit-X Program. The audit data processing capability of the tool allows the Security Administrator to perform sorts and searches against audit data fields such as PIN, domain selected, event failures, type of event, date and time, etc. Preformatted or user definable audit reports can then be generated that identify any security events that might require further attention.

Since the operations performed by the Security Administrator in administering PINs, security profiles, and audit data are extremely sensitive it is recommended that these operations be performed on a workstation with the proper security protection. A Sentinel protected PC or Workstation dedicated to an authorized Security Administrator could be easily setup to provide this security. All Smart Card programming and Audit Data Processing should be implemented within a restricted domain. In addition the workstation and the Security Administrator's Smart Card would be linked via a unique Machine Authorization Code so that only that card could be utilized to access the workstation.

E. Biometrics

The Sentinel is setup to use Biometrics as an add-on I&A and access control capability for operations within a restricted domain once the domain has been established by the Security Module. In most instances the Biometrics will consist of user fingerprint profiles that are created by a Fingerprint Scanner and then stored on the RHDD for each domain that the users will access. The scanner can easily be connected to one of the two USB ports that are under the control of the Security Module via the I/O Controller Card. Activation of the appropriate USB

Port will enable the operation of the Fingerprint Scanner as a component that interfaces with the selected domain in the same manner that a NIC interfaces with a domain. The Fingerprint Scanner would also require the appropriate application software to be loaded on the RHDD that is activated for operation in the domain.

The capability for biometrics can enhance various security capabilities including I&A, Access Control, and Audit. Although it is not a component of the TOE, a Commercial-Off-The-Shelf (COTS) scanner such as the Ethenticator can be utilized to support the TOE I&A process, as well as, providing additional access control to the data files and programs within a restricted domain. In essence the fingerprint profile would replace a user's password for controlling access to the RHDD and all files and programs on the RHDD that were password controlled. This capability could also be tied into the NT File System (NTFS) capabilities of Windows NT and Windows 2000 to provide an additional level of access control and audit capability within the domain.

F. Encryption

Encryption, in itself is not part of the Sentinel TOE. However, the Sentinel has been designed to utilize both media and telecommunication encryption systems. The data stored in the RHDDs and/or transmitted via modem is capable of being encrypted if the proper encryption modules are installed in the Sentinel. In the case of media encryption for a classified level RHDD, the RASP® product is used since it is the only available product approved by NSA for the protection of classified media. The RASP® product includes software and drivers that are installed on the classified RHDD and a Fortezza PCMCIA Card that is installed in the PCMCIA Card Reader located in the PCMCIA Card Reader Assembly. RASP® uses the Fortezza Type 2 encryption module (based on a public algorithm and secret key) that is implemented on the Fortezza PCMCIA Card. Media encryption for sensitive level data requires the use of an encryption product that has been evaluated by NIST as being FIPS 140 compliant. There are several software based encryption products that meet this requirement and can be loaded on the RHDD used for data processing in restricted domains at a security level lower than classified.

The Sentinel also has the capability for data encryption for both classified and sensitive data transmitted via a modem. This capability is available via the Palladium® Secure Modem, which also utilizes the Fortezza encryption module implemented in a PCMCIA Card format. The Palladium® is also installed in the PCMCIA Card Reader located in the PCMCIA Card Reader Assembly. When used for encrypting classified data, the Palladium must be coupled with the Optiva®server hardware outside the PC. This hardware is not required when the Palladium® is used for sensitive level data communications.

The Sentinel currently provides no encryption capability for network communications since it is assumed that this is provided for on the dedicated NIC interfaces with classified and sensitive level networks such as the NIPRNET and SIPRNET. Future enhancements, however, may include the incorporation of a multi-level/multi-category VPN that will eliminate the need for multiple NICs and will allow network communications at all levels over a single NIC. The capability to provide this capability for classified data will depend on the availability of a Type I encryption capability.

G. Physical Protection

The Sentinel utilizes various methods of protecting its subsystems and components against attempts at tampering with or disabling their security. Some of these methods are outside the TOE including an optional intrusion alarm system that activates if the computer case is opened or moved in an unauthorized manner. To deactivate the intrusion alarm, the alarm key must be inserted into the locking mechanism located on the side panel of the computer and turned. The intrusion alarm also has a battery pack located inside the case that powers the intrusion alarm even when power is removed from the Sentinel. Additional protection against intrusion into the case is provided by intrusion prevention screws that prevent the case from being opened without a special tool.

2.3 TOE Functional Description

This section presents a comprehensive description of the Sentinel Computer Security System from a functional perspective. All of the described functions are included within the ST TSFs and the TOE.

2.3.1 Security Functions

The Sentinel implements the basic security functions and policy described in the paragraphs below.

A. Identification and Authentication (I&A) Function

The Sentinel TOE I&A security function is required for access to restricted domains and is based on the use of a token in the form of a Smart Card with a stored encrypted PIN, a Machine Authorization Code, and user security profiles applicable to the Smart Card owner. It should be noted that access to the unrestricted domain is not controlled by the Sentinel, although other security systems such as those enabled by the operating system may be in place for access to this domain. The I&A process for access to restricted domains begins with the recognition of the card at power on when the Security Module compares the Machine Authorization Code with a code stored in the Secure Microcontroller to determine if the Smart Card is authorized for use in that specific PC or Workstation. This is done to ensure that the card owner can only be authorized for operation on a computer with the same Machine Authorization Code as that on the owner's' Smart Card. It also virtually eliminates the likelihood of unauthorized use by an outsider or an insider with a different Smart Card.

Once the Smart Card is recognized as authorized, the user is requested, via the LCD Module, to identify themselves by entering an unencrypted PIN of at least 6 alphanumeric characters in length from the keyboard. This PIN is then encrypted by the Secure Microcontroller and compared with the encrypted PIN stored on the Smart Card. If there is a match, the user is then requested, via the LCD Module, to enter a password from the keyboard that is at least 8 alphanumeric characters in length. This password is then compared with the password stored in the Secure Microcontroller that is linked to the entered PIN. If a match exists the user is identified and authorized to select one of the displayed security profiles stored on the user's Smart Card.

All PIN and Password entries appear as a series of asterisks on the LCD Module so that the actual values are never displayed. In addition, there is no feedback provided about the

required length of the password or PIN or if certain characters or types of characters are not allowed. The only message on PIN or password entry is that a user must repeat the entry process for PINs or passwords that are not accepted. All user PINs are maintained by the Security Administrator who periodically changes them. Passwords, however, are under the control of the user who can change the password as part of the login process and in fact is required to so during their first login to a Security Module. This process protects the Security Module I&A process so that only the user has access to all the required authentication data. The Security Module also eliminates the possibility of certain password vulnerabilities by preventing a selected password from being the same as the current password or the same as the user's PIN.

The overall I&A policy enforced by the Security Module is based on something the user has (Smart Card) and something the user knows (PIN and password). This policy is enhanced by linking the Smart Card to a specific computer, encrypting the PIN and storing it on the Smart Card. So if the Smart Card is lost, the PIN would be difficult to determine without breaking the card and knowing: a) that the PIN was encrypted; b) the encryption algorithm; and c) the encryption key. A further enhancement is that the password is stored within the Secure Microcontroller in encrypted form until needed. This essentially separates the location of the stored PIN and password and reduces the potential for theft and recovery of both. Additional protection is provided through the utilization of Smart Cards such as those from Spyrus® and Litronic®, which have built in tamper protection

The vulnerabilities in password management are reduced within the Sentinel TOE through a security policy that forces the user to select an initial password during first time login that has minimum length requirements of 8 characters. This forced password change process virtually eliminates the possibility of anyone knowing the password other than the user since it is under the sole control of the user after the initial change. Only the user can change the password, thereafter, and this should be done at least every 90 days. The Sentinel will also not allow a user to select a password identical to the PIN or the same as the current password.

At the physical level, all I&A functions including keyboard entries, command and data display, and Smart Card processes are independent of the computer operating system and associated applications software. The computer keyboard, LCD Module, and Smart Card Reader

have a direct hardware interface with the Security Module during the I&A process. This eliminates potential vulnerabilities based on security holes in the operating system and software that could allow password and PIN data to be intercepted and compromised. In addition, all I&A functions are performed before the computer is powered on to eliminate real-time password or PIN capture via an external computer port.

B. Access Control Function

The access control function is based on a HBAC Security Policy. The basic security within this policy is based on the fact that it is implemented from the user security profile stored on the user's Smart Card. A security profile consists of a user's security attributes including security clearance, access rights, role, and any time dependencies that modify other security attributes. All security attributes are defined independently by the Security Administrator and not the user. This removes the capability of the user to define their own policy, thereby, restricting access based on the security attributes identified by a neutral trusted party. The security of the access control process is also linked to the inherent security of the Smart Card token that defines a users security attributes and the fact that the Smart Card can only be programmed by an authorized Security Administrator. The Smart Card is also linked to both the user through the user's PIN that is stored on the card, and to the TOE through the Machine Authorization Code on the card that is linked to the same code stored in the Secure Microcontroller.

Another important factor in the HBAC policy is the independence of access control from the vulnerabilities of the operating system and applications software. All access control functions are implemented in hardware within the Security Module thus eliminating the inherent vulnerabilities in software based access control systems. Access is controlled to restricted hardware based domains consisting of controlled data objects as implemented by an RHDD, data communications objects consisting of the NIC, modem, and USB ports, and the available Read-Only Disk Drives such as the CD or DVD Drives. At a minimum the objects within a restricted domain can consist of just the RHDD which has a hardware label that defines its sensitivity level. Access to a domain is based on a user having a clearance level attribute that is equal to the sensitivity level attribute of the domain's RHDD. If an authorized user acting as a controlled

subject also has access rights to other controlled objects within the domain, access will be available to these objects and the operations that they entail. The controlled subject consisting of an authorized user is controlled through their password and the PIN and the active security attributes selected by the user from their Smart Card such that the attributes defining a user's clearance must equal the sensitivity level of all objects. This will ensure that all the controlled objects and subject that implement operations in the domain must have the same sensitivity level.

The actual implementation of HBAC is under the control of the Security Module which functions under the commands implemented within the Secure Microcontroller firmware. These commands comprise a set of TSFs within the overall TSP that are based on rules for:

1. Identifying the active security attributes of authorized users acting as a subject;

2. Identifying the security attributes of controlled hardware based objects;

3. Defining a restricted domain based on the security attributes of controlled objects and the controlled subject;

4. Processing the security attributes of controlled objects and controlled subjects to determine if access is granted to a restricted domain.

The actual selection and enabling of the controlled objects within a restricted domain is implemented by the Asset Status Sensor and Controller Board in the Security Module. This is controlled by the Secure Microcontroller on the Asset Status Sensor and Controller Board, which processes the profile selection inputs from the authorized user; the user attribute data from the user's Smart Card; and the attribute data provided by the hardware based labels of the objects against the rules in the TSP. The Secure Microcontroller then configures the control outputs from the Asset Status Sensor and Controller Board to enable the appropriate RHDD data storage object and the NIC, Modem, and/or USB port data communications objects within the authorized domain. All other R/W data storage objects within the computer are disabled by the Security Module if either restricted domain is enabled.

The Asset Status Sensor and Controller Board has also been designed so that any component failures including the failure of the Secure Microcontroller cannot enable access to a

domain at a higher security level than the selected domain. The failsafe mechanisms built into the board will prevent the failure of any component on the board from switching security levels after completion of successful login to a restricted domain. At the very worst a failure after login could cause a system lockup in which access to any restricted domain is denied until the system is powered off and the logon process for a restricted domain is repeated. If during subsequent login the indicator lights are incorrect a "hard" failure would have occurred and maintenance will be required. Even should this go unnoticed there is no way for the TSP to be violated since the level detection or ID validation circuitry in the RHDD would absolutely prevent this. Power failures to the Security Module that did not also effect the host computer during login to a restricted domain would lockout access to all restricted domains. If the power failure occurred after login to a restricted domain the RHDD would lockup. In addition to the Asset Status Sensor and Controller Board other key level selecting components such as the S/C and I/O controller cards are also designed to fail in the power off mode so that a "hard" failure of the card isolates the component controlled by the card. Other types of failures in the S/C card are certain to effect signal lines between the motherboard and the inserted device, which would certainly disable their operation. In reality it would take a statistically remote, if not impossible, combination of failures in the Security Module and the RHDD combined with some negligent or malicious activity of a user to violate the TSP.

In essence the Security Module provides access control to a domain at a selected and authorized security level. The Security Module also controls access to all the controlled objects consisting of the RHDDs, NICs, Modems, USB ports, and all other R/W Disk Drives in the computer. Access to the RHDD and NIC, Modem, and USB port controlled objects that define a domain is implemented through attribute based access control rules implemented by HBAC. This process is embedded in the TSP and requires the Security Module to compare the clearance and access rights of an authorized user acting as a subject with the sensitivity level and access requirements of the controlled objects within a selected domain. Since an exact match is required, there is no hierarchical policy in which access to a higher security level automatically implies access to a lower security level. This is unnecessary in a periods processing system in any case since a user can only gain access to one level during each user session.

A key benefit of the HBAC policy is its control over the host PC or workstation external interfaces such as the USB ports on the back panel used for I/O and the NICs used for network communications. These interfaces are controlled in the restricted domains through the selection of a security profile. If the user profile permits access to USB and/or the NIC interfaces as part of a user domain, these interfaces can be made available by the appropriate programming of their Smart Card. In the case of the USB enabled I/O operations, use should be restricted to printer operations or to support security add-ons such as Biometrics sensors. Printer operations should only be enabled if the printer is located in a controlled and secure location. The NIC interface and networking software should only be activated for the restricted domains if the user has access to a network with the appropriate protection level for the security level of the data within the domain.

The Security Module is also capable of implementing access control for individual users based on the time of day. This capability is implemented by designating the time of day during which a user can access designated security levels and/or the available processing components at each level. To do this the Security Administrator programs the user's Smart Card to allow the level and categories of access based on the time of day. The Security Module then utilizes this information during login along with the time of day information from the Secure Microcontroller's Real Time Clock to setup the access that will be granted to the various components to support networking, telecommunications, or I/O within the host PC or workstation. It should be noted that the Security Module will use this information during login to determine access to the RHDD, NIC, Modem, and/or USB ports for the duration of the session. This will ensure that a user's access will not be terminated to any object during a user session as long as access was granted during the initiation of the session. The decision on access is based on the actual time of day as determined from the Real Time Clock when access is to be granted or denied for each object. This is known as the time of logon and is indicated on the Security Module by the illumination of the LED indicating the level of restricted access that is allowed. The capability to control the access of authorized users based on time of day is a useful environmental constraint for restricting operations during periods when security administration or physical security is at a minimum.

The HBAC access control policy implemented by the TSP is ideal for a single user who has control over all the objects within the computer or workstation. In such an environment the authorized user would have control of the RHDD data storage object at a designated sensitivity level. The user would also have access to controlled data communications objects at that same sensitivity level through their access rights to hardware components such as NICs, Modems, and USB ports. Access restrictions to objects is strengthened to eliminate any vulnerabilities by keying the restricted RHDDs to a specific computer or workstation. This is done by creating a unique ID word for each drive that must be recognized by the Security Module for the drive to be utilized in a restricted domain.

C. Object Reuse Function

In a single user environment in which only one user is assigned to a PC, object reuse is not an issue for those objects within the PC's restricted domains since only one user can access these objects in any domain. The Sentinel's isolation of each domain through its periods processing mode of operation and its disabling of any write operations to embedded Non-Volatile Memories (NVMs) essentially eliminates the possibility of data objects in one domain from being accessed in another domain. This isolation consists of first deactivating all computer data storage components other than the designated RHDDs that have a non-volatile storage capability when operating in any restricted domain. Under this policy, all computer R/W drives or devices other than the RHDD that is authorized for operations in the selected restricted domain would be disabled. In addition, switching from any domain to another domain requires the computer to be powered off and then back on while one operating system is logged off on one hard drive and another is then logged on. This power transition clears all volatile memory such as RAM that might be shared between the domains. Any NVMs that are embedded in the host computer or workstation such as those used by the BIOS or by devices that are shared between domains will have their Write Command deactivated through signals from the Security Module when a user is operating in any domain. These same devices can be written to in the unrestricted domain if the Security Administrator enables the BIOS Update so that the necessary updates can be implemented for new hardware or software upgrades.

Object reuse does become an issue in a multi-user environment if the user leaves remnants of restricted information that could be accessed by users without authorization. Again, the isolation of domains and the periods processing mode of operation should prevent any data objects in a restricted domain from being available in a domain used by other users. Even if a user operates within the same domain as a previous user, the logoff and logon procedure that must be utilized for access to the domain will erase any memory in volatile memory such as RAM. In addition, the isolation of each group to a specific RHDD should prevent objects accessed by authorized users from being available to unauthorized users. This should provide the required controls for objects processed within the only available non-volatile memory in a restricted domain.

The Sentinel also limits access to data displayed on the computer or workstation display by locking the user session in a restricted mode if the user removes their Smart Card for any reason such as leaving the PC before ending the session. This locking capability is always activated and is implemented during logon and after access to a restricted domain is granted. If the Smart Card is removed, this condition will be immediately sensed by the card reader and reported to the Secure Microcontroller, which will initiate a system reset thereby terminating access to the host computer or workstation.

D. Audit Function

The audit function is implemented within the Secure Microcontroller, which is programmed to record, and time stamp various user events. Time stamped audit data is provided by the Security Module and its Secure Microcontroller on all user events and status related to I&A, access control, password changes, PIN Changes, audit data access, audit data warnings, audit storage shutdown, and audit data download failure. This data is stored within the memory of the Secure Microcontroller as an encrypted CSV file that can only be accessed by the Security Administrator via their Administrator Smart Card. Audit data is recorded in the Secure Microcontroller audit data memory at the completion of each singular event. All of the events for a user are recorded against the user’s PIN, time stamp for each event, type of event, and the success or failure of the event.

The time stamp applied to all audit data by the Security Module is generated from the Secure Microcontroller's Real Time Clock, which is set when initially programmed and continues uninterrupted for the life of the Secure Microcontroller. Real Time Clock time stamps include the month/day/year/hour/second and are automatically adjusted for daylight savings time if required. In addition, the Real Time Clock cannot be reset by a user or the Security Administrator once it is initially setup. It can only be modified by reprogramming the Secure Microcontroller firmware.

The audit data is stored until the Secure Microcontroller memory is full at which point further operations are disabled until the Security Administrator outputs the data to the Security Administrator's Smart Card. Warnings are provided to users of the PC when the memory reaches 90% and then 95% of the memory capacity. The Security Administrator downloads the audit data by logging onto the Sentinel via their Smart Card and their PIN (no password is required) and selecting their "Download Audit Data" profile, which is only available on their card. Audit data can then be downloaded to the security administrator's Smart Card and then uploaded to the Security Administrator workstation. Audit data is downloaded on a byte-by-byte basis. Any failure during an audit data download will not effect the integrity of the audit data since it is still retained in the Secure Microcontroller. However, the process will need to be repeated since the downloaded data file would be incomplete, possibly corrupted or inaccessible, with the loss of the last byte of data.

Once the data is uploaded to the Security Administrator's workstation, the Audit-X audit data processing program is then used to perform sorts and searches on the audit data for further analysis. In order to protect the audit data and also securely manage PIN and User Profile Assignments it is recommended that all administration functions and data be implemented within a Sentinel protected computer in a restricted domain to which only the Security Administrator has access.

A list of all the auditable events that are recorded and stored by the Sentinel Security Module include the following:

- Machine authorization code received from Smart Card (logon)

- Machine authorization code comparison success or failure indication
- Time/Date stamp of logon transaction
- PIN entered by user on keyboard
- PIN comparison success or failure indication (up to 3 attempts)
- Time/Date stamp of PIN transaction for each attempt
- Change password selection entered by user on keyboard
- Time/Date stamp of change password selection by user
- Time/Date stamp of completed password change process
- Password comparison success or failure indication (up to 3 attempts)
- Time/Date stamp of password transaction for each attempt
- Security domain selection by user
- Time/Date stamp of security domain selection transaction
- User's Allowed Security Profile as read from User's Smart Card
- Actual Security Profile selected by user from keyboard
- Implementation of Security Profile success or failure
- Time/Date stamp of Security Profile transaction (including failure to access selected domain)
- Audit Data Download Initiated Time/Date stamp
- Audit Data Incomplete Download Indication
- Audit Data Download complete time/date stamp (log off for administrator)
- Current user PIN entered by Administrator on keyboard for PIN change
- Current user PIN comparison success or failure indication
- Time/date stamp of Current User PIN transaction
- New user PIN entered by Administrator on keyboard
- New PIN comparison success or failure indication
- Time/date stamp of new PIN transaction (log off for administrator)
- BIOS Update enabled by Administrator
- Time/date stamp of BIOS Update enabled.
- Warnings issued for audit data at 90% and 95% of capacity
- Time/date stamp of 90% and 95% warnings
- Shutdown of Security Module when audit data is at 100% of capacity
- Time/date stamp of Security Module Shutdown
- Time/date stamp of Smart Card Removal

E. Security Administration Function

The Security Administration functions that relate to operations implemented under the Administrator Profile are within the TOE. These operations require the Security Administrator to login to a Sentinel in a host PC or workstation by first inserting their Smart Card in the Security Module. When the Security Module reads the role attribute on the Smart Card as an administrator, the Security Administrator will be requested, via the LCD Module, to enter their

PIN. If the PIN is entered correctly from the keyboard, "(A)dministration" will be displayed on the LCD. By depressing the "A" key on the keyboard the allowed Security Administration Profiles of "(C)hange PIN / (D)ownload Audit Data" will be displayed as options on the LCD. These options are the only Security Administration functions within the TOE.

The Security Administrator can change or deactivate a user's PIN within the TOE by selecting the "C" key on the keyboard. A message will appear on the LCD Module requesting the entry of the old PIN. If this PIN is stored on the Sentinel Secure Microcontroller, the Security Administrator will be requested to enter a new PIN. Once this process is completed, the user's PIN is changed within the Secure Microcontroller. To complete the process, however, the PIN must also be changed on the users Smart Card to exactly the same character string as was entered in the Secure Microcontroller. This latter process is implemented by making use of the Sentinel Audit-X Smart Card Programmer function that runs on the Security Administrator's Workstation. The process of changing the PIN on the Smart Card with Audit-X is not within the TOE, although it supports the TOE Security Administration Function.

The other Security Administration function that is within the TOE is downloading Audit Data from the Security Module. This is initiated by selecting the "(D)ownload Audit Data" profile by depressing the "D" key on the keyboard. Audit data is then downloaded on a byte-by-byte basis to the Security Administrator's Smart Card. Any failure during an audit data download will not effect the integrity of the audit data since it is still retained in the Secure Microcontroller. However, the process will need to be repeated since the downloaded data file would be incomplete, possibly corrupted or inaccessible, with the loss of the last byte of data. Again, the loading of this data into the Security Administrator's Workstation and the evaluation of the data using the Audit-X Tool are support functions that are outside the TOE.

Upon completion of any administrator role option from the Administration Menu, the LCD Module will display the following Message **"Press Enter to (UPDATE BIOS)"**. If the administrator presses "Enter" the Security Module will provide the outputs via the Asset Status Sensor and Controller Board to enable the write update for all NVMs shared between security levels and then activate the unrestricted domain. The administrator can then perform any

hardware or software updates that require modifications to the associated NVMs. Once this is completed the removal of the administrator's Smart Card will cause the Asset Status Sensor and Controller Board to disable the write update for these NVMs so that user's cannot access NVMs shared between security levels.

F. Performance Monitoring and Failsafe Control Function

The monitoring of the performance of the Sentinel to determine if it is operating correctly is completely implemented within the hardware design of the Asset Status Sensor and Controller Board in the Security Module. During initialization of the Sentinel at Power on, the GREEN LED will illuminate indicating that the Unrestricted Domain is available if no Smart Card is inserted into the Security Module. This LED is providing a direct indication through its placement in the power control circuitry for this domain that all hardware components are available.

The GREEN LED will remain illuminated even if a valid Smart Card is detected until the I&A and access control process within the Security Module is completed and a restricted domain has been selected and enabled by the Asset Status Sensor and Controller Board. The successful selection and enabling of the restricted domains will cause the YELLOW or RED LED to illuminate, respectively and simultaneously cause the GREEN LED to be extinguished. Again the YELLOW and RED LEDs are absolute indicators that a restrictive domain has been enabled since they are within the power control circuitry of their respective domains and can only be illuminated when the respective domains are enabled.

The above sequence of operations must occur exactly as described for the I&A and access control process to have been successfully implemented. This is definite since the design of the Asset Status Sensor and Controller Board is such that only one domain can and should be enabled at any one time. If more than one LED is illuminated at any point in the operation of the Security Module after Power on, the user should assume a system fault and immediately shut down the computer or workstation. If no LEDs are illuminated it is most likely that the LED has failed and the user should note whether the RHDD for the selected domain has started to power on. If this is the case, the user should proceed with the logon process and note that the RHDD

loads and the Operating System displays a Security Warning Banner identifying the user selected domain as being activated.

The above sequence of events assumes that there was no user error in the entry of the PIN and password and that the RHDD for the selected domain was correctly installed and locked into place. Failure to enter the PIN or password correctly after three attempts at each will cause the system to default to the Unrestricted Domain or Power Off the computer depending on the option implemented for that system. This same result will occur if the user installed an RHDD that was setup for a domain that was different than the one selected.

In addition to the simple test of correct operation, the Security Module has also been designed with a failsafe capability to prevent security vulnerabilities from occurring if Security Module parts or system power should fail. As was described previously, this failsafe capability is implemented within the Asset Status Sensor and Controller Board, the RHDDs, and the S/C and I/O Controller Cards through a design that prevents the enabling of a domain at a higher security level than would be allowed by the I&A and access control process. The key element of this capability is the selection of the type of parts and the interfacing of these parts on the various Sentinel Boards that control domain definition and access based on their known failure and power off states. One of the key parts selected to ensure failsafe operation is the Secure Microcontroller described in detail in the next paragraph. This Secure Microcontroller was specifically designed for crashproof operation even when operating in an environment with power irregularities. In addition to the selection of parts, there is built-in redundancy in the implementation of the TSP so that multiple failures in the operation of the TOE and user operation would be required for the TSP to be violated. This allowed the TOE to be designed so that virtually any combination of component failures would not impact system vulnerability.

G. Physical Protection Function

The Physical Protection function is based on the policy that the key device within the TOE that must be protected against tampering is the Secure Microcontroller located on the Asset Status Sensor and Controller Board in the Security Module. This device stores and runs the firmware that implements the TSP and also stores the audit data that is a key element of various

TSFs. The Secure Microcontroller is actually commercially available from Dallas Semiconductor as its DS2252T Secure Microcontroller Module. Protection of program information and stored data is implemented within the Secure Microcontroller by encrypting all of its memory with a proprietary data encryption algorithm that is known only to the manufacturer. This encryption capability is enabled every time the module is powered down which occurs at the termination of each user session in a restricted domain. Additional protection is provided through the implementation of dummy instructions during the processing of the instructions that implement the TSP. This prevents the actual operations of the microcontroller from being monitored and interpreted while it is operating. Finally, the DS2252T has a tamper proofing mechanism that detects any attempt to discover the on-chip data, program information, and encryption keys and responds by erasing everything stored in the module.

In addition to protecting the Secure Microcontroller, it is also necessary to control connections to all external interfaces so that they cannot be easily changed after the Sentinel is installed and setup. The installation and setup process must ensure that network connections to each NIC are correct as are the connection of a printer to the USB port designated for printing. All connections to external ports will be tested to determine that they are correct during the installation process and will then be secured with the Back Panel Cable Lock Shield security device that will prevent users or other unauthorized personnel from changing the connections.

In addition to the physical protection mechanisms that are within the TOE, there are optional protective capabilities available that include intrusion prevention screws for securing the case and an audible alarm system that is enabled if the computer case is opened or moved in an unauthorized manner

2.3.2 Sentinel TSF Interfaces/TOE Boundary

The Sentinel TOE consists of the components of the Sentinel that establish and control access to the restricted domains within the PC or workstation. This includes the following:

1. Security Module
2. Cables, Connectors and Cable Locks
3. ISA Sensor/Controller Cards
4. PCI Sensor/Controller Cards
5. I/O Controller Board

6. RHDD Drive Frame
7. LCD Module
8. Back Panel Assembly
9. Tamper Proof Secure Microcontroller
10. NVM Control Interface
11. PCMCIA Card Reader (Optional)

The security functions that make up the TSF for the Sentinel TOE are listed below in Table 2.1 with a cross-reference to the ST paragraph where they are described. All descriptions of ST functions are provided in a summary format. A more detailed description of the enabling ST function and the exact description of each TSF is provided in Chapters 5 and 6 of this ST.

Table 2.1 ST Functional Requirements As Enabled in TOE

ST TSF	ST Paragraph	Description of Enabling ST Function
FAU_GEN.1	2.3.1D	Audit data recording by Security Module
FAU_GEN.2	2.3.1D	All audited events are linked to User PIN (ID)
FAU_SAR.1	2.3.1D	Audit data downloaded by Security Admin with Smart Card
FAU_SAR.2	2.3.1D	Admin Smart Card required for access to audit data
FAU_STG.1	2.3.1D	Admin Smart Card required for access to audit data
FAU_STG.4	2.3.1D	Alarms and access to restricted domains denied when audit memory at capacity
FDP_ACC.2	2.3.1B	HBAC Policy implemented by Security Module
FDP_ACF.1	2.3.1B	HBAC Policy implemented by Security Module
FDP_RIP.1	2.3.1C	Protection of a subset of residual data in restricted domains after user session
FIA_AFL.1	2.3.1A	Security Module allows 3 authentication attempts before default state enabled
FIA_ATD.1	2.3.1A&B	Smart Card profile and HBAC Policy implemented by Security Module
FIA_SOS.1	2.3.1A	Restrictions on the minimum length of passwords and PINs
FIA_UAU.2	2.3.1A	Access to restricted domains based on profile requires prior user authentication
FIA_UAU.7	2.3.1A	LCD Module obscures the entry of PIN and Password
FIA_UID.2	2.3.1A&B	ID must be completed before profile is established for restricted domains
FIA_USB.1	2.3.1A&B	Provided by profile on Smart Card and access rules in Security Module
FMT_MSA.1	2.3.1E	All access rights are defined and controlled by Security Administrator
FMT_MSA.2	2.3.1A	Changes in password restricted to secure values
FMT_MSA.3	2.3.1B	Security attributes are put on Smart Card by admin for restricted domains.
FMT_MTD.1	2.3.1E	Only Security Admin can set profiles and PINs and access audit data
FMT_REV.1	2.3.1E	Only Security Admin can modify profiles and revoke PINs
FMT_SMR.2	2.3.1E	Security Module has complete control over user and administrator roles
FPT_FLS.1	2.3.1F	Design of Security Module prevents failures that result in non-secure state
FPT_PHP.3	2.3.1G	Tamper proofing and protection mechanisms in Secure Microcontroller
FPT_RVM.1	2.3.1A&B	Implementation of TSP by isolated and tamper proof Security Module
FPT_SEP.1	2.3.1A&B	Isolation of Security Module from computer data processing and software
FPT_STM.1	2.3.1D	Time stamping of auditable events in Security Module
FTA_LSA.1	2.3.1B	Security profile includes attributes related based on time of day
FTA_TSE.1	2.3.1A&B	Security Module can deny session based on clearance and time of day

CHAPTER 3. Target of Evaluation Security Environment

3.0 Introduction

This chapter will define the security environment that the TOE has been designed to operate in. The description of the environment will include a description of the following environmental factors:

1. Intended usage of the TOE
2. User characteristics
3. Facility Characteristics
4. Security Support Roles
5. Assets the TOE will be required to protect
6. Threats
7. Assumptions

All of these factors will be described in the paragraphs below.

3.1 Intended Usage of TOE

The Sentinel TOE is essentially a Computer Security System in the form of a kit that is capable of being installed in any modern Personal Computer or workstation. It is intended to provide sufficient security for unrestricted and up to two levels of restricted data to be processed in a single computer. Since the Sentinel TOE is operating system and software independent, there is no impact on a user's capability to use any software package that can be used in any other PC or workstation. The user will be required to use a Smart Card during operations in a restricted mode.

Installation of the TOE kit can be implemented as a retrofit for existing computers that require increased security or as a system that can be installed as an option into new Commercial Off-The-Shelf (COTS) computers and workstations. The installation process is capable of being completed in most computers in less than 2 hours by a qualified and trained installer. It should be noted that the delivery, installation, and setup of the TOE has important security implication

related to the target EAL 4 assurance level that must be complied with to maintain secure usage of the computer.

3.2 Facility Characteristics

The TOE is capable of being utilized in virtually any type of facility that will support the processing of multiple levels of restricted data on a computer or workstation. At a minimum the facility need only have the necessary level of physical security to support access to the restricted data with no further security capabilities or resources. Certain capabilities such as access to restricted networks such as the SIPRNET or NIPRNET will be required for network operations at a restricted level. The TOE has been designed to be easily customized to both the user and facility requirements by allowing a Security Administrator to only enable the processing capabilities that are supported by the facility capabilities and the rights of the user. This customization is implemented through the programming of a user's Smart Card. In addition to its flexibility, the TOE has special protective security capabilities that will allow it to operate with less physical security than most environments and should allow the storage of restricted data directly on the host computer.

3.3 User Characteristics

Once installed, the security system can be utilized by virtually any user that has sufficient skills to operate a PC. The TOE was specifically designed to support the full range of desktop computer users, from those who need regular access to restricted data to those who only need to access this data occasionally. While all users must have the clearances necessary to operate at the restricted levels that are established on the computer, this is not a problem since the Smart Card and TOE operation will automatically control what a user can access. The user Smart Cards are controlled by a Security Administrator that will set each user's access rights for the security level of the data they need to access. It is assumed that each user will have access to their own PC or workstation since this is a normal usage of a PC. This is not mandatory, however, since multiple users can use the same PC and either get access to only their data or time share the same data.

3.4 Operator Roles

The TOE will support two types of operator roles, authorized user and authorized administrator. An authorized user is any user that has access to the PC and has a Smart Card that will allow access to restricted data and restricted operations. An authorized administrator is an operator that has a Smart Card that will allow them to control a user's PIN and download audit data from the TOE. The TOE distinguishes between the two roles and ensures that an authorized administrator cannot also be an authorized user on the same computer or workstation.

3.5 Protected Assets

The assets to be protected by the TOE include any restricted data and restricted operations performed on that data. In essence the TOE provides a hardware based security shell that allows the computer or workstation to securely perform all its normal operations using COTS operating systems and software. It does this by controlling access to specific hardware used for storing data and processing the data at each restricted level. This prevents any data from being stored or processed by either a user or resources that do not have the required authorization. The capabilities of the TOE to implement this protection via hardware makes it immune to the normal software based vulnerabilities and attack modes. Untrusted and even malicious software cannot interfere with the capability of the TOE to implement its security functions and policy.

3.6 Threats

The TOE has been explicitly designed to counter threats from organizational insiders who are employed by, consult with, or have apparent authorized access to the facility where the TOE is installed. It is assumed that this threat environment includes individuals with IT skills that range from that of the average PC user to highly trained IT specialists. In addition, it must be assumed that the threat has a superior knowledge of the IT environment that includes knowledge of where assets are located and how they are being protected. Finally it must also be assumed that threat is anonymous, motivated, and has access to those areas in the facility where restricted data and information is stored and processed.

3.6.1 Threat Agents

Threat agents are individuals within the insider community that are capable of posing a threat to the TOE and the assets being protected by the TOE. The threat agents that are relevant to the subject TOE are:

- unauthorized users of the TOE, i.e. individuals who have not been granted the required Identification and Authentication information and/or the clearance or access rights necessary to access the system, restricted information, or restricted processes; or

- authorized users of the TOE, i.e. individuals who have been granted the required Identification and Authentication information and/or the clearance or access rights necessary to access the system, restricted information, or restricted processes.

3.6.2 Threats to TOE

The threats listed below are those that are capable of being implemented by the threat agents within the threat environment described above.

[T.ACCESS_SECRETS] An unauthorized user of the TOE gains access to the secrets used for identification and authentication of an authorized user to perform operations that could disable the TOE and/or provide unauthorized access to restricted information.

[T.ACCESS_INFO] An unauthorized or authorized user of the TOE accesses, modifies, or destroys restricted information without having the necessary security clearance.

[T.PROCESS_INFO] An unauthorized or authorized user of the TOE accesses restricted processes to perform operations on restricted information that causes the information to be put in a non-secure state.

[T.DISABLE_TOE] An authorized or unauthorized user of the TOE performs an operation or an act designed to disable the TOE in order to gain access to restricted information to which they would not otherwise have access.

[T.ADMIN_RIGHTS] Unauthorized use of TOE functions that require administration rights by an authorized or unauthorized user of the TOE in order to gain access to and/or modify or destroy audit or security attribute data.

3.7 Assumptions

This paragraph identifies the minimum Information Technology, Physical and Procedural measures required to maintain security of the TOE.

3.7.1 Physical Assumptions

The following are the physical assumptions that pertain to the TOE:

[A.LOCATE] It is assumed that the TOE is located in a controlled facility with sufficient physical security to prevent the TOE from being removed from the host computer or the facility by anyone other than authorized maintenance personnel.

[A.PROTECT] It is assumed that the physical protection within a controlled facility will prevent TOE hardware critical to security policy enforcement from being removed from the host computer and the facility by anyone other than authorized maintenance personnel.

3.7.2 Personnel Assumptions

The following are the personnel assumptions that pertain to the TOE:

[A.ADMIN] It is assumed that there is at least one competent individual who is assigned to securely administer the TOE audit and user identification functions and that they have procedures for establishing user clearances and authorization for the data and resources available in each of the domains. Such personnel are assumed not to be careless, willfully negligent or hostile.

[A. ROLES] It is assumed that authorized administrators and authorized users will have distinct roles such that an authorized user of the TOE cannot simultaneously be the administrator for that TOE.

3.7.3 Connectivity Assumptions

The following are the connectivity assumptions that pertain to the TOE:

[A. PEER] It is assumed that any other systems or peripherals outside of the Host computer or workstation with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints as the TOE.

[A.CONNECT] All connections to peripheral devices and networks reside within the controlled access facilities and the connections to networks and peripherals at an assigned level of sensitivity will be made to TOE network and I/O access points at that same level of sensitivity.

CHAPTER 4. Security Objectives

4.0 Introduction

This Chapter defines the security objectives of the TOE and its supporting environment. Security objectives, categorized as either IT security objectives or non-IT security objectives, reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. All of the identified threats and organizational policies are addressed under one of the following categories

4.1 TOE Security Objectives

The following are the IT security objectives:

[O. IDENTIFICATION] The TOE must ensure that all authorized users are identified before they can access restricted data and processes on a host computer through a process that requires the use of a secure token in addition to the use of a unique PIN.

[O. AUTHENTICATION] The TOE must ensure that all authorized users are authenticated with a password after being identified by their unique PIN before they can access restricted data and processes on a host computer.

[O. HBAC] The TOE must ensure that all authorized users can only gain access to the level of restricted data and processes on a host computer that are permitted by the user's clearance and access rights at the time of logon as mediated by the access control function.

[O. RESIDUAL_INFO] The TOE must ensure that all processes performed by an authorized user on a host computer during a user session will not leave residual information of a restricted nature on any readable computer data storage system that can be accessed by another user without the necessary clearance and access rights.

[O. AUDIT] The TOE must ensure that all user initiated processes involving TOE security functions are recorded as audit data that includes a time stamp and user identity

and that this data is protected against unauthorized access, modification or deletion by users.

[O. ENFORCEMENT] The TOE must enforce its security policy without being vulnerable to attack by means of the operating system, applications software, or by user interaction through the normal computer user interfaces.

[O.FAILSAFE] The TOE should have no failure modes due to the loss of power or the failure of host computer software or hardware that could result in restricted data or processes being made insecure.

[O.SEPARATION] The TOE will only allow user access to data and processes that are at the same sensitivity level during an authorized user's session.

4.2 Security Objectives for the Environment

The Sentinel TOE is assumed to be complete and self-contained and, as such, is not dependent upon any other products to perform properly. However, certain objectives with respect to the operating environment must be met. The following are the non-IT security objectives:

[O.INSTALL] Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner, which maintains IT security objectives.

[O. PHYSICAL] Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack that might compromise IT security objectives.

[O.SECRETS] Those responsible for the TOE must ensure that all user security attributes used for Identification and Authentication such as PINs and passwords are protected by the users in a manner that maintains IT security objectives.

4.3 Security Objectives Rationale

This section of the ST will describe how the Security Objectives can be traced to: the Threat described in paragraph 3.6; the Organizational Security Policy described in paragraph 3.7; and the Assumptions described in paragraph 3.8. A detailed description of how the Security Objectives are suitable to address each threat, organizational security policy, and assumption is also provided.

4.3.1 Threat v. Security Objectives for TOE

The mapping of threats to the TOE and how they are addressed by the TOE Security Objectives is shown in Table 4.1. A description of how each threat is addressed by the Security Objectives for the TOE is described in the paragraphs below. It should be noted that some threats are also addressed by the Security Objectives for the Environment as described in paragraph 4.3.2.

Table 4.1 Threat v. Security Objectives for TOE

THREATS TO TOE	SECURITY OBJECTIVES FOR TOE
[T.ACCESS_SECRETS]	[O. IDENTIFICATION] [O. AUTHENTICATION]
[T.ACCESS_INFO]	[O. HBAC] [O. RESIDUAL_INFO] [O.SEPARATION] [O.FAILSAFE]
[T.PROCESS_INFO]	[O. HBAC] [O.SEPARATION] [O.FAILSAFE]
[T.DISABLE_TOE]	[O. ENFORCEMENT]
[T.ADMIN_RIGHTS]	[O.HBAC] [O. AUDIT]

4.3.1.1 [T.ACCESS_SECRETS] v. Security Objectives for TOE

The [O.IDENTIFICATION] objective protects against the [T.ACESS_SECRETS] threat by requiring unique PIN entries that are protected against observation, guessing and brute force attacks. In addition a secure token must be used in addition to the entry of the unique PIN from the keyboard so that getting access to the PIN is not sufficient without also possessing the correct secure token. The [O.AUTHENTICATION] objective protects against the [T.ACESS_SECRETS] threat by requiring PASSWORD entries to be protected against observation, guessing and brute force attacks. Addition protection against the [T.ACCESS_SECRETS] threat is provided by Security Objectives for the Environment as described in paragraph 4.3.3.1.

4.3.1.2 [T.ACCESS_INFO] v. Security Objectives for TOE

The [O.HBAC] objective protects against the [T.ACESS_INFO] threat by only allowing an authorized user access to the data and processes that their security profile allows at the time of logon to the PC or workstation. In addition, the [O.RESIDUAL_INFO] objective eliminates the possibility of residual data from a previous user from being accessed by a user that has no authorization to access or process that data. The [O.SEPARATION] objective prevents data from being transferred from one security level to another where it could possibly be accessed by users without the required clearance level or access rights. Finally, unauthorized access to data due to failure of the TOE is prevented by the [O.FAILSAFE] objective. All of these objectives taken as a whole address all the logical threat scenarios for the [T.ACCESS_INFO] threat.

4.3.1.3 [T.PROCESS_INFO] v. Security Objectives for TOE

The [O.HBAC] objective protects against the [T.PROCSS_INFO] threat by only allowing authorized users with the proper clearance level and access rights at the time of logon to access processes that have the potential for putting restricted data in a non-secure state. Protection against the unauthorized use of processes to send restricted data outside the host computer so that said data is in a non-secure state is addressed by the [O.HBAC] objective. The [O.SEPARATION] objective prevents any processes from being used by any user to send data across security levels thus potentially placing the data in a non-secure state. Finally, unauthorized access to protected processes due to power failures or failures of the TOE is

addressed by the [O.FAILSAFE] objective. all of these objectives taken as a whole address all the logical threat scenarios for the [T.PROCESS_INFO] threat.

4.3.1.4 [T.DISABLE_TOE] v. Security Objectives for TOE

The [O.ENFORCEMENT] objective prevents the TOE from being disabled and allowing unauthorized access to restricted data by ensuring that the security policy that protects said data is not vulnerable to attack by a user. Security Objectives for the Environment as described in paragraph 4.3.3.2 provide additional protection against the [T.DISABLE_TOE].

4.3.1.5 [T.ADMIN_RIGHTS] v. Security Objectives for TOE

The [O.HBAC] objective ensures that user security attributes and audit data is not accessible to any user without administration rights. All audit data for user initiated processes is protected against unauthorized access by users by the [O.AUDIT] objective. All of these objectives taken as a whole address all the logical threat scenarios for the [T.ADMIN_RIGHTS] threat.

4.3.2 Threat v Security Objectives for Environment

The mapping of threats to the Security Objectives for the Environment is shown in Table 4.2, below. A description of how each threat is addressed by the Security Objectives for the Environment is described in the paragraphs below.

Table 4.2 Threat v. Security Objectives for the Environment

THREATS TO TOE	SECURITY OBJECTIVES FOR ENVIRONMENT
[T.ACCESS_SECRETS]	[O. SECRETS]
[T.DISABLE_TOE]	[O. INSTALL] [O. PHYSICAL]

4.3.2.1 [T.ACCESS_SECRETS] v Security Objectives for Environment

In addition to those Security Objectives for the TOE described in paragraph 4.3.1.1, the [O.SECRETS] Security Objective for the Environment is required to completely address the [T.ACCESS_SECRETS] threat scenario. The [O.SECRETS] objective addresses the threat by requiring users and administrators to protect security attributes such as user PINs and passwords from unauthorized access and use.

4.3.2.2 [T.DISABLE_TOE] v Security Objectives for Environment

In addition to those Security Objectives for the TOE described in paragraph 4.3.1.4, the [O.INSTALL] and [O.PHYSICAL] Security Objectives for the Environment are required to completely address the [T.ACCESS_SECRETS] threat scenario. The [O.INSTALL] objective limits the vulnerability of the TOE by ensuring that the installation of the TOE is done correctly so that there are no readily available TOE access points that would allow it to be disabled. In addition, the [O.PHYSICAL] objective protects against threats that would disable the TOE by means of physical attacks.

4.3.3 Assumptions v Security Objectives for Environment

The mapping of Assumptions to the Security Objectives for the Environment is shown in Table 4.3, below. A description of how each assumption is addressed by the Security Objectives for the Environment is described in the paragraphs below.

Table 4.3 Assumptions v Security Objectives for the Environment

ASSUMPTIONS	SECURITY OBJECTIVES FOR THE ENVIRONMENT
[A.LOCATE]	[O. PHYSICAL]
[A.PROTECT]	[O. PHYSICAL]
[A.ROLES]	[O.SECRETS]
[A.CONNECT]	[O. INSTALL]

4.3.3.1 [A.LOCATE] v Security Objectives for Environment

The [O.PHYSICAL] objective supports the [A.LOCATE] assumption by ensuring that the TOE is located in a controlled facility to prevent the TOE from being obtrusively attacked within the facility or removed from the facility and attacked at a remote location.

4.3.3.2 [A.PROTECT] v Security Objectives for Environment

The [O.PHYSICAL] objective supports the [A.PROTECT] assumption by ensuring that the TOE is located in a controlled facility to prevent the TOE from being removed from the facility by unauthorized personnel.

4.3.3.3 [A.ROLES] v Security Objectives for Environment

The [O.SECRETS] objective supports the [A.ROLES] assumption by requiring the programming of security attributes including PIN to be under the separate control of an administrator with passwords being controlled by users. This division of secrets is necessary to ensure that users cannot access audit data and PINs and administrators cannot access restricted user data and processes protected by the TOE.

4.3.3.4 [A.CONNECT] v Security Objectives for Environment

The [O.INSTALL] objective supports the [A.CONNECT] assumption by requiring all connections to the TOE to be correct.

CHAPTER 5. Information Technology Security Requirements

5.0 Introduction

This chapter defines the functional requirements within the ST that are the basis of the Sentinel TOE Functional Requirements. Each of the TOE Security Functions (TSFs) will be referenced to the applicable requirements in Part 2 of the Common Criteria. The TOE will implement various classes of functional requirements that are defined by a three letter mnemonic that include the following:

- Class FAU - Security Audit
- Class FDP - User Data Protection
- Class FIA - Identification and Authentication
- Class FMT - Security Management
- Class FPT - Protection of the TSF
- Class FTA - TOE Access

Within each of the above classes the TOE will implement a specific functional requirement that fall within the family of security functional requirements. The family is represented by a second three-letter mnemonic while a specific functional requirement, referred to as a component, is defined by a number. For example, the Audit Data Generation Family is defined by FAU_GEN with individual components in the family being defined by .1 or .2. In some families the components are hierarchical so that the highest number encompasses the requirements of components with lower numbers. This is not always the case since in some families a component with a higher number may not encompass the functions performed by a component with a lower number. In Table 5.1 all of the components that define the functional requirements for the Sentinel TOE are listed in the far left column. It is evident that within this table some of the components are independent and, therefore, the requirements must be addressed independently within the TOE.

Table 5.1 Sentinel Security Functional Requirements

TSF Requirement	Functional Description	ST Paragraph Reference
FAU_GEN.1	Audit Data Generation	2.3.1D
FAU_GEN.2	User Identity Association	2.3.1D
FAU_SAR.1	Audit Review	2.3.1D
FAU_SAR.2	Restricted Audit Review	2.3.1D
FAU_STG.1	Guarantees of Audit Data Availability	2.3.1D
FAU_STG.4	Prevention of Audit Data Loss	2.3.1D
FDP_ACC.2	Complete Access Control	2.3.1B
FDP_ACF.1	Security Attribute Based Access Control	2.3.1B
FDP_RIP.1	Subset Residual Information Protection	2.3.1C
FIA_AFL.1	Authentication Failures	2.3.1A
FIA_ATD.1	User Attribute Definition	2.3.1A&B
FIA_SOS.1	Specification of Secrets	2.3.1A
FIA_UAU.2	Authentication	2.3.1A
FIA_UAU.7	Protected Authentication Feedback	2.3.1A
FIA_UID.2	Identification	2.3.1A
FIA_USB.1	User-Subject Binding	2.3.1A&B
FMT_MSA.1	Management of Security Attributes	2.3.1E
FMT_MSA.2	Secure Security Attriibutes	2.3.1E
FMT_MSA.3	Static Attribute Initialization	2.3.1B&E
FMT_MTD.1	Management of TSF Data	2.3.1E
FMT_REV.1	Revocation of Security Attributes	2.3.1E
FMT_SMR.2	Security Management Roles	2.3.1E
FPT_FLS.1	Failure with Preservation of Secure State	2.3.1F
FPT_PHP.3	Resistance to Physical Attack	2.3.1G
FPT_RVM.1	Non-bypassability of the TSP	2.3.1A&B
FPT_SEP.1	TSF Domain Separation	2.3.1A&B
FPT_STM.1	Reliable Time Stamps	2.3.1D
FTA_LSA.1	Limit on Scope of Selectable Attributes	2.3.1B
FTA_TSE.1	TOE Session Establishment	2.3.1A&B

5.1 TOE Security Functional Requirements

Table 5.1 gives the security functional requirements for the Sentinel as derived from the CC and provides a reference to the function description in the ST where each functional requirements is implemented in the TOE. The paragraphs that follow will define each functional requirement from the CC as they relate to the Sentinel TOE. In some cases this will require the selection of the specific parameters or variables that are open to assignment or selection in the applicable CC components within the overall ST. The assignment and/or selection of these variables will be represented by the text in the stated requirement that is underlined. In some cases refinements to individual components will be required for the purpose of definition, elaboration, or interpretation of a requirement as it relates to the TOE. Refinements will always be in the nature of a restriction to the requirement as stated in the CC and will be indicated by italicized text. Refinements and Deviations from the audit requirements for a component due to inability to implement based on the scope of control of the TOE will be noted and referenced to the individual components in Table 5.2.

5.1.1 Security Audit Data Generation Requirements

The Security Audit Data Generation Requirements for the Sentinel TOE are described against the FAU_GEN Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FAU_GEN.1 Audit Data Generation

FAU_GEN.2 User identity association

The specific requirements for each of these components are described in the paragraphs 5.1.1.1 and 5.1.1.2, below.

5.1.1.1 FAU_GEN.1 Audit Data Generation

This security requirement is stated as:

A. FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Startup and shutdown of the audit functions;

b) All the auditable events for the level of audit not specified; and

c) All the events listed in Table 5.2.

Table 5.2 Auditable Events

Component	Requirement	Level
FAU_GEN.1	Start-up and shutdown of the audit functions.	As defined in FAU_GEN1.2
FAU_GEN.2	None	N/A
FAU_SAR.1	Reading of information from the audit records.	Basic
FAU_SAR.2	Unsuccessful attempts to read information from the audit records.	Basic
FAU_STG.1	None	N/A
FAU_STG.4	Actions taken due to audit storage failure.	Basic
FDP_ACC.2	None	N/A
FDP_ACF.1	The specific security attributes used in making an access check.	Detailed
FDP_RIP.1	None	N/A
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the and the actions taken.	Minimal
FIA_ATD.1	None	N/A
FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret.	Basic
FIA_UAU.2	All use of the authentication mechanism.	Basic
FIA_UAU.7	None	N/A
FIA_UID.2	All use of the user identification mechanism, including the user identity (PIN) provided.	Basic
FIA_USB.1	Success and failure of binding security attributes to a user.	Basic
FMT_MSA.1	All modifications of the values of security attributes.	Basic
FMT_MSA.2	All offered and accepted secure values of security attributes.	Detailed
FMT_MSA.3	Modifications of the default setting of restrictive rules. All modifications of the values of security attributes.	Basic
FMT_MTD.1	All modifications to values of TSF data.	Basic
FMT_REV.1	All attempts to revoke security attributes.	Basic
FMT_SMR.2	Every use of the rights of a role.	Detailed.
FPT_FLS.1	Failure of the TSF *as indicated by a failure to implement security profile that is not in accordance with TSP*.	Refinement
FPT_PHP.3	None	N/A

Component	Requirement	Level
FPT_RVM.1	None	N/A
FPT_SEP.1	None	N/A
FPT_STM.1	Providing a timestamp	Detailed
FTA_LSA.1	All attempts at selecting a session security attributes.	Basic
FTA_TSE.1	All attempts at establishment of a user session.	Basic

B. FAU_GEN 1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, audit data identifying the Smart Card Security Token used during the session.

5.1.1.2 FAU_GEN.2 User Identity Association

This security requirement is stated as:

A. FAU_GEN.2.1

The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.2 Security Audit Review Requirements

The Security Audit Review Requirements for the Sentinel TOE are described against the FAU_SAR Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FAU_SAR.1 Audit Review

FAU_SAR.2 Restricted Audit Review

The specific requirements for each of these components are described in the paragraphs 5.1.2.1 and 5.1.2.2, below.

5.1.2.1 FAU_SAR.1 Audit Review

This security requirement is stated as:

A. FAU_SAR.1.1

The TSF shall provide authorized administrators with the capability to read all the audit information described in Table 5.2 from the audit records.

B. FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.2.2 FAU_SAR.2 Restricted Audit Review

This security requirement is stated as:

A. FAU_SAR.2.1

The TSF shall prohibit all users read access to the audit records, except those users *defined as authorized administrators,* that have been granted explicit read-access.

The italicized portion of this requirement is a refinement to the CC statement, which is necessary since the TSP does not permit users of the TOE to also be authorized administrators.

5.1.3 Security Audit Event Storage Requirements

The Security Audit Event Storage Requirements for the Sentinel TOE are described against the FAU_STG Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FAU_STG.1 Protected audit trail storage

FAU_STG.4 Prevention of audit data loss

The specific requirements for each of these components are described in the paragraphs 5.1.3.1 and 5.1.3.2 below.

5.1.3.1 FAU_STG.1 Protected audit data storage

This security requirement is stated as:

A. FAU_STG.1.1

The TSF shall protect the stored audit records from unauthorized deletion.

B. FAU_STG.1.2

The TSF shall be able to prevent modifications to the audit records.

5.1.3.2 FAU_STG.4 Prevention of Audit Data Loss

This security requirement is stated as:

FAU_STG.4.1

The TSF shall prevent auditable events, except those taken by the authorized *administrators defined as users* with special rights and provide visual warnings of data storage status if the audit trail is full.

The italicized portion of this requirement is a refinement to the CC statement, which is necessary since the TSP does not permit users of the TOE to also be authorized administrators.

5.1.4 Access Control Policy Requirements

The Access Control Policy Requirements for the Sentinel TOE are described against the FDP_ACC Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FDP_ACC.2 Complete access control

The specific requirements for this component is described in paragraph 5.1.4.1

5.1.4.1 FDP_ACC.2 Complete Access Control

This security requirement is stated as:

A. FDP_ACC.2.1

The TSF shall enforce the Hardware Based Access Control Policy on a controlled subject consisting of an authorized user or authorized administrator with an active set of security attributes and controlled objects consisting of data storage objects, data communications objects, with an identified set of security attributes within the TSC and all operations among subjects and objects covered by the SFP.

B. FDP_ACC.2.2

The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.1.5 Access Control Functions

The Access Control Functions Requirements for the Sentinel TOE are described against the FDP_ACF Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FDP_ACF.1 Security attribute based access control

The specific requirements for this component is described in paragraph 5.1.5.1

5.1.5.1 FDP_ACF.1 Security Attribute Based Access Control

This security requirement is stated as:

A. FDP_ACF.1.1

1. **The TSF shall enforce the Hardware Based Access Control Policy to objects based on a controlled subject's clearance, access rights to data communications**

objects, role, and time based attributes plus the sensitivity level and ID of the RHDD data storage object, sensitivity level and access requirements of a data communications object, ID of the RHDD data storage object, and time of day.

B. FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. **The HBAC TSF will only enable operations involving a controlled subject and any controlled object at a restricted sensitivity level if there is an RHDD data storage object at that level of sensitivity within the TSC;**

2. **The HBAC TSF will only enable a controlled subject to access and perform operations on a RHDD data storage object within the TSC if the subject has a security clearance attribute at the time of logon that is equal to the sensitivity level of the RHDD and the RHDD ID has been identified as valid by the TOE;**

3. **The HBAC TSF will only enable a controlled subject, to perform an operation on a RHDD data storage object that requires a NIC, Modem, and/or a USB port data communications object if: the RHDD has a valid ID and sensitivity level; the data communications object is within the TSC at the same level of sensitivity as the RHDD; and the subject has a security clearance at the time of logon equal to the level of sensitivity of the RHDD and has the necessary access rights at the time of logon to each of the required data communications objects at the same level of sensitivity as the RHDD.**

C. FDP_ACF.1.

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

1. **The HBAC TSF will allow a controlled subject operating at a restricted security level to perform operations that require access to any Read-Only data storage object .**

2. **The HBAC TSF will allow a controlled subject operating as an authorized administrator to have access to User PIN and Audit Data stored within the TOE Secure Microcontroller and to Non-Volatile Memories shared between security levels.**

3. **The HBAC TSF will allow any subject operating at an unrestricted security level access to any unrestricted data storage object by default.**

D. FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the:

1. **HBAC TSF denying a controlled subject ,operating at a restricted security level, access to any R/W data storage object other than the RHDD within the TSC at that security level.**

2. **HBAC TSF denying any subject other than an authorized administrator access to User PIN and Audit Data and to Non-Volatile Memories shared between security levels.**

3. **HBAC TSF denying a controlled subject operating as an authorized administrator access to any data storage or data communications objects at a restricted security level.**

5.1.6 Residual Information Protection Requirements

The Residual Information Protection Requirements for the Sentinel TOE are described against the FDP_RIP Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FDP_RIP.1 Subset residual information protection

The specific requirement for this component is described in paragraph 5.1.6.1 below.

5.1.6.1 FDP_RIP.1 Subset Residual Information Protection

This security requirement is stated as:

A. FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to the following objects:

1. **R/W Data Storage Objects other than the RHDD;**
2. **Data Communications Objects;**
3. **Read-Only Data Storage Objects;**
4. **Non-Volatile Memories; and**
5. **Volatile Memories.**

5.1.7 Authentication Failures Requirements

The Authentication Failures Requirements for the Sentinel TOE are described against the FIA_AFL Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FIA_AFL.1 Authentication failure handling

The specific requirement for this component is described in paragraphs 5.1.7.1, below.

5.1.7.1 FIA_AFL.1 Authentication Failure Handling

This security requirement is stated as:

A. FIA_AFL.1.1

The TSF shall detect when three (3) unsuccessful authentication attempts occur related to the user's entry of their password.

B. FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall cause the TOE to enter a default mode which can either be the unrestricted domain or a power off state.

5.1.8 User Attribute Definition Requirements

The Attribute Definition Requirements for the Sentinel TOE are described against the FIA_ATD Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FIA_ATD.1 User attribute definition

The specific requirement for this component is described in paragraph 5.1.8.1, below.

5.1.8.1 FIA_ATD.1 User Attribute Definition

This security requirement is stated as:

A. FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users:

a) PIN as a User Identifier; and

b) Password as Authentication Data.

5.1.9 Specification of Secrets Requirements

The Specification of Secrets Requirements for the Sentinel TOE are described against the FIA_SOS Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FIA_SOS.1 Verification of secrets

The specific requirement for this component is described in paragraph 5.1.9.1, below.

5.1.9.1 FIA_SOS.1 Verification of Secrets

This security requirement is stated as:

A. FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet the following:

a) **For each attempt to use the authentication mechanism during password entry, the probability that a random attempt will succeed is less than one in 1,000,000;**
b) **For multiple attempts to use the authentication mechanism for password entry during a one minute period, the probability that a random attempt during that minute will succeed is less than one in 100,000; and**
c) **Any feedback given during an attempt to use the authentication mechanism for password entry will not reduce the probability below the above metrics.**

5.1.10 User Authentication Requirements

The User Authentication Requirements for the Sentinel TOE are described against the FIA_UAU Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FIA_UAU.2 User authentication before any action

FIA_UAU.7 Protected authentication feedback

The specific requirements for each of these components are described in paragraphs 5.1.10.1 and 5.1.10.2 below.

5.1.10.1 FIA_UAU.2 User Authentication Before Any Action

This security requirement is stated as:

A. FIA_UAU..2.1

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on the behalf of that user.

5.1.10.2 FIA_UAU.7 Protected Authentication Feedback

This security requirement is stated as:

A. FIA_UAU.7.1

The TSF shall provide only obscured feedback to the user while the authentication is in progress.

5.1.11 User Identification Requirements

The User Identification Requirements for the Sentinel TOE are described against the FIA_UID Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FIA_UID.2 User Identification before any action

The specific requirement for this component is described in paragraph 5.1.11.1, below.

5.1.11.1 FIA_UID.2 User Identification Before Any Action

This security requirement is stated as:

A. FIA_UID.2.1

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.12 User-Subject Binding Requirements

The User-Subject Binding Requirements for the Sentinel TOE are described against the FIA_USB Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FIA_USB.1 User-subject binding

The specific requirement for this component is described in paragraph 5.1.12.1, below.

5.1.12.1 FIA_USB.1 User-Subject Binding

This security requirement is stated as:

A. FIA_USB.1.1

The TSF shall associate the appropriate user security attributes with subjects acting on the behalf of that user.

5.1.13 Management of Security Attributes Requirements

The Management of Security Attributes Requirements for the Sentinel TOE are described against the FMT_MSA Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FMT_MSA.1 Management of security attributes

FMT_MSA.2 Secure security attributes

FMT_MSA.3 Static attribute initialization

The specific requirements for each of these components are described in paragraphs 5.1.13.1, 5.1.13.2, and 5.1.13.3 below.

5.1.13.1 FMT_MSA.1 Management of Security Attributes

This security requirement is stated as:

A. FMT_MSA.1.1

The TSF shall enforce the Hardware Based Access Control SFP to restrict the ability to:

a) Modify or delete the security attributes associated with a PIN as a User Identifier to an authorized administrator.

b) Modify the security attributes associated with a Password as Authentication Data to an authorized user.

5.1.13.2 FMT_MSA.2 Secure Security Attributes

This security requirement is stated as:

A. FMT_MSA.2.1

The TSF shall ensure that only secure values are accepted for security attributes.

5.1.13.3 FMT_MSA.3 Static Attribute Initialization

This security requirement is stated as:

A. FMT_MSA.3.1

The TSF shall enforce the Hardware Based Access Control SFP to provide restrictive default values for security attributes that are used to enforce the SFP.

B. FMT_MSA.3.2

The TSF shall allow the authorized administrator to specify alternative initial values to override the default values when an object or information is created.

5.1.14 Management of TSF Data Requirements

The Management of TSF Data Requirements for the Sentinel TOE are described against the FMT_MTD Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FMT_MTD.1 Management of TSF data

The specific requirement for this component is described in paragraph 5.1.14.1, below.

5.1.14.1 FMT_MTD.1 Management of TSF Data

This security requirement is stated as:

A. FMT_MTD.1.1

The TSF shall restrict the ability to delete and clear the audit trail and modify or delete user PINs to authorized administrators.

5.1.15 Revocation Requirements

The Revocation Requirements for the Sentinel TOE are described against the FMT_REV Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FMT_REV.1 Revocation

The specific requirement for this component is described in paragraph 5.1.15.1, below.

5.1.15.1 FMT_REV.1 Revocation

This security requirement is stated as:

A. FMT_REV.1.1

The TSF shall restrict the ability to revoke security attributes associated with the authorized users within the TSC to authorized administrators.

B. FMT_REV.1.2

The TSF shall enforce the rules for the revocation of all user security attributes through the deletion of the user PIN by an authorized administrator.

5.1.16 Security Management Roles Requirement

The Security Management Roles Requirement for the Sentinel TOE are described against the FMT_SMR Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FMT_SMR.2 Restrictions on security roles

The specific requirement for this component is described in paragraph 5.1.16.1, below.

5.1.16.1 FMT_SMR.2 Restrictions on Security Roles

This security requirement is stated as:

A. FMT_SMR.2.1

The TSF shall maintain the roles:

1) **Authorized administrator; and**
2) **Authorized users.**

B. FMT_SMR.2.2

The TSF shall be able to associate users *and administrators* with roles.

C. FMT_SMR.2.3

The TSF shall ensure that the conditions listed are satisfied.

1. **An authorized user cannot be an authorized administrator and an authorized administrator cannot be an authorized user within the same system.**
2. **The authorized user role can only be initiated after the user's Smart Card is validated for the user role and user identification and authentication is successfully completed.**
3. **The authorized administrator role can only be initiated after the administrator's Smart Card is validated for the administrator role and administrator identification is successfully completed.**

5.1.17 Fail Secure Requirements

The Fail Secure Requirement for the Sentinel TOE are described against the FPT_FLS Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FPT_FLS.1 Failure with preservation of secure state

The specific requirement for this component is described in paragraph 5.1.18.1, below.

5.1.17.1 FPT_FLS.1 Failure with Preservation of Secure State

This security requirement is stated as:

A. FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur:

a) Failure of any or all of the electronic components in the TOE.

b) Power failure to Security Module.

c) Failure or malfunction of any software including operating systems and applications on host computer or workstation during operations at any restricted level.

5.1.18 TSF Physical Protection Requirements

The TSF Physical Protection Requirement for the Sentinel TOE are described against the FPT_PHP Family of requirements defined in Part 2 of the CC Version 2.1 for the following:

FPT_PHP.3 Resistance to physical attack

The specific requirement for this component is described in paragraph 5.1.19.1, below.

5.1.18.1 FPT_PHP.3 Resistance to Physical Attack

This security requirement is stated as:

A. FPT_PHP.3.1

The TSF shall resist any attempts to gain information relating to the program that defines the TSP and/or TOE audit data through physical or electrical attacks to the Security Module and its Secure Microcontroller by responding automatically such that the TSP is not violated.

5.1.19 Reference Mediation Requirements

The Reference Mediation Requirement for the Sentinel TOE are described against the FPT_RVM Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FPT_RVM.1 Non-bypassability of the TSP

The specific requirement for this component is described in paragraph 5.1.20.1, below.

5.1.19.1 FPT_RVM.1 Non-bypassability of the TSP

This security requirement is stated as:

A. FPT_RVM.1.1

The TSF shall ensure that the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.20 Domain Separation Requirements

The Domain Separation Requirement for the Sentinel TOE are described against the FPT_SEP Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FPT_SEP.1 TSF domain separation

The specific requirement for this component is described in paragraph 5.1.21.1, below

5.1.20.1 FPT_SEP.1 TSF Domain Separation

This security requirement is stated as:

A. FPT_SEP.1.1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by un-trusted subjects.

B. FPT_SEP.1.2

The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.21 Time Stamps Requirements

The Time Stamps Requirement for the Sentinel TOE are described against the FPT_STM Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FPT_STM.1 Reliable time stamps

The specific requirement for this component is described in paragraph 5.1.22.1, below

5.1.21.1 FPT_STM.1 Reliable Time Stamps

This security requirement is stated as:

A. FPT_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use.

5.1.22 Limitation on Scope of Selectable Attributes Requirement

The Limitation on Scope of Selectable Attributes Requirement for the Sentinel TOE are described against the FTA_LSA Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FTA_LSA.1 Limitation on scope of selectable attributes

The specific requirement for this component is described in paragraph 5.1.23.1, below

5.1.22.1 FTA_LSA.1 Limitation on Scope of Selectable Attributes

This security requirement is stated as:

A. FTA_LSA.1.1

The TSF shall restrict the scope of the session security attributes consisting of clearance level and access rights based on time of day.

5.1.23 TOE Session Establishment Requirement

The TOE Session Establishment Requirement Requirement for the Sentinel TOE is described against the FTA_TSE Family of requirements defined in Part 2 of the CC Version 2.1 for the following components:

FTA_TSE.1 TOE session establishment

The specific requirement for this component is described in paragraph 5.1.25.1, below

5.1.23.1 FTA_TSE.1 TOE Session Establishment

This security requirement is stated as:

FTA_TSE.1.1

The TSF shall be able to deny session establishment based on:

a) Failure to identify and authenticate Smart Card; or

b) Failure of Identification; or

c) Failure of Authentication; or

d) Failure to accept user clearance level.

5.2 TOE Security Assurance Requirements

With respect to the Threat defined in paragraph 3.6.2, the TOE will need to implement counter-measures based on security functions that are, as a whole, of at least medium strength. Based on this, it is believed that the overall Strength of Function Level for the ST is at least SOF Medium. In addition, the complexity of the TOE and the risks associated with the threat environment will require an assurance level of EAL 4. Table 5.3 gives the security assurance requirements for the Sentinel. Assurance requirement components at EAL 4.

Table 5.3 Sentinel Security Assurance Requirements

Assurance Requirement	Description
ACM_AUT.1	Partial Configuration Management (CM) Automation
ACM_CAP.4	Generation Support and Acceptance Procedures
ACM_SCP.2	Problem Tracking CM Coverage
ADO_DEL.2	Detection of Modification
ADO_IGS.1	Installation, Generation, and Start-up Procedures
ADV_FSP.2	Fully Defined External Interfaces
ADV_HLD.2	Security Enforcing High-Level Design
ADV_IMP.1	Subset of Implementation Representation of the TSF
ADV_LLD.1	Descriptive Low-Level Design
ADV_RCR.1	Informal Correspondence Demonstration
ADV_SPM.1	Informal TOE Security Policy Model
AGD_ADM.1	Administrator Guidance
AGD_USR.1	User Guidance
ALC_DVS.1	Identification of Security Measures
ALC_LCD.1	Developer Defined Life Cycle Model
ALC_TAT.1	Well Defined Development Tools
ATE_COV.2	Security Testing: Coverage
ATE_DPT.1	Security Testing: Depth
ATE_FUN.1	Functional Testing
ATE_IND.2	Independent Testing – Sample
AVA_MSU.2	Validation of Analysis
AVA_SOF.1	Strength of TOE Security Function
AVA_VLA.2	Independent Vulnerability Analysis

5.3 Security Requirements Rationale

This section of the ST will describe how the Security Objectives described in paragraph 4.1 can be traced to each of the TOE Security Requirements and how the TOE Security

Objectives address each security requirement. The mapping of the TOE Security Objectives to the TOE Security Requirements is shown in Table 5.4. A description of how each TOE Security Objectives is supported by the TOE Security Requirements is described in the paragraphs below. When Table 5.4 is coupled with the paragraph 4.3 Security Objectives Rationale, the relationship between TOE Security Requirements, TOE Security Objectives, Threats, Organizational Security Policy, and Assumptions is clearly traceable. The mapping of security requirements to security objectives, to threats, to organizational security policy, and to assumptions clearly demonstrates how the TOE Security Requirements are internally consistent and form a mutually supportive whole.

Table 5.4 TOE Security Objectives v TOE Security Requirements

TOE Security Objectives	TOE Security Requirement
[O.IDENTIFICATION]	FIA_ATD.1, FIA_SOS.1, FIA_UID.2, FMT_MSA.2, FTA_TSE.1,
[O.AUTHENTICATION]	FIA_ATD.1, FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.7, FMT_MSA.2, FTA_TSE.1
[O.HBAC]	FDP_ACC.2, FDP_ACF.1, FIA_USB.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1, FMT_SMR.2, FTA_LSA.1, FTA_TSE.1, FPT_STM.1
[O.RESIDUAL_INFO]	FDP_RIP.1
[O.AUDIT]	FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4, FPT_STM.1
[O.ENFORCEMENT]	FPT_RVM.1
[O.TOE_PROTECT]	FPT_PHP.3
[O.FAILSAFE]	FPT_FLS.1
[O.SEPARATION]	FPT_SEP.1

5.3.1.[O.IDENTIFICATION] v TOE Security Requirements

The combination of the FIA_ATD.1, FIA_SOS.1, FIA_UID.2, FMT_MSA.2, and FTA_TSE.1 security requirements provide the functionality needed to support the [O.IDENTIFICATION] objective. The FIA_ATD.1 requirement defines the need for a PIN; FIA_SOS.1 requires the PIN to meet a minimum level of secrecy; FIA_UID.2 supports the

requirement that restricted data cannot be accessed unless the identification process is successfully completed; FMT_MSA.2 supports a requirement for high assurance and administrator control of user PIN identification data that is met by the use of a secure token; and FTA_TSE.1 supports the use of a Smart Card keyed to the TOE as a Secure Token.

5.3.2 [O.AUTHENTICATION] v TOE Security Requirements

The combination of the FIA_ATD.1, FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.7, FMT_MSA.2, and FTA_TSE.1 security requirements provide the functionality needed to support the [O.AUTHENTICATION] objective. The FIA_ATD.1 requirement defines the need for a password; FIA_AFL.1 protects against password guessing and brute force attacks based on trial and error; FIA_SOS.1 requires the password to meet a minimum level of secrecy; FIA_UAU.2 requires authentication to be successfully completed before restricted data and processes can be accessed; FIA_UAU.7 requires the password to be protected against observation; FMT_MSA.2 supports a requirement for a secure password controlled by the user.

5.3.3 [O.HBAC] v TOE Security Requirements

The combination of the FDP_ACC.2, FDP_ACF.1, FIA_USB.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1, FMT_SAR.2, FTA_LSA.1, FTA_TSE.1, and FPT_STM.1 security requirements provide the functionality needed to support the [O.HBAC] objective. The FDP_ACC.2 requirement defines HBAC as the complete access control policy to be implemented by the TOE; FDP_ACF.1 defines the HBAC rules including those under [O.HBAC]; FDP_USB.1 defines the linkage of the user's security attributes with the user via the user's secure token; FMT_MSA.1 and FMT_MSA.3 defines the requirement for access to and management of security attributes under HBAC; FMT_MTD.1 defines the requirement for access to and control over the clearing of audit data and the deletion of a user's PIN under HBAC; FMT_REV.1 defines the requirement for access to and revocation of user security attributes under HBAC; FMT_SMR.2 defines how roles are implemented via HBAC; FTA_LSA.1 defines the requirement for restricting user access based on their clearance and rights at a defined time of day; FTA_TSE.1 defines the conditions under which user access under HBAC will be denied; and FPT_STM.1 defines how HBAC will determine time of day.

5.3.4 [O.RESIDUAL_INFO] v TOE Security Requirements

The FDP_RIP.1 security requirement supports the [O.RESIDUAL_INFO] objective by requiring a subset of all previous information processed or accessed by a user using all available resources to be unavailable after the objects used by these resources are reallocated to a new user.

5.3.5 [O.AUDIT] v TOE Security Requirements

The combination of the FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4, and FPT_STM.1 security requirements provide the functionality needed to support the [O.AUDIT] objective. The FAU_GEN.1 requirement defines the audit data that must be generated and recorded during a user session; FAU_GEN.2 defines the requirement for audit data user identity; FAU_SAR.1 defines the requirement for the review of audit data; FAU_SAR.2 defines the requirement for restricting audit data access to only authorized users; FAU_STG.1 defines the requirement for the protection of audit data against modification or deletion by unauthorized users; FAU_STG.4 defines the requirement for the prevention of audit data loss due to storage overflow; and FPT_STM.1 defines the requirement for time stamps.

5.3.6 [O.ENFORCEMENT] v TOE Security Requirements

The FPT_RVM.1 security requirement supports the [O.ENFORCEMENT] objective by requiring the TOE Security Policy to be incapable of being bypassed in any manner. In essence the enforcement of the TOE Security Policy requires each security function to be implemented in sequence before the next function can proceed.

5.3.7 [O.TOE_PROTECT] v TOE Security Requirements

The FPT_PHP.3 security requirement supports the [O.TOE_PROTECT] objective by requiring the program that defines the TOE Security Policy to be protected from unauthorized access by means of physical or electrical attacks to the Security Module.

5.3.8 [O.FAILSAFE] v TOE Security Requirements

The FPT_FLS.1 security requirement supports the [O.FAILSAFE] objective by requiring the TOE to maintain a secure state after any failure to the electronic components in the TOE, power failures to Security Module, or the failure of any host software or hardware.

5.3.9 [O.SEPARATION] v TOE Security Requirements

The FPT_SEP.1 security requirement supports the [O.SEPARATION] objective by requiring separation between security domains so that all data stored or processed by objects during a session must be at the sensitivity level of the domain.

5.4 Security Requirements Dependencies

Many of the Security Functional Requirements taken from the CC that are listed in Section 5.1, depend on other Security Functional and Assurance Requirements that also must be selected. These are identified in Table 5.5 which shows how dependency requirements are met.

In some cases the dependent security functions are hierarchical under other functions in the same family, such as FIA_UAU.1 and FIA_UAU.2. If the ST functional requirement is dependent on a functional requirement not in the ST but is hierarchically below a functional requirement that is in the ST, both will be listed since either can support the dependency requirement. In the case of the previous example, this is represented in Table 5.5 as FIA_UAU.1/UAU.2. When this is taken into account, is seen that each of the dependent security functional requirements defined in the middle column of Table 5.5 are within the ST as is seen from their listing in the left column. This indicates that all dependencies based on security functional requirements are addressed.

The only dependent security assurance requirement as seen from Table 5.5 is the ADV_SPM.1 Informal TOE Security Policy Model. This requirement is addressed in the Security Target as described in paragraph 6.2.25. Based on this analysis it is clear that all ST dependency requirements are addressed.

Table 5.5 Functional Requirements Dependencies

ST Security Functional Reqmts.	Dependent Security Functional Reqmts.	Dependent Security Assurance Reqmts.
FAU_GEN.1	FPT_STM.1	None
FAU_GEN.2	FAU_GEN.1 and FIA_UID.1	None
FAU_SAR.1	FAU_GEN.1	None
FAU_SAR.2	FAU_SAR.1	None
FAU_STG.1	FAU_GEN.1	None
FAU_STG.4	FAU_STG.1	None
FDP_ACC.2	FDP_ACF.1	None
FDP_ACF.1	FDP_ACC.1/ACC.2 and FMT_MSA.3	None
FDP_RIP.1	None	None
FIA_AFL.1	FIA_UAU.1/ UAU.2	None
FIA_ATD.1	None	None
FIA_SOS.1	None	None
FIA_UAU.2	FIA_UID.1/UID2	None
FIA_UAU.7	FIA_UAU.1/ UAU.2	None
FIA_UID.2	None	None
FIA_USB.1	FIA_ATD.1	None
FMT_MSA.1	FDP_ACC.1/ACC.2 and FMT_SMR.1	None
FMT_MSA.2	FDP_ACC.1/ACC.2, FMT_MSA.1 & FMT_SMR.1/SMR.2	ADV_SPM.1
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	None
FMT_MTD.1	FMT_SMR.1/SMR.2	None
FMT_REV.1	FMT_SMR.1/SMR.2	None
FMT_SMR.2	FIA_UID.1/UID2	None
FPT_FLS.1	None	ADV_SPM.1
FPT_PHP.3	None	None
FPT_RVM.1	None	None
FPT_SEP.1	None	None
FPT_STM.1	None	None
FTA_LSA.1	None	None
FTA_TSE.1	None	None

CHAPTER 6. Target of Evaluation Summary Specification

6.0 Introduction

This chapter relates the Sentinel security functions, mechanisms, and techniques described in paragraph 2.2.1 of this document to the ST functional requirements defined in Chapter 5 and the policies, threats, and assumptions described in Chapter 3 of this document. The compliance of the ST with the EAL 4 level Assurance Measures is also described.

6.1 TOE Security Functions

This section will relate to each ST security requirement by defining and describing the security functions, mechanisms, and techniques that support each security requirement given in Chapter 5. The strength of function of these functions is SOF-medium.

6.1.1 FAU_GEN.1 Audit Data Generation

The Sentinel TOE complies with all ST Audit Data Generation Requirements. This is demonstrated by Table 6.1, which lists the actual audit data generated within the TOE and matches it against the requirements in Table 5.2. As described in paragraph 2.2.1D all the audit events are recorded against the user's PIN, time stamp for each event, type of event, and the success or failure of the event. This is in accordance with the ST requirement in paragraph 5.1.1.1 that requires date and time of the event, type of event, subject (user or administrator) identity, and the outcome (success or failure) of the event. The TOE implementation of the audit data requirement is based on the list of auditable events provided by the Sentinel TOE as listed in paragraph 2.2.1D.

The audit data generated within the TOE by the Security Module is extensive and relates primarily to the I&A and Access Control events during the logon process to a restricted domain by a user and the administration tasks performed by the Security Administrator. All audit data requirements relating to controlled objects and subjects are defined in relation to the TOE's control over the RHDD data storage object and the NIC, Modem, and USB port data communications objects and authorized users selecting a set of active security attributes during a

Table 6.1 Implementation of Audit Data Requirements

Component	Requirement	TOE Implementation
FAU_GEN.1	Start-up and shutdown of the audit functions.	1st logon and last logon transactions with time/date stamp.
FAU_SAR.1	Reading of information from the audit records.	Audit Data Download Initiated and completed with time/date stamps.
FAU_SAR.2	Unsuccessful attempts to read information from the audit records.	Audit Data Incomplete with time/date stamp.
FAU_STG.4	Actions taken due to audit storage failure.	Shutdown of Security Module with time/date stamp
FDP_ACF.1	The specific security attributes used in making an access check.	Success or failure of Security Profile transactions with time/date stamp
FIA_AFL.1	The reaching of the threshold (3 attempts) for the unsuccessful authentication attempts and the subsequent implementation of a default state.	Success or failure of all password transactions for all identified users with time/date stamp and the termination of a session after 3 unsuccessful attempts.
FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret.	Success or failure of all PIN and Password transactions with time/date stamp
FIA_UAU.2	All use of the authentication mechanism.	Success or failure of all password transactions with time/date stamp.
FIA_UID.2	All use of the user identification mechanism.	Success or failure of all PIN transactions with time/date stamp.
FIA_USB.1	Success and failure of binding user security attributes to a subject.	Success or failure of Security Profile transactions with time/date stamp.
FMT_MSA.1	All modifications of the values of security attributes.	Change Password transaction by user and Change PIN transaction by administrator with time/date stamps.
FMT_MSA.2	All offered and accepted secure values of security attributes.	Password and PIN change completion with time/date stamp.
FMT_MSA. 3	Modifications of the default setting of restrictive rules. All modifications of the values of security attributes.	User security profile settings. Change Password transaction by user and Change PIN transaction by administrator with time/date stamps.
FMT_MTD.1	All modifications to values of TSF data.	All successful completion of audit data downloads and PIN changes by administrator with time/date stamp.
FMT_REV.1	All attempts to revoke security attributes.	Attempted changes of user PIN by Security Administrator that are not within the normal routine as shown by time/date stamp.
FMT_SMR.2	Every use of the rights of a role.	Security domain selection by user and PIN change and Audit Data transactions by administrator with time/date stamp ..
FPT_FLS.1	Failure of the TSF *as indicated by a failure to properly implement security profile in accordance with TSP*.	Failure to implement security profile selected coupled with user security profile that should have enabled the selection with time/date stamp.
FPT_STM.1	Providing a timestamp	The time/date stamp for all events
FTA_LSA.1	All attempts at selecting a session security attributes.	Attempts to implement denied security profile based on time with time/date stamp.
FTA_TSE.1	All attempts at establishment of a user session.	All successful and unsuccessful user ID, Password, and Security Profile transactions with time/date stamp.

user session. Finally, it is clear that some of the audit data requirements are met when the audit data provided by the TOE is combined or is interpreted based on knowledge of TOE operations, capabilities, and limitations.

6.1.2 FAU_GEN.2 User Identity Association

The Sentinel TOE complies with all ST User Identity Association Requirements. During initial logon a user inserts their Smart Card into the Security Module for validation of the card as being acceptable. If the Machine Authorization Code on the Smart Card matches the code stored in the Security Module's Secure Microcontroller the Smart Card is validated and the user is requested to enter their PIN. The PIN entered from the keyboard is encrypted by the Secure Microcontroller and compared with the encrypted PIN stored on the Smart Card. If the PIN comparison is successful the user will then be requested to enter their password. A user is allowed 3 attempts at entering the correct PIN before the Security Module goes into a default mode in which the host computer is either powered off or the unrestricted domain is enabled. The option for either is not user selectable since it is a policy option that must be specified at the time the Security Module is manufactured. Once the PIN is validated the Security Module will apply the PIN to all audited events under the control of the Security Module until the user logs off the host computer. This includes the selection of a restricted security domain by the user and the authorization for that domain by the Security Module as determined from the user's security profile on their Smart Card.

6.1.3 FAU_SAR.1 Audit Review

The Sentinel TOE complies with all ST Audit Review Requirements. Audit data for all events under the control of the Security Module is stored within the memory of the Secure Microcontroller as an encrypted CSV file that can only be accessed by the Security Administrator via their Administrator Smart Card. The Security Administrator has sole access to the stored audit data, which is stored as an encrypted file when the Security Module is inactive. Access to the audit data requires the Security Administrator to logon to the Security Module using their Administrator Smart Card with its Security Administrator Profile. Once the Smart Card is recognized as an admin card the Security Administrator will be required to enter their

PIN. When the PIN is validated against the encrypted PIN stored on the card, the administrator will select an allowed admin procedure from their Administrator Profile such as downloading audit data from the Security Module to their Smart Card. This is initiated by selecting the "(D)ownload Audit Data" profile by depressing the "D" key on the keyboard.. Audit data is downloaded on a byte-by-byte basis. Any failure during an audit data download will not effect the integrity of the audit data since it is still retained in the Secure Microcontroller. However, the process will need to be repeated since the downloaded data file would be incomplete, possibly corrupted or inaccessible, with the loss of the last byte of data.

6.1.4 FAU_SAR.2 Restricted Audit Review

The Sentinel TOE complies with all ST Restricted Audit Review Requirements. This includes protecting all audit data in the Security Module from unauthorized access. The Security Module protects this data by only allowing a user with a valid Smart Card that has an administrator profile to access the data. This requirement is met only by designated Security Administrators who logon to the Security Module and are only allowed access to their administrator profile. The administrator profile allows them to change user PINs and download Audit Data. Users only have a security profile that allows access to restricted domains so they are unable to access the stored audit data. Further protection of the audit data is provided by the encryption of the data while it is stored in the Secure Microcontroller and the tamper proofing of the Secure Microcontroller.

6.1.5 FAU_STG.1 Guarantees of Audit Data Availability

The Sentinel TOE complies with all ST Audit Data Availability Requirements. Audit data within the Secure Microcontroller can only be accessed by a Security Administrator with a Smart Card that has the admin profile. In addition, the only administrative task allowed is the downloading of the data. There is no mechanism that allows the data to be modified or deleted until a successful download is completed.

6.1.6 FAU_STG.4 Prevention of Audit Data Loss

The Sentinel TOE complies with all ST Requirements for the Prevention of Audit Data Loss. Audit data stored in the Secure Microcontroller is very limited when compared to the data

that can be stored on the RHDDs. It is most important that this data be preserved so that when memory capacity is reached the existing data cannot be destroyed by new audit data. The Secure Microcontroller continually monitors the status of its memory storage and provides alarms when the memory is at 90% and 95% of capacity. These alarms request the user to inform the Security Administrator that a download of audit data is necessary. At 99% of capacity the Secure Microcontroller will disable any further logons by users until the audit data is downloaded by the Security Administrator. This prevents the loss of any audit data as required.

6.1.7 FDP_ACC.2 Complete Access Control

The Sentinel TOE complies with all ST Complete Access Control Policy Requirements. This requires that all operations between a subject and objects in the TSC to be controlled by a TSF within the access control SFP. The HBAC TSF within the Sentinel TOE is implemented within the Security Module and the firmware in its internal Secure Microcontroller that stores the TSP. In essence the Security Module controls an authorized user's access to a restricted domain at a single sensitivity level. The authorized user operates as the controlled subject through the process of being bound to selected attributes stored on the user's Smart Card and to the TOE itself. This binding is performed by the TOE which first determines that the Smart Card is validated for use with the Security Module through its Machine Authorization Code. The user is then identified by their role attribute on their Smart Card and as the owner of the Smart Card by entering their PIN and comparing it against the PIN stored on the Smart Card. If the role attribute and PIN identify and authenticate the controlled subject as an Authorized "Administrator" they can than perform only allowed Administrator functions. A subject that has the "User" role attribute is authenticated to the TOE as an authorized user with the attributes on the Smart Card by entering a password which is authenticated against the password stored within the Security Module. The Authorized User then selects the level of clearance and the access rights attributes for the user session. If the TOE accepts this selection the Authorized User becomes a controlled subject with the attributes selected during the access control process. In addition to the selected attributes, some attributes can be invoked through external conditions such as Time of Day which could change an Authorized User's access to each object depending upon when the user

session is initiated. The controlled subject is singular during the length of a user session since no other subject can exist.

A restricted domain is defined by the controlled objects that a controlled subject can access within the domain during a user session. The HBAC TSF controls this access for all objects within the TSC by invoking access rules that apply to the subject for each class of object. These rules are defined as follows:

1. Access by a controlled subject to the controlled RHDD data storage object within the TSC is allowed if the subject operating as an Authorized User has a level of clearance that is equal to the level of sensitivity of the RHDD when the user session was initiated and the RHDD is valid for operations with the TOE.

2. Access by a controlled subject to a controlled data communications object within the TSC including a NIC, Modem, and/or USB port is allowed if the subject operating as an Authorized User has access rights at the level of sensitivity of the controlled object that is equal to the access rights of the object.

3. Access by a controlled subject to any controlled R/W data storage object within the TSC, other than an RHDD, and including a HDD, FDD, R/W CD, R/W DVD, or Zip type drive is not allowed at any restricted security level.

4. Access by any subject to any Read-Only data storage object including a CD or DVD Drive within the TSC is always allowed.

5. Access to PIN and Audit Data stored within the TOE and to NVMs shared between security levels is only allowed to a controlled subject operating as an authorized administrator.

6. Access to any unrestricted object is allowed for a subject when operating at any unrestricted security level.

The Security Module controls the access of any controlled subject operating as an authorized user to the controlled RHDD data storage object by sending an activation signal to the RHDD based on the clearance level of the controlled subject as read from the Smart Card. If the

RHDD returns the same signal, access is pre-enabled, otherwise access is denied. In addition, the Security Module interrogates the RHDD for its ID which must match an ID within the Security Module for the enabling of RHDD access to be completed. Access to a controlled data communications subject requires successful completion of the RHDD access control process and a subject with access rights to the selected object at the level of clearance of the RHDD as determined from the subject's Smart Card. The Security Module will also automatically disable any R/W Disk Drives if an RHDD is successfully accessed by a subject. All Read-Only Disk Drives are enabled for operations at any security level. Access to PIN and Audit data and to NVMs shared between security levels is restricted by the Security Module to authorized administrators. In addition, authorized administrators have no access to the RHDD restricted data storage objects or restricted data communications objects. Since all operations between the controlled objects and subjects is clearly controlled by the HBAC SFP, the Complete Access Control requirements are met.

6.1.8 FDP_ACF.1 Security Attribute Based Access Control

The Sentinel TOE Access Control as described in paragraph 2.2.1 addresses all of the ST Access Control requirements defined for Security Attribute Based Access Control in accordance with CC component FDP_ACF.1. Table 6.2, below will match each of the FDP_ACF.1 requirements listed in paragraph 5.1.5.1 against the implementing security functions within the TOE as supported by the Chapter 2 TOE Description. It is clear from this comparison that all of the requirements for Security Attribute Based Access Control are met by the HBAC SFP implemented within the Security Module of the TOE.

Table 6.2 Implementation of Access Control Requirements

ST Requirement Paragraph	TOE Security Function Description	TOE Description Paragraph
5.1.5.1A.1	A subjects clearance, access rights to data communications objects, role, and time based attributes from Smart Card plus Sensitivity level and ID of RHDD from RHDD label and Time of Day from the Secure Microcontroller Real TimeClock are processed by the HBAC TSF instructions in the Secure Microcontroller as security attributes that control access to objects.	1.2, 2.2, 2.2.1, 2.2.2A, 2.2.2B & 2.3.1B

ST Requirement Paragraph	TOE Security Function Description	TOE Description Paragraph
5.1.5.1B.1	The HBAC TSF will only enable a restricted security level selected by a subject if an RHDD with a valid ID and an electronic sensitivity label at the required sensitivity level is installed in the computer	1.2, 2.2.1, 2.2.2A, 2.2.2B, 2.3.1B
5.1.5.1B.2	The HBAC TSF will only allow a controlled subject to gain access to a RHDD data storage object if the RHDD's ID is validated by the Secure Microcontroller and the subjects active clearance attribute as read by the Secure Microcontroller from the subject's Smart Card is equal to the sensitivity level of the RHDD as determined by the Secure Microcontroller from the RHDDs electronic sensitivity label at the time of logon.	1.2, 2.2.1, 2.2.2A, 2.2.2B & 2.3.1B
5.1.5.1B.3	The HBAC TSF will only allow a controlled subject to gain access to a data communications object such as a NIC, Modem, and/or USB port if the data communications object is installed in the computer along with a RHDD with a valid ID and a sensitivity label that is equal to the clearance level attribute of the subject and the access rights of the subject as read from the subject's Smart Card allow access to the subject at the time of logon.	1.2, 1.5, 2.2.1, 2.2.2A, & 2.3.1B
5.1.5.1C1.	The HBAC TSF will allow any Read Only data storage object such as a CD or DVD Drive to be accessed by any subject at a restricted security level if the restricted security level is enabled with an installed RHDD with a valid ID and an electronic sensitivity level label that is equal to the active clearance level of the subject.	1.2, 1.5, 2.2.1, 2.2.2C & 2.3.1B
5.1.5.1C2.	The HBAC TSF will allow a controlled subject operating as an authorized administrator to have access to User PIN and Audit Data stored within the TOE and to NVMs shared between security levels.	1.2, 1.5, 2.2.1, 2.2.2A, 2.2.2D & 2.3.1E
5.1.5.1C3	The HBAC TSF will allow any subject operating at an unrestricted security level access to any unrestricted Object by default.	1.2, 1.5, 2.2.1, 2.2.2A &2.2.2B
5.1.5.1D1.	The HBAC TSF will not allow any subject to access a R/W data storage object other than a valid RHDD during any operations performed at a restricted security level.	1.2, 1.5, 2.2.1, 2.2.2C & 2.3.1B
5.1.5.1D2	The HBAC TSF will not allow any subject other than an authorized administrator access to PIN and Audit Data or to NVMs shared between security levels.	1.2, 1.5, 2.2.1, 2.2.2A, 2.2.2D & 2.3.1E
5.1.5.1D3.	The HBAC TSF will not allow a controlled subject operating as an authorized administrator access to any data storage or data communications objects at a restricted security level.	1.2, 1.5, 2.2.1, 2.2.2A, 2.2.2B, & 2.3.1E

6.1.9 FDP_RIP.1 Complete Residual Information Protection

The Sentinel TOE complies with all ST Subset Residual Information Protection Requirements with respect to ensuring that there are no resources capable of retaining

information that could be accessed after objects within the TSC, with the single exception of the RHDD, are reallocated to another user. This protection is inherent in the operation of the Sentinel with respect to all R/W data storage devices within the TSC, with the single exception of the RHDDs, since these devices are disabled during operations in a restricted domain. In addition, the devices that are enabled in restricted domains such as the Non-Volatile Memories (NVMs), Volatile Memories, Data Communications Objects, and Read-Only Memories are prevented from storing Residual Information by the TOE. In the case of NVMs, they are prevented from storing any user data based on the HBAC rules described in paragraph 5.1.5.1C.2. and paragraph 6.1.7. Volatile Memories such as RAM that are utilized during a user session are erased when the user logs off and the computer and all resources are powered off. The next user begins their session with all resources cleared. Since this logoff and power down procedure is required before another session can begin there is never any possibility of accessing any residual information. Read-Only Data Storage Devices such as CDs or DVDs cannot store data by their very nature so they present no residual information protection issues. Finally, Data Communications Objects have no non-volatile storage capability but if they did it would be in the form of an NVM which is already protected as described above.

The allocation of the RHDDs is under the control of the TSC via the level detection and ID validation circuitry in the RHDD thus preventing an unauthorized user from getting access to the data of an authorized user of the RHDD. In addition, if the RHDDs are shared with more than one user the presumption is that all of these users have authorized access to the stored data and, therefore, such data is not generally a security issue. However, RHDDs do not technically meet the residual information protection requirement since any data used during a session is not erased by the operating system even if deleted by the user.

6.1.10 FIA_AFL.1 Authentication Failures

The Sentinel TOE complies with all ST Authentication Failure Requirements through the policy implemented by the Security Module during user logon. A user is only able to authenticate themselves after previously having successfully completed the Identification Process. During the Authentication Process the user’s Smart Card continues to be inserted in the

Smart Card Reader slot of the Security Module. The LCD Module will request the user to enter their password after successfully completing the PIN entry process during Identification. A user will enter the password from the keyboard and the Security Module's Secure Microcontroller will determine if it matches the password stored in its memory for that user. The user's password is linked in the Secure Microcontrollers memory to the previously verified PIN. If the password is not the same as that which was stored the user will be requested to reenter the password. No feedback is provided to a user as to the reason the password is being rejected and all password entries are displayed as asterisks so they are obscured. After three unsuccessful attempts the Security Module will default to a secure state that can either be the unrestricted domain of a power off of the host computer. The choice of the default state is selected by the organization as a policy since it is programmed into the Secure Microcontroller firmware prior to delivery of the Sentinel.

6.1.11 FIA_ATD.1 User Attribute Definition

The Sentinel TOE complies with all ST User Attribute Definition Requirements with respect to individual users including User Identifier and Authentication Data. Within the Sentinel TOE the Security Module maintains a record of the user's PIN and password in the memory of the Secure Microcontroller as well as Time of Day. While these are the only user attributes that are stored within the TOE, users can have other attributes that are stored on their Smart Card such as clearance and access rights. It should be noted that a user's PIN is stored in both the Secure Microcontroller and the Smart Card. The Smart Card also stores a Machine Authorization Code that is also stored in the Secure Microcontroller and is used to validate the Smart Card Token as being authentic.

By authenticating the Smart Card Token and the owner of that token the Security Module will accept the additional User Security Attributes stored on the Smart Card as belonging to the authenticated user. In this manner the user's clearance and access rights become security attributes for the user during the established session. These attributes are under the control of the administrator and not the user and can be easily be reprogrammed as circumstances demand. The PIN is also under the control of the administrator who can periodically change it in the Secure Microcontroller as long as the same changes are made to the PIN stored on the user's Smart

Card. Deletion of a PIN in the Secure Microcontroller or modifications that are not also implemented on the user's Smart Card will effectively terminate a user's access to the TOE. Passwords are under the control of the user who can modify their password during any session logon. By allowing passwords to only be available to the user a single point of potential vulnerability is eliminated since the administrator cannot also become a user of the TOE.

6.1.12 FIA_SOS.1 Strength of Authentication Data

The Sentinel TOE complies with all ST Strength of Authentication Data Requirements through the Security Module's use of a user password of at least 8 alphanumeric characters. For an initial attempt to use the authentication mechanism, the probability that a random attempt will succeed is 1 in 36^8 or 1:2,821,109,907,456. After multiple attempts to use the authentication mechanism during a one-minute period, the probability that a random attempt during that minute will succeed is 1:470,184,984,576. These probabilities are well beyond what is required by the ST. The Security Module also does not provide any feedback to the user for failed password entries. It should also be noted that the function is strengthened by the limitation on authentication attempts that will continually cause the host computer or PC to revert to the default state after every three bad attempts. This will certainly slow the progress of any brute force effort. Because of this it is believed that the Strength of Function for this component is high.

6.1.13 FIA_UAU.2 User Authentication Before Any Action

The Sentinel TOE complies with all ST User Authentication before Any Action Requirements. Authentication of a user is a necessary condition before the Security Module will accept data from the Smart Card and the user relating to the enabling of a domain at a selected sensitivity level followed by the selection of the controlled objects in the domain. During this process the TSP in the Secure Microcontroller will mediate the domain selected by comparing the users security clearance and access rights against the attribute requirements of the domain. After authentication, the TSP will allow a user to change their current password. If this option is not selected, the user will select the restricted domain to be accessed. The TSP will then mediate access to the domain based on the security attributes of the user and the selected domain. Non-

mediated actions after authentication are limited to system power down after removal of the user's Smart Card.

6.1.14 FIA_UAU.7 Protected Authentication Feedback

The Sentinel TOE complies with all ST User Authentication Feedback Requirements including obscuring the entry of password data by only displaying asterisks on the LCD Module as each character of a password is entered from the keyboard.

6.1.15 FIA_UID.2 User Identification Before Any Action

The Sentinel TOE complies with all ST User Identification Before Any Action Requirements. User identification through the entry of a PIN is the first procedure implemented by a user after inserting their Smart Card in the Security Module Smart Card Reader. The TSP implements a sequential process that requires a user to be successfully identified before they can proceed to the authentication process described in paragraph 6.1.13. User identification is a prerequisite for user authentication, which, as described in paragraph 6.1.13, must be completed before any action mediated by the Security Module on behalf of users. This means that user identification and authentication are both necessary before the TSP will implement any access mediation to restricted domains.

In the case of administrators, identification is the only requirement before the Security Module will allow the performance of any actions using the administrator profile. Administrators logon to the Sentinel by first inserting their Smart Card with its Administrator Profile in the Security Module Smart Card Reader. The Security Module recognizes the card as an administrator card and requires the entry of a PIN for identification. Upon successful entry of the PIN the TSP will present the administrator with their options which include changing user PINs or downloading audit data. Upon selection of either option the TSP will allow enable the requested task. Again, no action is allowed by the TSP until the identification process is successfully completed.

6.1.16 FIA_USB.1 User-Subject Binding

The Sentinel TOE complies with all ST User-Subject Binding Requirements. User-Subject binding is implemented at a very basic level by the TSC since the TSP essentially establishes a single restricted domain for a single user during each user session. Subjects are enabled when a user completes the I&A process and the access control process which allows an authorized user to assume a subset of the security attributes programmed on their Smart Card. These attributes allow the authorized user acting as a subject to perform operations at a selected security level based on the user's active security attributes and the attributes of controlled objects. In essence the subject is bound to the user through the security attributes that are read by the TOE from the authenticated user's Smart Card and then selected by the user for operations during a user session. Some attributes are also invoked or modified by the TOE based on time of day.

6.1.17 FMT_MSA.1 Management of Security Attributes

The Sentinel TOE complies with all ST requirements for the Management of Security Attributes. This includes the implementation of a TSP that implements HBAC as described in paragraphs 6.1.7 and 6.1.8. The TSP provides a capability to manage the PIN and password security attributes which, as described in paragraph 6.1.11, are the only security attributes managed directly within the TOE. Management of user PINs was controlled by the TSP via the administrator profile that was enabled when an authorized administrator was identified and then selected the (A)dministration option from the keyboard. If the (C)hange PIN option is selected the TSP will allow the administrator to modify or delete a user's current PIN. Password changes are enabled by the TSP immediately after authentication of the user. The authorized user is restricted by the TSP in the passwords that can be selected based on password metric requirements and restrictions against selecting the same password or a password that is identical to user's PIN.

6.1.18 FMT_MSA.2 Secure Security Attributes

The Sentinel TOE complies with all ST requirements for Secure Security Attributes. This requirement is met through various types of restrictions on imposed on password and PIN selection by the TSP. These include requirements that PINs be at least 6 alphanumeric characters in length while passwords must be at least 8 characters in length. Other restrictions include denying changes to passwords if the new password is the same as the current password or if it is identical to the user's PIN. Additional security is provided via the TSP by implementing an I&A process that requires the use of a validated Smart Card with an encrypted user PIN. In essence, this prevents an unauthorized user from defeating the I&A process by obtaining an authorized user's PIN and password unless they also gained access to their Smart Card.

6.1.19 FMT_MSA.3 Static Attribute Initialization

The Sentinel TOE complies with all ST requirements for Static Attribute Initialization. This requirement is addressed by the HBAC Policy that restricts access to users based on the security profile consisting of the security attributes programmed on their Smart Card. The default value of the security attributes is defined by a user with no Smart Card; a Smart Card without a valid Machine Authorization Code; a Smart Card without a valid PIN; or a valid Smart Card with no clearance or access rights. Any of these security attributes will cause the user to be restricted to the unrestricted domain and to only access or create data that is at the unrestricted level. Access to a restricted domain can only be implemented through the programming of the proper security attributes on the user's Smart Card by the Security Administrator. This will allow a user to access or create data at a restricted level of access.

6.1.20 FMT_MTD.1 Management of TSF Data

The Sentinel TOE complies with all ST requirements for the Management of TSF Data. Within the TOE, TSF data includes the audit data and user PIN data that can only be accessed by administrators via their administrator profile. The TSP implements this restriction by only enabling PIN changes and audit data access after an administrator has been identified through their Admin Smart Card and the entry of their PIN. Administrator PINs are similar to user PINs in that they are stored as an encrypted value in the Smart Card. The PIN entered from the

keyboard is then encrypted by the Secure Microcontroller and compared with the encrypted value read from the Admin Card. If they are identical the Administrator is allowed to select their administrator profile which includes the (C)hange PIN/(D)ownload Audit Data options. The PIN change option allows the administrator to change or delete the user PINs stored in the Secure Microcontroller. Similarly the download audit data option allows the administrator to download the audit data to their Smart Card thus clearing the audit trail and essentially deleting all the audit data from the Secure Microcontroller so that it can be reset.

6.1.21 FMT_REV.1 Revocation of User Attributes

The Sentinel TOE complies with all ST requirements for the Revocation of User Attributes. This capability is implemented within the Security Module by restricting the modification including the revocation of user security attributes to the Security Administrator. The Security Administrator has sole control over revocation, which is enabled within the TOE via the Change PIN option in the administrator profile. If a user's PIN is deleted from the Secure Microcontroller or is changed to a new value without also changing the PIN on the user's Smart Card the user can no longer be identified by the TSP. The result is that the user no longer has any security attributes that will be recognized by the TSP. In addition, all subject and object security attributes that relate to security clearance, access rights, sensitivity levels, or role are managed outside the TOE.

6.1.22 FMT_SMR.2 Restrictions on Security Roles

The Sentinel TOE complies with all ST requirements for Restrictions on Security Roles. This capability is implemented within the Security Module by the TSP that establishes separate user and administrator profiles based on the Smart Card validation process. After a Smart Card is inserted by an individual into the Security Module's Smart Card Reader, the Security Module determines if the card is validated for operations with that Security Module. This is done by checking the Machine Authorization Code against the codes stored in the memory of the Secure Microcontroller. If the code is valid the information on the Smart Card that identifies the available profile is read. Based on the type of profile on the card, the TSP will either invoke the

logon procedures and options for a user or an administrator. Since there is only one type of profile allowed on a Smart Card, an authenticated Smart Card user can only assume either the role of a user or the role of an administrator.

The logon procedures for a user as implemented by the TSP require that the user be identified through the entry of a valid PIN and then authenticated through the entry of a valid password before selecting the available user options. These include changing a user password or designating the restricted domain that the user wants to access. The logon procedures for an administrator only require entry of a valid PIN. This is done to prevent an administrator from having any control over passwords since these are designated as a security attribute that is managed and owned by users.

6.1.23 FPT_FLS.1 Failure with Preservation of Secure State

The Sentinel TOE complies with all ST requirements for Failure with Preservation of Secure State. This requirements is met through the design of the Asset Status Sensor and Controller Board, which ensures that any TOE component failures including the failure of the Secure Microcontroller cannot enable access to a domain at a higher security level than the selected domain. The failsafe mechanisms built into the board will prevent the failure of any component on the board from switching security levels after completion of successful login to a restricted domain. At the very worst a failure after login could cause a system lockup in which access to any restricted domain is denied until the system is powered off and the logon process for a restricted domain is repeated. If during subsequent login the indicator lights are incorrect with respect to the selected security level a “hard” failure would have occurred and maintenance will be required. Even should this go unnoticed there is no way for the TSP to be violated since both the level detection and ID validation circuitry in the RHDD would absolutely prevent this.

Power failures to the Security Module that did not also effect the host computer during login to a restricted domain would lockout access to all restricted domains. If the power failure occurred after login to a restricted domain the RHDD would lockup. In addition to the Asset Status Sensor and Controller Board other key level selecting components such as the S/C and I/O controller cards are also designed to fail in the power off mode so that a “hard” failure of the card isolates the component controlled by the card. Other types of failures in the S/C card are

certain to effect signal lines between the motherboard and the inserted device, which would certainly disable their operation. In reality it would take a statistically remote, if not impossible, combination of failures in the Security Module and the RHDD combined with some negligent or malicious activity of a user to violate the TSP. It should also be obvious that the isolation of the Security Module and the TSP from all host data processing hardware and software interfaces will absolutely prevent any software based failures, malfunctions, or malicious actions from effecting the secure state maintained by the TSP.

6.1.24 FPT_PHP.3 Resistance to Physical Attack

The Sentinel TOE complies with all ST requirements for Resistance to Physical Attack. This requirement is implemented through the design of the Secure Microcontroller in the Security Module that implements the TSP. The Secure Microcontroller is actually commercially available from Dallas Semiconductor as its DS2252T Secure Microcontroller Module. Protection of program information and stored data is implemented within the Secure Microcontroller by encrypting all Secure Microcontroller memory with a proprietary data encryption algorithm that is known only to the manufacturer. This encryption capability is enabled every time the module is powered down which occurs at the termination of each user session in a restricted domain. Additional protection is provided through the implementation of dummy instructions during the processing of the instructions that implement the TSP. This prevents the actual operations of the Secure Microcontroller from being monitored and interpreted while it is operating. Finally, the DS2252T has a very sophisticated tamper proofing mechanism that detects any attempt to discover the on-chip data, program information, and encryption keys and responds by erasing everything stored in the module.

6.1.25 FPT_RVM.1 Non-bypassability of the TSP

The Sentinel TOE complies with all ST requirements for Non-bypassability of the TSP. This function is implemented within the Security Module at every step of the I&A and Access Control processes. It begins with monitoring the insertion of a Smart Card and continues for each step required in the enabled profile as implemented by the instructions in the Secure Microcontroller. The Secure Microcontroller implements the instructions that define the TSP in

accordance with its stored firmware. This firmware is totally isolated from the host computer or workstation and is not accessible by either administrators or users. Its very nature of being programmed directly into the Secure Microcontroller memory as firmware makes it incapable of being changed or modified through user or administrator inputs as the program implementing the TSP is being run. The program is also designed so that the implementation of the TSP is serial in that there are no functions that can be performed in parallel that could allow another function to be bypassed. Therefore, there is no way that any TSP controlled function implemented by the Secure Microcontroller could be bypassed by a user, administrator, or anyone else in an operational environment. Even in an off-line environment the Secure Microcontroller implements protective mechanisms such as the use of dummy instructions, memory encryption, and tamper proofing that make the program virtually invulnerable to unauthorized modification.

In addition to the protection of the TSP, the design of the program that implements the TSP and the design of the Asset Status Sensor and Controller Board provide a built-in verification of the security functions for allowing access to restricted domains. This verification is provided by the validation of the sensitivity levels of the controlled objects selected by an authorized user acting as a subject. The selection of a controlled object is not automatically implemented by the Security Module based on the determination that an authorized user has the clearance and access rights sufficient to enable the selected domain. Instead, the Security Module under the control of the TSP validates the label and ID attached to the controlled RHDD object within a domain to ensure that the domain being implemented is in actuality the correct domain. If the label and ID are not authenticated by the TSP the user is denied access to the restricted domain. This provides feedback information that prevents a user from gaining access to any controlled objects that should not be allowed under the TSP. A similar verification mechanism is provided during identification and authentication, which requires a user to be authenticated through both something they know (password and PIN) and something they have (valid Smart Card). This makes it very difficult for a potential user to bypass or defeat the I&A process.

6.1.26 FPT_SEP.1 Domain Separation

The Sentinel TOE complies with all ST requirements for Domain Separation. This function is implemented within the Security Module by isolating the Security Module, including its Secure Microcontroller and all its security functions as defined in the TSP, from the host

computer or workstation hardware and software based data processing interfaces. In essence the Security Module and its TSFs operate within a hardware-based domain that is totally isolated from the processing domains that it enables and controls. This allows it to be totally isolated from the subject and the objects within the processing domains. In addition, the TSP and all TSFs are implemented in the firmware that is stored and run in the Secure Microcontroller. This firmware is totally protected by security mechanisms that are built-in to the Secure Microcontroller. This includes: the use of encryption to protect the firmware and all other stored data; the use of dummy instructions to prevent the firmware program from being monitored as it is run; and, the physical and electrical tamper proofing of the Secure Microcontroller module.

The Security Module also isolates all domains by only allowing one domain to exist at any given time and disabling the Write Command to any embedded NVMs that are shared between domains. Write updates to NVMs can only be enabled by an authorized administrator in the unrestricted domain. This essentially isolates the subject and objects in one domain from the subject and objects in another domain. Isolation of the domains is ensured by the design of the Asset Status Sensor and Controller Board within the Security Module, which automatically and simultaneously disables one restricted domain when it enables another. It also outputs the required signals to deactivate the Write Command for any embedded NVMs that are shared between domains while these domains are accessed by authorized users. These NVMs can only be write enabled by the Asset Status Sensor and Controller Board in an unrestricted domain in response to the action of an authorized administrator. The design of the Asset Status Sensor and Controller Board links the hardware based objects assigned to a domain at a given sensitivity level to a common parallel power grid via a series of Normally Closed Relays. If no valid Smart Card is detected by the Security Module after powering up the host, none of the relays is activated and the unrestricted domain is the only domain that will be enabled since it is connected to the normally closed power lead.

Access to either restricted domain will require the relay connecting power to the unrestricted domain to be activated so that power is applied to the selected restricted domain. The restricted domains are connected to power via a common relay so that only one domain can be activated when the relay is in a closed or open position. Within each domain selected

components are activated based on the output from relays that are controlled by the Secure Microcontroller in accordance with the TSP. The TSP selects the domain to be activated including the controlled RHDD data object and the controlled data communications objects based on the rules that compare the security attributes of the subject as defined on their Smart Card and the attributes of the domain as defined in its label and ID.

6.1.27 FPT_STM.1 Reliable Time Stamps

The Sentinel TOE complies with all ST Reliable Time Stamp requirements. This function is implemented within the Security Module through the utilization of the Secure Microcontrollers real time clock. This clock is set when the Secure Microcontroller is initially enabled during programming and cannot be reset by users or the Security Administrator. The time stamp provided by the Secure Microcontroller Real Time Clock is setup in a month/day/year/hour/second format. It can also be setup to account for changes due to daylights saving time if necessary. The degree of accuracy of the Real Time Clock in the Secure Microcontroller is roughly equivalent to that used in a host computer or workstation since the same technology is used to control their time base.

6.1.28 FTA_LSA.1 Limit on Scope of Selectable Attributes

The Sentinel TOE complies with all ST Limit on Scope of Selectable Attributes requirements. This requirement is implemented by the capability of the Security Module to adjust the clearance level and access rights of an authorized user based on time of day information from the Secure Microcontroller’s Real Time Clock. The security attributes and access rights of an authorized user as stored on their Smart Card can be made time dependent by appropriately programming the Smart Card. If the Smart Card includes a time-dependent attribute, the Secure Microcontroller will implement this attribute based on the time the user completes their authentication and logon process. The time of logon will then be used to determine the user’s clearance and access rights. It should be noted that security attributes granted after authentication will be good for the length of the session.

6.1.29 FTA_TSE.1 TOE Session Establishment

The Sentinel TOE complies with all ST TOE Session Establishment requirements. This requirement is met by the Security Module and the TSP which will deny a user the capability to establish a session in a restricted domain if the Secure Microcontroller:

1. Fails to accept the user's Smart Card as valid; or
2. Fails to accept the user PIN as valid; or
3. Fails to accept the user password as valid; or
4. Fails to match the user clearance to the sensitivity level of the domain.

6.2 Assurance Measures

This section will relate to each assurance requirement by providing references to supporting documentation for the assurance requirements given in Chapter 5. The supporting documentation will describe the assurance measures used to satisfy the requirements as defined by the ST. The strength of function of these requirements is SOF-medium

6.2.1 ACM_CAP.3 Authorization Controls

The Sentinel Configuration Management (CM) Plan provided with the documentation package for the Sentinel will address the system used to track the development and manufacture of the Sentinel. Each Sentinel is provided with a serial number for each unit. The serial numbers consist of a group of 3 alphanumeric digits followed by a dash, a group of 6 numbers followed by a dash, and a group of 5 numbers. The first 3 digits represent the model or project acronym, and the version number of that generation of the Sentinel. The following group of 6 numbers represents the shipping date of the specific unit. The last group of numbers represents the sequence number of the unit. Decals with the serial number for the unit are located on the rear panel of the Security Module at the upper left hand corner (facing).

Each Sentinel is provided with a materials list generated from an Agile automated configuration management database. The materials list provides the configuration items used to assemble the unit as well as a list of the documentation provided with the unit.

6.2.2 ACM_SCP.1 TOE CM Coverage

The CM Plan provided with the Sentinel supporting documentation addresses the CM system used during the development of the Sentinel. This plan addresses the expansion of the system to cover the manufacture of the Sentinel. The CM Plan addresses the procedures for tracking the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation. The CM plan describes how the configuration items are tracked by the CM system used in the development of the Sentinel.

6.2.3 ADO_DEL.1 Delivery Procedures

The delivery procedures for the Sentinel are provided in the documentation package and are titled “Sentinel Delivery Procedures”.

6.2.4 ADO_IGS.1 Installation, Generation, and Start-up Procedures

Installation, generation, and start-up procedures are provided in the documentation package and are titled “Sentinel Installation and Start-up”.

6.2.5 ADV_FSP.1 Informal Functional Specification

An informal function specification is provided in the documentation package and is titled “Sentinel Informal Functional Specification”. The functional specification describes the TSF and its external interfaces, and the purpose and method of use of all external TSF interfaces.

6.2.6 ADV_HLD.2 Security Enforcing High-Level Design

An informal presentation of the security enforcing high-level design of the Sentinel is provided in the documentation package and is titled “Sentinel High Level Design”. This presentation describes the structure of the TSF in terms of subsystems and the security functionality provided by each subsystem. All hardware and its functions are identified. The interfaces to the subsystems are described including those that are externally visible. The purposes and method of use of all interfaces to the TSF is included in the high level design.

6.2.7 ADV_RCR.1 Informal Correspondence Demonstration

An informal presentation of the analysis of correspondence of the Sentinel is provided in the documentation package and is titled “Sentinel Analysis of Correspondence”. The first analysis shows the relationships between the Sentinel Security System, the functional specification and the high-level design. The second analysis shows the relationships between the functional specification and the TOE summary of this ST. The third analysis shows the relationships between the high-level design and the low-level design. The fourth analysis shows the relationships between the low-level design and a subset of the TOE implementation representation.

6.2.8 AGD_ADM.1 Administrator Guidance

A separate manual is provided in the documentation package that is titled “Trusted Facility Manual for the Sentinel”. This manual provides the guidance for the system administrative personnel of the Sentinel. A manual is also provided titled “Administrator’s Guide to AuditX” providing administrator personnel guidance on the use of the AuditX utility.

6.2.9 AGD_USR.1 User Guidance

A separate manual is provided in the documentation package that is titled “Security Features User’s Guide for the Sentinel”. This manual provides the guidance for the users of the Sentinel, giving information defining user responsibilities and defining the restricted, and unrestricted user operations.

6.2.10 ALC_DVS.1 Identification of Security Measures

A separate document is provided in the documentation package that is titled “Sentinel Development Security Measures”. This document describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

6.2.11 ATE_COV.2 Analysis of Coverage

A separate document is provided in the documentation package that is titled “Sentinel Analysis of Test Coverage”. This document provides a matrix indicating the security functions of the Sentinel and the title of the test that addresses the security function.

6.2.12 ATE_DPT.1 Testing: High-Level Design

A separate document is provided in the documentation package that is titled “Sentinel Analysis of Depth of Testing”. This document provides a matrix indicating the subsystems and hardware of the Sentinel and the title of the test that tests the subsystem and its hardware.

6.2.13 ATE_FUN.1 Functional Testing

A separate section is provided in the documentation package that is titled “Sentinel Test Plan”. The test plan contains the plan, test procedures, and test results for the testing of the Sentinel.

6.2.14 ATE_IND.2 Independent Testing – Sample

Delta Security Technologies will provide a Sentinel Security System installed in a PC suitable for testing to an independent laboratory.

6.2.15 AVA_MSU.1 Examination of Guidance

Besides the Sentinel Security Features User’s Guide and the Trusted Facility Manual, an AuditX Manual is provided. Other documentation is listed in the documentation list provided with the Sentinel.

6.2.16 AVA_SOF.1 Strength of TOE Security Function Evaluation

Strength of function evaluation is provided for the password mechanism of the Sentinel as part of the documentation package. The document is titled “Sentinel Strength of Function Analysis”.

6.2.17 AVA_VLA.1 Developer Vulnerability Analysis

A vulnerability analysis is provided as part of the documentation package for the Sentinel. The document is titled “Sentinel Vulnerability Analysis”.

6.2.18 ACM_AUT.1 Partial Configuration Management Automation

This requirement drives a partial automation of the Configuration Management (CM) system that addresses automated access control measures, automated generation support procedures, identification and maintenance of TOE configuration items, version control of the TOE, automated authorized change control, and tracking of the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws. The requirements of this assurance element are described in the CM Plan and the automated system supporting documentation.

6.2.19 ACM_CAP.4 Generation Support and Acceptance Procedures

This assurance requirement adds the additional stipulations of acceptance procedures for modified or newly created configuration items of the TOE and output from the implemented CM system that provides evidence of the system use and controls to the ACM_CAP.3 requirements. The document titled “Acceptance Plan” and printouts from the CM system will address the additional evidence and procedures driven by this requirement.

6.2.20 ACM_SCP.2 Problem Tracking CM Coverage

This assurance element requires the addition of security flaw tracking to the CM system and documentation requirements. Security flaw tracking will be addressed in the CM Plan and the CM system documentation.

6.2.21 ADO_DEL.2 Detection of Modification

This requirement adds the additional components of providing for detection of modifications and prevention of masquerading attempts to the delivery procedures required by

ADO_DEL.1. These additional components will be addressed in the document titled “Sentinel Delivery Procedures”.

6.2.22 ADV_FSP.2 Fully Defined External Interfaces

This requirement adds the additional element of a rationale showing that the TSF is completely represented in the Informal Functional Specification. This component will be presented in the document titled “Sentinel Informal Functional Specification”.

6.2.23 ADV_IMP.1 Subset of the Implementation of the TSF

This requirement levies the provision of an implementation representation for a selected subset of the TSF. This requirement will be addressed by drawings, schematics, and annotated source code presented in a package titled “Sentinel Subset of Implementation Representation”. The document titled “Sentinel Analysis of Correspondence Low-Level Design to Subset of Implementation Representation” will present the TSF coverage demonstration for the provided package.

6.2.24 ADV_LLD.1 Descriptive Low-Level Design

This requirement introduces the component of the low-level design description of the TOE. This requirement is addressed in the document titled “Sentinel Low-Level Design”.

6.2.25 ADV_SPM.1 Informal TOE Security Policy Model

This assurance requirement introduces the component of an informal security policy model describing the security policies enforced by the TOE. This component is addressed in the document titled “Sentinel Informal Security Policy Model”. A demonstration of correspondence is presented in the document titled “Sentinel Demonstration of Correspondence Functional Description to Security Policy Model”.

6.2.26 ALC_LCD.1 Developer Defined Life-Cycle Model

This requirement adds the element of a life cycle model that describes and controls the development and maintenance of the TOE. This requirement is addressed in the document titled “Sentinel Life Cycle Model”.

6.2.27 ALC_TAT.1 Well-Defined Development Tools

This assurance component requires the developer to identify the tools used to develop the TOE and describe the TOE dependencies on these tools. This requirement is addressed in the document titled “Sentinel Development Tools”.

6.2.28 AVA_MSU.2 Validation of Analysis

This assurance requirement requires the developer to document an analysis of the TOE guidance documentation. This requirement is addressed in the document titled “Sentinel Validation of Misuse Analysis”.

6.2.29 AVA_VLA.2 Independent Vulnerability Analysis

This requirement adds the additional elements of justification to the vulnerability analysis and performance of an independent vulnerability analysis. This component is addressed by the document titled “Sentinel Vulnerability Analysis” and documentation from an independent facility demonstrating the results of penetration testing for the TOE.

6.3 Summary Specification Rationale

It is clear from the TOE summary specification that all of the IT Security Functional Requirements are addressed by the TOE. Since all of the functional requirements were defined against CC components the implementation of each of these components as described in the summary specification provides a direct correspondence.