Cybex SwitchView SC Series Switches Security Target

Document Version 3.0

Prepared for:

Avocent Corporation
4991 Corporate Drive
Huntsville, Alabama, 35805-6201

Prepared by:

Computer Sciences Corporation
7231 Parkway Drive
Hanover, MD 21076

Table of Contents

List of Tables

List of Figures

1 INTRODUCTION

This Chapter presents security target (ST) identification information and an overview of the ST. An ST document provides the basis for the evaluation of an information technology (IT) product or system (e.g., Target of Evaluation). An ST principally defines:

- A security problem expressed as a set of assumptions about the security aspects of the environment; a list of threats which the product is intended to counter; and any known rules with which the product must comply (in Chapter 3, Security Problem Definition).
- A set of security objectives and a set of security requirements to address that problem (in Chapters 4 and 5, Security Objectives and IT Security Requirements, respectively).
- The IT security functions provided by the Target of Evaluation (TOE) that meet the set of requirements (in Chapter 6, TOE Summary Specification).

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 6.

1.1 ST and TOE Identification

This section provides information needed to identify and control this ST and its Target of Evaluation (TOE), the TOE Name. This ST targets an Evaluation Assurance Level (EAL) 4 (augmented with ALC_FLR.2) level of assurance.

ST Title	Cybex SwitchView SC Series Switches Security Target
ST Version	Version 3.0
Revision Number	Revision 1.5
Publication Date	March 2, 2009
Authors	Computer Sciences Corporation, Common Criteria Testing Lab Avocent Corporation
TOE Identification	Cybex SwitchView SC420 Model 520-753-502 Cybex SwitchView SC440 Model 520-721-502 Cybex SwitchView SC540 Model 520-728-502
CC Identification	Common Criteria for Information Technology Security Evaluation, Version 3.1R2, September 2007
ST Evaluation	Computer Sciences Corporation
Keywords	Device sharing, multi-way switch, peripheral switching, keyboard-video-monitor/mouse (KVM) switch

1.2 TOE Overview

The TOE is a device, hereinafter referred to as a Peripheral Sharing Switch (PSS), or simply switch, that permits a single set of human interface devices, USB keyboard, DVI-I video, audio (input and output), USB mouse, and Common Access Card (CAC) or SmartCard reader, to be shared among two or more

computers. Users who access secure and unsecure networks from one set of peripherals can rely on the SwitchView SC series of switches' unique architecture to keep their private data completely separate and secure at all times. There is no software to install or boards to configure.

The SwitchView SC series of switches work with IBM PC/AT and Sun systems and have ports for USB keyboard, USB mouse, DVI-I video, audio (input and output), and USB Common Access Card (CAC) or SmartCard reader. Each switch has a "select" button associated with each specific port.

A summary of the SwitchView SC series switches security features can be found in Section 1.4, TOE Description. A detailed description of the SwitchView SC series switches security features can be found in Section 6, TOE Summary Specification.

1.3 References

The following documentation was used to prepare this ST:

[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2006, Version 3.1, CCMB-2006-09-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated September 2007, Version 3.1, CCMB-2007-09-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated September 2007, Version 3.1, CCMB-2007-09-003
[CEM]	Common Evaluation Methodology for Information Technology Security Evaluation, dated September 2007, Version 3.1, CCMB-2007-09-004
[PSS_PP]	*Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008

1.4 TOE Description

This Chapter provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

1.4.1 Product Type

The TOE is a device, hereinafter referred to as a Peripheral Sharing Switch (PSS), or simply switch, that permits a single set of human interface devices: USB keyboard, DVI-I video, USB mouse, audio (input and output), and Common Access Card (CAC) or SmartCard reader, to be shared among two or more computers. Users who access secure and unsecure networks from one set of peripherals can rely on the SwitchView SC series of switches' unique architecture to keep their private data completely separate and secure at all times. There is no software to install or boards to configure.

The SwitchView SC series of switches work with IBM PC/AT and Sun systems and have ports for USB keyboard, USB mouse, DVI-I video, audio (input and output), and USB Common Access Card (CAC) or SmartCard reader. Each switch has a "select" button associated with each specific port.

1.4.2 Physical Scope and Boundary

The TOE is a peripheral sharing switch. The physical boundary of the TOE consists of one SwitchView switch (see Table 1: TOE Models and Features), and its accompanying User and Administrator Guidance. Updated User and Administrator Guidance can be downloaded from the http://www.avocent.com website at any time.

Table 1: TOE Models and Features

Model	TOE Identification Part Numbers	Ports	Interfaces
SwitchView SC420	520-753-502	2	Dual-link DVI-I, USB keyboard, USB mouse, CAC/SmartCard, Audio input and output
SwitchView SC440	520-721-502	4	Dual-link DVI-I, USB keyboard, USB mouse, CAC/SmartCard, Audio input and output
SwitchView SC540	520-728-502	4	Dual-head, Dual-link DVI-I, USB keyboard, USB mouse, CAC/SmartCard, Audio input and output

The evaluated TOE configuration does not include any peripherals or computer components, to include cables or their associated connectors, attached to the TOE. The following figure depicts the TOE and its environment.

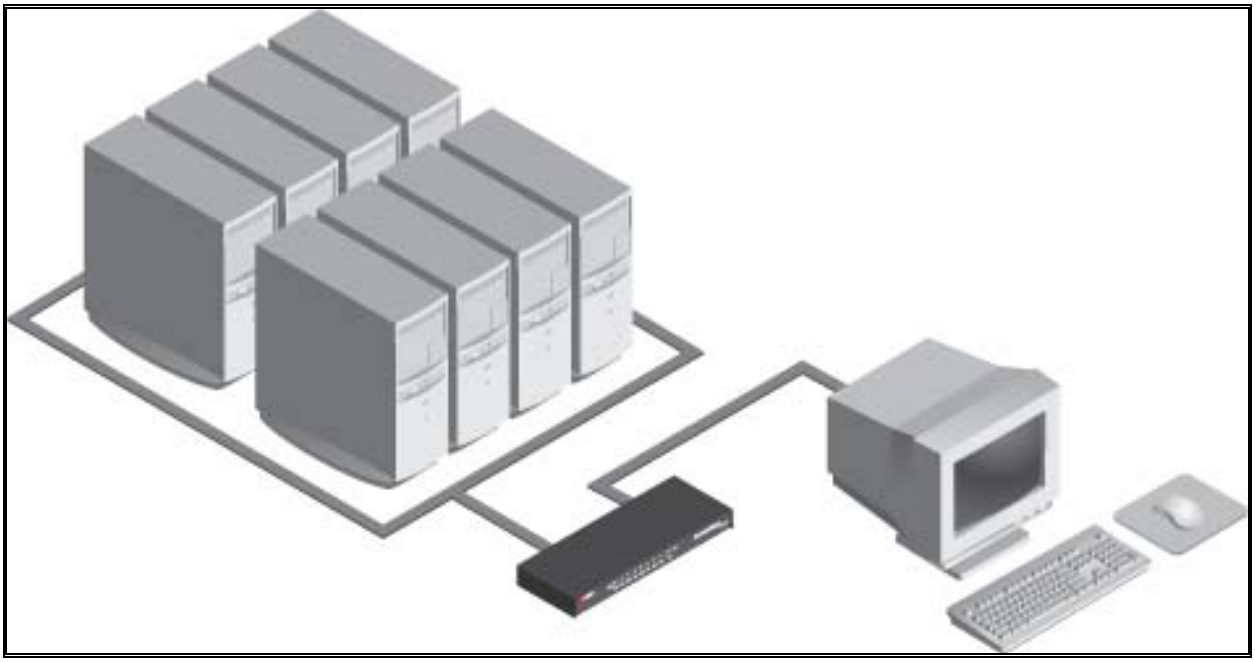

Figure 1: Depiction of TOE Deployment

1.4.3 Logical Scope and Boundary

The TOE logical scope and boundary consists of the security functions/features provided/controlled by the TOE.

The TOE provides the following security features:

- Data Separation (TSF_DSP), and
- Security Management (TSF_MGT)
- Tamper Detection (TSF_TMP)

The TOE implements the Data Separation Security Function Policy (SFP) as outlined in Section 2 of *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008. In operation, the TOE is not concerned with the user information flowing between the shared peripherals and the switched computers. It only provides a single logical connection between the shared peripheral group and the one selected computer (TSF_DSP). Data Separation is accomplished as explained in section 8.1.1.

The TOE allows for the connected computers to be powered-up all-at-once or one at a time. The green LEDs over each channel will light, indicating that the attached computer is powered on. To select or switch computers, the TOE provides *select* switches, that allow the human user to explicitly determine to which computer the shared set of peripherals is connected (TSF_MGT). This connection is visually displayed by an amber LED over the selected channel. Security Management is accomplished as explained in section 8.1.2.

Any attempt to open the TOE by removing the security screw will activate a tamper-detection "suicide" switch. If one of these models has been physically tampered with in this manner, the lights on the front of the TOE will all flash in unison to alert an administrator to the interference, and all TOE functions will be permanently disabled. Tamper Detection is accomplished as explained in section 8.1.3.

1.4.4 TOE Features Outside of Evaluation Scope

There are no features of the TOE that are outside of the scope of evaluation.

2 CONFORMANCE CLAIMS

This section describes the conformance claims of this Security Target.

2.1 Common Criteria Conformance Claims

The Security Target is based upon

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 1, CCMB-2006-09-001,
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 2, CCMB-2007-09-002,
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 2, CCMB-2007-09-003

referenced hereafter as [CC].

This Security Target claims the following CC conformance:

- Part 2 conformant
- Part 3 conformant
- Evaluation Assurance Level (EAL) 4+

2.2 Protection Profile (PP) Claims

This ST claims demonstrable compliance for the following PP:

> *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008

2.3 Package Claims

This Security Target claims conformance to the EAL 4 package augmented with ALC_FLR.2.

3 SECURITY PROBLEM DEFINITION

The Security Problem Definition describes assumptions about the operational environment in which the TOE is intended to be used and represents the conditions for the secure operation of the TOE.

3.1 Definitions

In the Common Criteria, many terms are defined in Section 4 of Part 1. The following terms are a subset of those definitions. They are listed here to aid the user of the Security Target.

Authentication data	Information used to verify the claimed identity of a user.
Authorized User	A user who may, in accordance with the SFRs, perform an operation.
External entity	Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.
Identity	A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Object	A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Subject	An active entity in the TOE that performs operations on objects.
User	See **external entity**.

In addition to the above general definitions, terminology that is specific to this ST is given in “Terms of Reference,” Pages 47 - 49, of *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008.

3.2 TOE Security Environment

The assumptions and threat identification combined with any organization security policy statement or rules requiring TOE compliance provides the definition of the security environment. It is necessary that a comprehensive security policy be established for the site in which the product is operated and that it is enforced and adhered to by all users of the product. The security policy is expected to include measures for:

- ***Physical security*** - to restrict physical access to areas containing the product, computer system and associated equipment and protect physical resources, including media and hardcopy material, from unauthorized access, theft or deliberate damage.
- ***Procedural security*** - to control the use of the computer system, associated equipment, the product and information stored and processed by the product and the computer system, including use of the product's security features and physical handling of information.

- ***Personnel security*** - to limit a user's access to the product and to the computer system to those resources and information for which the user has a need-to-know and, as far as possible, to distribute security related responsibilities among different users.

3.2.1 Assumptions

The specific conditions listed in "Secure Usage Assumptions," Section 3.1, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008, are assumed to exist for the TOE.

3.2.2 Threats

Threats may be addressed either by the TOE or by its intended environment (for example, using personnel, physical, or administrative safeguards). These two classes of threats are discussed separately.

3.2.2.1 Threats Addressed by the TOE

"Threats to Security," Section 3.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008, identifies threats to the assets against which specific protection within the TOE is required.

3.2.2.2 Threats Addressed by the Operating Environment

Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 1.2, dated August 21, 2008, identifies no threats to the assets against which specific protection within the TOE environment is required.

3.2.3 Organizational Security Policies

Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 1.2, dated August 21, 2008, identifies no organization security policies (OSPs) to which the TOE must comply.

4 SECURITY OBJECTIVES

The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE, and
- Security objectives for the Operating Environment.

4.1 Security Objectives for the TOE

"Security Objectives for the Target of Evaluation," Section 4.1, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008, identifies the security objectives to address security concerns that are directly addressed by the TOE.

4.2 Security Objectives for the IT Environment

"Security Objectives for the Environment," Section 4.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008, identifies security objectives to address security concerns that are directly addressed by the TOE environment.

5 EXTENDED COMPONENTS DEFINITION

The Extended Components Definition describes components for security objectives which cannot be translated or could only be translated with great difficulty to existing requirements.

NOTE: The *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008 contains extended components but does not include an Extended Components Definition. In order to comply with the Common Criteria, this ST provides the required definition.

5.1 Class EXT: Extended – Inspection

Visual confirmation provides the user with important information regarding the connection made through the TOE. This allows the user to confirm that their data is being securely transported to the proper computer.

5.1.1 Visual Inspection (EXT_VIR)

Family Behaviour

This family defines requirements for providing a means of determining which computer is connected to which set of peripheral devices.

Component leveling

EXT_VIR.1 Visual Indication Rule, provides a visual indication of the connections between the computer and a set of peripheral devices.

Management: EXT_VIR.1

There are no management activities foreseen.

Audit: EXT_VIR.1

There are no auditable events foreseen.

EXT_VIR.1	**Visual Indication Rule**	
	Hierarchical to:	No other components
	Dependencies:	None
EXT_VIR.1.1	A visual method of indicating which COMPUTER is CONNECTED to the shared set of PERIPHERAL DEVICES shall be provided.	

Application Note: Does not require tactile indicators, but does not preclude their presence. The indication shall persist for the duration of the CONNECTION.

5.2 Class EXP: Extended – Tampering

Tamper-proofing of the TOE protects all peripheral devices connected to that TOE. This prevents any alterations of the chips and circuits within the TOE. This in turn, prevents improper or corrupt data from being transferred to the peripheral devices connected to it.

5.2.1 Physical Tampering Security (EXP_TMP)

Family Behaviour

This family defines the response taken if the enclosure cover screws are removed.

Component leveling

EXP_TMP Prevention of Physical Tampering, the TSF shall disable all functions if the enclosure screws are removed.

Management: EXP_TMP.1

a) There are no management activities foreseen.

Audit: EXP_TMP.1

a) There are no auditable events foreseen.

EXP_TMP.1	**Prevention of Physical Tampering**	
	Hierarchical to:	No other components
	Dependencies:	None
EXP_TMP.1.1	The TSF shall permanently disable all TOE functions in the event of attempts to gain access to TOE internal circuitry through opening the enclosure via removing the enclosure cover screws.	

6 IT SECURITY REQUIREMENTS

This section defines the IT security requirements that shall be satisfied by the TOE or its environment:

The CC divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.

- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g., configuration management, testing, and vulnerability assessment).

These requirements are discussed separately within the following subsections.

6.1 Conventions

This section describes the conventions used to denote CC operations on security requirements and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows several operations to be performed on security functional components; *assignment, refinement, selection,* and *iteration* as defined in Section C.4 of Part 1 of the CC:

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value in square brackets [assignment_value(s)].

- Iteration of a component is used when a component is repeated more than once with varying operations. Iterated components are given unique identifiers by an iteration number or name in parenthesis appended to the component and element identifiers.

- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *underlined italicized text.*

Plain *italicized text* is used for both official document titles and text meant to be emphasized more than plain text.

6.2 TOE Security Functional Requirements

The TOE satisfies the SFRs delineated in "Target of Evaluation Security Requirements," Section 5.1, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008. The SFR's have been reproduced here merely for the convenience of the customer.

6.2.1 Class FDP: User Data Protection

6.2.1.1 FDP_ETC.1 Export of User Data Without Security Attributes

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 subset information flow control
FDP_ETC.1.1	The TSF shall enforce the [Data Separation SFP] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.1.2	The TSF shall export the user data without the user data's associated security attributes.

6.2.1.2 FDP_IFC.1 Subset Information Flow Control

Hierarchical to:	No other components.
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.1.1	The TSF shall enforce the [Data Separation SFP] on [the set of PERIPHERAL PORT GROUPS and the bi-directional flow of PERIPHERAL DATA and STATE INFORMATION between the SHARED PERIPHERALS and the SWITCHED COMPUTERS].

6.2.1.3 FDP_IFF.1 Simple Security Attributes

Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1	The TSF shall enforce the [Data Separation SFP] based on the following types of subject and information security attributes: [PERIPHERAL PORT GROUPS (SUBJECTS), PERIPHERAL DATA and STATE INFORMATION (OBJECTS), and PERIPHERAL PORT GROUP IDs (ATTRIBUTES)].
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [Switching Rule: PERIPHERAL DATA can flow to a PERIPHERAL PORT GROUP with a given ID only if it was received from a PERIPHERAL PORT GROUP with the same ID].
FDP_IFF.1.3	The TSF shall enforce the [No additional information flow control SFP rules].
FDP_IFF.1.4	The TSF shall explicitly authorise an information flow based on the following rules: [No additional rules].

FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [No additional rules].

6.2.1.4 FDP_ITC.1 Import of User Data Without Security Attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation
FDP_ITC.1.1	The TSF shall enforce the [Data Separation SFP] when importing user data, controlled under the SFP, from outside the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [No additional rules].

6.2.2 Class FMT: Security Management

6.2.2.1 FMT_MSA.1 Management of Security Attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles
FMT_MSA.1 .1	The TSF shall enforce the [Data Separation SFP] to restrict the ability to *modify* the security attributes [PERIPHERAL PORT GROUP IDS] to [the USER].

Application Note: An AUTHORIZED USER shall perform an explicit action to select the COMPUTER to which the shared set of PERIPHERAL devices is CONNECTED.

6.2.2.2 FMT_MSA.3 Static Attribute Initialisation

Hierarchical to:	No other components.
Dependencies:	FDP_MSA.1 Management of Security Attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the [Data Separation SFP] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

Application Note: On start-up, one and only one attached COMPUTER shall be selected.

FMT_MSA.3.2	The TSF shall allow the [none] to specify alternative initial values to override the default values when an object or information is created.

6.2.2.3 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	None
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [none].

6.3 TOE Security Assurance Requirements

The security assurance components (EAL4 augmented with ALC_FLR.2) are specified in "Target of Evaluation Security Assurance Requirements," Section 5.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008.

6.4 Security Requirements for the IT Environment

There are no security functional requirements for the IT Environment.

6.5 Explicitly Stated Requirements for the TOE

This ST contains the explicitly stated requirement for the TOE as specified in "EXT_VIR.1 (Visual Indication Rule)," Section 5.1.3, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008. It has been reproduced here:

EXT_VIR.1 Visual Indication Rule

Hierarchical to:	No other components
Dependencies:	None
EXT_VIR.1.1	A visual method of indicating which COMPUTER is CONNECTED to the shared set of PERIPHERAL DEVICES shall be provided.
Application Note:	Does not require tactile indicators, but does not preclude their presence. The indication shall persist for the duration of the CONNECTION.

This ST does contain an additional explicitly stated requirement for the TOE as specified below:

EXP_TMP.1 Prevention of Physical Tampering

Hierarchical to:	No other components
Dependencies:	None
EXP_TMP.1.1	The TSF shall permanently disable all TOE functions in the event of attempts to gain access to TOE internal circuitry through opening the enclosure via removing the enclosure cover screws.

7 RATIONALE

This section demonstrates the completeness and consistency of this ST by providing justification for the following:

Traceability	The security objectives for the TOE and its environment are explained in terms of threats countered and assumptions met. The SFRs are explained in terms of objectives met by the requirement. The traceability is illustrated through matrices that map the following: • security objectives to threats encountered • environmental objectives to assumptions met • SFRs to objectives met
Assurance Level	A justification is provided for selecting an EAL 4 level of assurance for this ST.
SOF	A rationale is provided for the SOF level chosen for this ST.
Dependencies	A mapping is provided as evidence that all dependencies are met.

7.1 Rationale for Security Objectives

This section demonstrates that all security objectives for the TOE are traced back to aspects of the identified threats to be countered and/or aspects of the organizational security policies to be met by the TOE.

This ST claims conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008, without additional objectives. Consequently the security objectives rationale is provided in Section 6.1, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008, and are claimed to be adequate for this ST.

NOTE: The security objectives rationale in the Protection Profile is incomplete; while mapping T.INSTALL to OE.MANAGE, the Protection Profile does not provide a rationale for the mapping. This ST provides this rationale below:

T.INSTALL The TOE may be delivered and installed in a manner, which violates the security policy.	OE.MANAGE The TOE shall be installed and managed in accordance with the manufacturer's directions.	OE.MANAGE Installing and delivering the TOE in accordance with the manufacturer's instructions mitigates they risk of violation of the security policy during delivery and installation.

7.2 Environmental Objectives Rationale

This section demonstrates that all objectives for the environment are traced back to aspects of the identified threats to be countered and/or aspects of the organizational security policies to be met by the environment.

This ST claims conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008, without additional environmental objectives. Consequently the environmental objectives rationale is provided in Section 6.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008, and are claimed to be adequate for this ST.

7.3 Security Requirements Rationale

This section provides evidence that demonstrates that the security objectives for the TOE and the IT environment are satisfied by the security requirements.

This ST claims conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008, without any operations performed on the IT security requirements specified in the cited PP. Consequently the security requirements rationale is provided in Section 6.3, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008, and are claimed to be adequate for this ST for those requirements taken from the PP.

Rationale for the additional explicitly stated requirement (EXP_TMP.1) is as follows:

O.NOPROG Logic contained within the TOE shall be protected against unauthorized modification. Embedded logic must not be stored in programmable or re-programmable components.	EXP_TMP.1 (Prevention of Physical Tampering)	EXP_TMP.1: The TSF needs to ensure that it protects itself against physical changes which might compromise its security functionality. Part 2 of the Common Criteria does not provide a component appropriate to express the requirement for physical tamper prevention.
O.ROM TOE software/firmware shall be protected against unauthorized modification. Embedded software must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.	EXP_TMP.1 (Prevention of Physical Tampering)	EXP_TMP.1: The TSF needs to ensure that it protects itself against physical changes which might compromise its security functionality. Part 2 of the Common Criteria does not provide a component appropriate to express the requirement for physical tamper prevention.

NOTE: The security requirements rationale in the Protection Profile is incomplete; the Protection Profile does not provide a mapping or rationale for the new requirement FMT_SMF.1. The requirement FMT_SMF.1, as written in the PP provides for no management functions to be performed. With no management functions to be performed and no management objective to contribute to, this requirement has nothing to be mapped to in the rationale of either the Protection Profile or this ST and is included only because it is required by the Protection Profile.

7.4 Rationale for SFR and SAR Dependencies

This ST claims conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008. The rationale with respect to SFR and SAR dependencies from the PP is given in Sections 6.4 of the referenced PP.

The explicitly stated requirement EXP_TMP.1 does not contain any dependencies.

7.5 Mapping Tables

This ST claims conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008. The mapping tables for threats, objectives and dependencies are found in Section 6.5 of the Protection Profile. The following additional mappings are required for the requirement EXP_TMP.1 which is extended and appears only in the ST.

	O.CONF	O.CONNECT	O.INDICATE	O.INVOKE	O.NOPROG	O.ROM	O.SELECT	O.SWITCH
EXP_TMP.1					X	X		

Table 2: Mapping of Security Functional Requirements to Objectives

Dependency	**FDP_IFC.1**	**FDP_IFF.1**	**O.INDICATE**		**FMT_MSA.1**	**FMT_MSA.3**	**FMT_SMF.1**	
EXP_TMP.1								

Table 3: Mapping of Security Functional Requirements Dependencies

8 TOE SUMMARY SPECIFICATION

This section presents an overview of the security functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

8.1 TOE Security Functions

This section presents the security functions performed by the TOE to satisfy the identified SFRs in Section 5.1. Traceability to SFRs is also provided.

8.1.1 Data Separation (TSF_DSP)

The TOE implements the Data Separation Security Function Policy (SFP) as outlined in Section 2 of *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008.

Signals processed by the TOE are keyboard data, mouse data, keyboard LED data, Data Display Channel information, analog video signals, Common Access Card (CAC) or SmartCard reader data, audio data and USB status. Specific versions of the TOE accommodate subsets of the listed signals to support popular types of computers. In all cases, the TOE ensures data separation for all signal paths using both hardware and firmware.

The basic arrangement of the microprocessors used for shared peripheral data ensures data separation in hardware by physical separation of the microprocessors connected to the user's peripheral devices from the microprocessors connected to the attached computers. In operation, the main processor moves data received from the shared peripherals to the microprocessor corresponding to the selected computer. The processor dedicated to the selected computer sends data to the computer. Separation is ensured in hardware by use of separate microprocessors for each of the computers and for the shared user peripheral devices.

Separation in firmware is ensured by firmware design consisting dedicated functions and static memory assignment with no third-party library functions or multitasking executives.

In operation the TOE is not concerned with the content of user information flowing between the shared peripherals and the switched computers. It only provides a single logical connection between the shared peripheral group and the one selected computer supporting the Data Separation Security Functional Policy – "the TOE shall allow peripheral data and state information to be transferred only between peripheral port groups with the same ID." The TOE interfaces ensure that confidentiality of information is not violated by isolating signals electrically and through firmware modules that ensure that information is passed only between the user peripherals and the selected computer.

Keyboard LED status for each computer is stored by the processor associated with each computer. The TOE does not have software to install, or boards to configure. The logic contained within the TOE is protected from unauthorized modification through the use of discrete components.

FUNCTIONAL REQUIREMENTS SATISFIED: FDP_ETC.1, FDP_IFC.1, FDP_IFF.1, FDP_ITC.1

8.1.2 Security Management (TSF_MGT)

The TOE allows for the connected computers to be powered-up all-at-once or one at a time. The green LEDs over each channel will light, indicating that the attached computer is powered on. To select or switch computers, the TOE provides port-specific switches, that allow(s) the human user to explicitly determine to which computer the shared set of peripherals is connected. This connection is visually displayed by an amber LED over the selected channel.

FUNCTIONAL REQUIREMENTS SATISFIED: FMT_MSA.1, FMT_MSA.3, EXT_VIR.1

8.1.3 Tamper Detection (TSF_TMP)

A switch inside the unit is activated when a screw used to fasten the top cover of the unit is removed. The tamper switch is powered by the main power supply or a dedicated battery so that it can always detect intrusions. After the switch is activated, TOE operation is disabled and the amber indicators on the front panel of the unit flash in unison. When the amber indicators are flashing in unison, operation of the TOE cannot be restored; the TOE must be replaced.

FUNCTIONAL REQUIREMENTS SATISFIED: EXP_TMP.1

9 ACRONYMS

9.1 Common Criteria Acronyms

The following abbreviations from the Common Criteria are used in this Security Target:

CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

9.2 ST Acronyms

The following abbreviations are used in this Security Target to help describe the TOE, and the IT environment.

CAC	Common Access Card
DVI-I	Digital Video Interface - Integrated
IBM	International Business Machines, Inc.
LED	Light Emitting Diode
PC/AT	Personal Computer / Advanced Technology
VGA	Video Graphics Array
USB	Universal Serial Bus

Acronyms specific to this ST, and the referenced PP are given in “Acronyms,” Page 49, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008.