Trust Technology Assessment Program

Validation Report

Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile Version 1.0

TTAP Report Number: TTAP-VR-0012

Version 1.0

August 2000

Prepared By:
Trust Technology Assessment Program (TTAP)
National Security Agency (V13)
9800 Savage Road, Suite 6740
Ft. George G. Meade, MD 20755-6740

Arrangement
on the
Recognition of Common Criteria Certificates
in the field of
Information Technology Security

The Trust Technology Assessment Program (TTAP) Oversight Board is a member of the above Arrangement. As such, it confirms that a Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and that the certificate has been issued in accordance with the terms of this Arrangement. The judgements contained in the evaluation and this Validation Report are those of the Oversight Board which issues it and of the evaluation facility which carried out the evaluation. There is no implication of acceptance by Members of the Arrangement of liability with respect to judgements or losses sustained as a result of reliance placed upon information contained herein.

Executive Summary

Production and evaluation of the Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 1.0, was sponsored by the National Security Agency.

This profile has been designed for use under Common Criteria Scheme party to the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (ARCC). The Protection Profile (PP) evaluation was completed in August 2000 by CygnaCom Solutions, Inc. (an accredited Trust Technology Assessment Program (TTAP) evaluation facility in the United States) and has been shown to be conformant with Part 3 of the Common Criteria for Information Technology security Evaluation, version 2.1 (CCv2.1) requirements for Protection Profiles. The Common Evaluation Methodology version 1.0 was used to conduct the PP evaluation to show conformance to CCv2.1 Part 3.

The PSS PP specifies U.S. Department of Defense minimum security requirements for peripheral switches; devices which enable a single set of human interface devices to be shared between two or more computers.

1.0 Introduction

This report states the outcome of the PP evaluation of the Peripheral Sharing Switch (PSS) for Human Interface Devices, version 1.0 dated 8 August 2000. The report is intended to characterize the nature of the PP and its evaluation to assist potential users when judging the suitability of the PP in the context of their specific requirements. Prospective users of the PP are advised to read this report in conjunction with the PSS PP which specifies the functional, environmental and assurance requirements for a PSS PP conformant switch.

1.1 Functional Requirements of the PSS PP

The purpose of the PSS PP is to specify the assurance and security functional requirements of a TOE that permits a single set of human interface devices to be shared between two or more computers. The PSS PP environment and security functional requirements are specified such that the TOE will only be connected to one computer at a time and does not allow for the sharing of information between computers that are attached to the TOE. The TOE requires an explicit action to be taken by the user to switch to another computer. When the TOE is in a switched state it gives a visual indication of what computer is connected to the interfacing devices.

The functional requirements for the TOE are drawn from Part 2 of the CC with one of the functional requirements being explicitly stated. The following two tables specifies the functional requirements present in the PSS PP:

TABLE 1. CC Functional Requirements in the PSS PP

CC Functional Class	CC Functional Component Identifier
User Data Protection	FDP_ETC.1 (Export of User Data Without Security Attributes) FDP_IFC.1 (Subset Information Flow Control) FDP_IFF.1 (Simple Security Attributes) FDP_ITC.1 (Import of User Data Without Security Attributes)
Security Management	FMT_MSA.1 (Management of Security Attributes) FMT_MSA.3 (Static Attribute Initialisation)
Protection of the TOE Security Functions	FPT_RVM.1 (Non-bypassability of the TSP) FPT_SEP.1 (TSF Domain Separation)

TABLE 2. Explicitly Stated Functional Requirement in the PSS PP

Explicit Component	Explicit Component Identifier
Extended Requirements	EXT_VIR.1 (Visual Indication Rule)

1.2 Assurance Requirements of the PSS PP

The PSS PP specifies EAL4 for the assurance level of the TOE. The assurance level specifies activities that are carried out by the developer and evaluators that are used to gain assurance that the TOE claiming compliance to the PSS PP has the security functionality specified in the PSS PP.

> EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.
>
> EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.[CC part 3, page 60]

The following table summarizes the EAL4 assurance requirements that appear in the PSS PP:

TABLE 3. Assurance Requirements in the PSS PP

Assurance Class	Assurance Component Identifier
Configuration Management	ACM_AUT.1 (Partial CM Automation) ACM_CAP.4 (Generation Support and Acceptance Procedures) ACM_SCP.2 (Problem Tracking CM Coverage)
Delivery and Operation	ADO_DEL.2 (Detection of Modification) ADO_IGS.1 (Installation, Generation, and Start-up Procedures)
Development	ADV_FSP.2 (Fully Defined External Interfaces) ADV_HLD.2 (Security Enforcing High-level Design) ADV_IMP.1 (Subset of the Implementation of the TSF) ADV_LLD.1 (Descriptive Low-level Design) ADV_RCR.1 (Informal Correspondence Demonstration) ADV_SPM.1 (Informal TOE Security Policy Model)
Guidance Documents	AGD_ADM.1 (Administrator Guidance) AGD_USR.1 (User Guidance)
Life Cycle Support	ALC_DVS.1 (Identification of Security Measures) ALC_LCD.1 (Developer Defined Life-Cycle Model) ALC_TAT.1 (Well-Defined Development Tools)

TABLE 3. Assurance Requirements in the PSS PP

Assurance Class	Assurance Component Identifier
Tests	ATE_COV.2 (Analysis of Coverage) ATE_DPT.1 (Testing: High-level Design) ATE_FUN.1 (Functional Testing) ATE_IND.2 (Independent Testing - Sample)
Vulnerability Assessment	AVA_MSU.2 (Validation of Analysis) AVA_SOF.1 (Strength of TOE Security Function Evaluation) AVA_VLA.2 (Independent Vulnerability Analysis)

2.0 Evaluation

The evaluation of the PSS was conducted using Chapter 3, “PP Evaluation”, of the CEM version 1.0 dated August 1999 and using the Class APE, “Protection Profile evaluation”, of Part 3 of the CC version 2.1 dated August 1999.

3.0 Results of the evaluation

The PSS PP evaluation was conducted by CygnaCom Solutions, Inc. It was completed and validated by the TTAP Oversight Board in August 2000. This section of the report summarizes the results of the evaluation of the PSS PP.

The following table summarizes the APE components the evaluator used to conduct the PP evaluation:

TABLE 4. CEM Evaluator Activities for the PSS PP

Evaluator Action	Content Identifier
Evaluation of the TOE Description	APE_DES.1
Evaluation of the Security Environment	APE_ENV.1
Evaluation of the PP Introduction	APE_INT.1
Evaluation of the Security Objectives	APE_OBJ.1
Evaluation of the IT Security Requirements	APE_REQ.1
Evaluation of Explicitly Stated Requirements	APE_SRE.1

At the conclusion of the PSS PP evaluation all APE CC and CEM evaluator activities were passed.

Several National Interpretations impacted the PSS PP evaluation. The interpretations that affected the evaluation are attached in Appendix A. Interpretations #0364 and #0385 interpret the CC in a manner that adds new content elements and evaluator actions.

The following table specifies the activities the evaluator undertook to confirm that any provided application notes meet all requirements for content and presentation of evidence.

TABLE 5. Activities Undertaken for Interpretation #0364

Interpretation Component Element	Evaluator Activities
APE_APP.1.1C	The evaluator examined the application notes to determine that they are informative only.
APE_APP.1.2C	The evaluator: • checked that there is a clear association between an application note and the element to which they apply, and • checked that the application note is consistent with the specific element of the PP to which the note applies.

The evaluators followed the activities in the following table to confirm that the two content elements presented for the identification of standards meet the content and presentation requirements specified in these two elements.

TABLE 6. Activities Undertaken for Interpretation #0385

Interpretation Component Element	Evaluator Activities
APE_REQ.1.xC[a]	The evaluator checked if the functional or assurance requirements were claiming compliance to an external standard. The evaluator: • checked to see if the external standard(s) are unambiguously specified and • examine the external standard(s) to determine if the meaning of compliance to the standard(s) is clear.
APE_REQ.1.xC[b]	The evaluator examined all external standards to determine that it is clear how compliance is ascertained.

a. This element is referring to the first content element that is specified in the National Interpretation under the “Criteria and/or Methodology Changes” section.

b. This element is referring to the second content element that is specified in the National Interpretation under the “Criteria and/or Methodology Changes” section.

At the conclusion of the PSS PP evaluation it was seen that all National Interpretations affecting the PSS PP evaluation are satisfied.

4.0 Conclusions and Recommendations

The PSS PP evaluation has met all the evaluator activities for a PP evaluation in both the CC Part 3 and the CEM Part 2. Further the PSS PP evaluation has satisfied all National and International Interpretations that had been finalized on the start date of the evaluation.

5.0 Appendix A - National Interpretations

This appendix of the validator's report includes the National Interpretations (#0354, #0364, and #0385) that were considered during the course of the PSS PP evaluation. The National Interpretations are also posted at:

http://www.radium.ncsc.mil/tpep/library/interps/interps.html

#0354: Association Of Information Flow Attributes W/Subjects And Information

```
NUMBER:             0354
STATUS:             Approved by TTAP/CCEVS Management
TYPE:               Interpretation

TITLE:              Association Of Information Flow Attributes W/Subjects And
                    Information

EFFECTIVE DATE:     2000-03-27

CCITSE FAMILY:      Information Flow Control Functions (FDP_IFF)
SCOPE:              Common Criteria CC_PART2_V2 (CCITSE V2.1 Functional
                    Requirements)
                    Common Criteria CC_PART2A_V2 (CCITSE V2.1 Functional
                    Requirements Annex)
DOCUMENT(S):        <None>
RELATED TO:
     #0353            Association Of Access Control Attributes With Subjects And
Objects
```

STATEMENT:

The following interprets the FDP_IFF.1 and FDP_IFF.2 components:

Information Flow Control Policies shall provide a clear association of controlled entities (subjects, information) with relevent security attributes.

CRITERIA AND/OR METHODOLOGY CHANGES:

To address this interpretation, the FDP_IFF.1.1 and FDP_IFF.2.1 elements should be reworded to the following (additions marked thusly; deletions marked thusly):

> FDP_IFF.x.1: The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: the minimum number and type of security attributes *list of subjects and information controlled under the indicated SFP, and for each, the SFP-relevant security attributes*]

In the Part 2 Annex (Section F.6), the second paragraph for the assignment operation for both FDP_IFF.1.1 and FDP_IFF.2.1 should be replaced with:

> In FDP_IFF.x.1, the PP/ST should specify, for each type of controlled subject and information, the security attributes that are relevant to the specification of the SFP rules. For example, such security attributes may be things such the subject identifier, subject sensitivity label, subject clearance label, information sensitivity label, etc. The types of security attributes should be sufficient to support the

environmental needs.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

The CC wording for FDP_IFF.1.1 and FDP_IFF.1.2 is confusing and unclear when it refers to an assignment of "the minimum number and type of security attributes":

- This is confusing in the area of "minimum number"; the annex fails to clarify this when it refers to a "minimum number...to support the environmental needs".
- This is unclear in that it seems to call for a simple list of security attributes, without association of security attributes to the controlled entities.

This interpretation corrects this problem. It makes it clear that an appropriate assignment is one that provides, for each controlled entity, the SFP-relevant security attributes of that entity. This can be clearly provided as a two column table: one column is the controlled entity (subject, information), the other is a list of SFP-relevant security attributes for that controlled entity.

#0364: Application Notes In Protection Profiles Are Informative Only

```
NUMBER:             0364
STATUS:             Approved by TTAP/CCEVS Management
TYPE:               Interpretation

TITLE:              Application Notes In Protection Profiles Are Informative
                    Only

EFFECTIVE DATE:     2000-03-27

CCITSE FAMILY:      Part 1: Introduction and General Model (PART_1)
SCOPE:              Common Criteria CC_PART1_V2 (CCITSE V2.1 Introduction and
                    General Model)
                    Common Evaluation Methodology CEM_PART2_V1 (Common
                    Evaluation Methodology V1.0 Part 2)
DOCUMENT(S):        <None>
RELATED TO:         <None>
```

STATEMENT:

The following interprets Section B.2.7 of Part 1, which states:

> B.2.7 Application notes
>
> This optional section may contain additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.

Application Notes are not normative; they provide information only.

CRITERIA AND/OR METHODOLOGY CHANGES:

To address this interpretation, the following paragraph should be added to Part 1, Section B.2.7.:

> Application notes should not contain normative information; rather, they should provide additional clarification or guidance information. It should be clear to what document element (e.g., threats, objectives, component elements) the application note applies, and the application note should be consistent with that document element.

To make Part 3 consistent with Part 1, the following should be added to the APE class:

> Application Notes (APE_APP)
>
> **Objectives**

#0364: Application Notes In Protection Profiles Are Informative Only

> Application Notes, if present, provide additional clarification or guidance information with respect to document elements (e.g., threats, objectives, component elements) of the PP.
>
> **APE_APP.1 Application Note Requirements**
>
> Dependencies: No Dependencies
>
> Developer Action Elements:
>
> None, as application notes are optional.
>
> Content and Presentation Elements:
>
> APE_APP.1.1C Application notes, if provided, shall be informative only.
>
> APE_APP.1.2C Application notes, if provided, shall be consistent with the specific elements of the PP to which they apply.
>
> Evaluator Action Elements:
>
> APE_APP.1.1E The evaluator shall confirm that any provided application notes meet all requirements for content and presentation of evidence.

There should be corresponding changes in the CEM to reflect the new Part 3 component.

PROJECTED IMPACT:

Some existing PPs may contain application notes with normative or inconsistent material.

SUPPORT:

The words in Part 1, Section B.2.7 are potentially misleading with respect to application notes, as the phrase "useful for the ... evaluation" has been read by some to allow normative material in application notes. However, for functional elements, the application notes are contained in the Part 2 Annex, which states at the beginning of the annex:

> This annex contains informative guidance for the families and components found in the main body of Part 2, which may be required by users, developers or evaluators to use the components.

Further, Section A.1.2 of the Part 2 Annex clearly notes that any user or evaluator notes are informative (A.1.2.2, A.1.2.3). Section A.1.3.2 notes that the application notes at the component level are "additional refinement in terms of narrative qualification as it pertains to a specific component." Refinement of an informative section can never be normative.

This leads to the conclusion that application notes are informative *only*, and that any normative material should be expressed through predefined components, refinements of predefined components (such as to specify a specific method of implementation) or explicitly specified requirements.

Further, application notes should not contradict the document element to which they apply. For example, it would be confusing to an evaluator or developer to have an element require only passwords, and the associated application discuss the use of non-password biometric devices. A larger scope of consistency analysis is not required due to transitivity: if the note is consistent with its associated element, and that element is consistent with the remainder of the PP (when called for in the APE requirements), then the application note should be

similarly consistent.

Application notes are unique in Part 1, Annex B in that they are not explicitly mentioned in any other document area, and that they are optional. However, practice has allowed them to appear in other document areas. As such, the easiest way to address application notes in Part 3 was to create a new family to address application notes, wherever they may appear.

#0385: Identification Of Standards

```
NUMBER:             0385
STATUS:             Approved by TTAP/CCEVS Management
TYPE:               Interpretation

TITLE:              Identification Of Standards

EFFECTIVE DATE:     2000-03-27

CCITSE FAMILY:      Protection Profile, IT Security Requirements (APE_REQ)
SCOPE:              Common Criteria CC_PART3_V2 (CCITSE V2.1 Assurance
                    Requirements)
                    Common Evaluation Methodology CEM_PART2_V1 (Common
                    Evaluation Methodology V1.0 Part 2)
DOCUMENT(S):        <None>
RELATED TO:         <None>
```

STATEMENT:

The following interprets both the APE_REQ and ASE_REQ families in Part 3 of the Common Criteria:

Claims about use of a standard must be unambiguous with respect to the source of a metric and the meaning of compliance. If a compliance claim is made, the PP/ST author must provide an indication of how compliance is to be determined.

CRITERIA AND/OR METHODOLOGY CHANGES:

To address this intepretation, the following elements should be added to the Content and Presentation elements of APE_REQ.1, with parallel additions to the Content and Presentation elements of ASE_REQ.1:

> APE_REQ.1.xC: All requirements that claim compliance with an external standard shall be unambiguous with respect to the source of the metric and the meaning of compliance.
>
> APE_REQ.1.xC: All requirements that claim compliance with an external standard shall stipulate how compliance is ascertained.

For these units, an application note should be added along the lines of the following:

> In some instances, it is appropriate for a PP/ST to claim compliance with an external standard, such as the definition of an encryption algorithm. When the standards document provides only one mode of operation of the algorithm, or level of use of the algorithm, this is not a problem. However, some standards define multiple approaches, and a simple citation is insufficient. Citations of an external standard should be unambiguous with respect to what is being required.

#0385: Identification Of Standards

> If the standards specifies multiple modes or manners of operations, the citation should be specific enought to determine which mode or manner of operation applies to the TSF.
>
> Additionally, there are many ways of determining compliance with a standard. It may be performed as part of the TOE evaluation, it might be a developer claim, or it might be verified by an independent party. In order to have consistency across evaluations, the PP/ST author should specify the means of determining compliance, so that consistency of interpretation across all uses of the PP/ST is achieved.

Additional work units should be added to the CEM to address these new elements.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

In some instances, it is appropriate for a PP/ST to claim compliance with an external standard, such as the definition of an encryption algorithm. When the standards document provides only one mode of operation of the algorithm, or level of use of the algorithm, this is not a problem. However, some standards define multiple approaches, and a simple citation is insufficient. This interpretation requires citations of an external standard to be unambiguous with respect to what is being required. If the standards specifies multiple modes or manners of operations, the citation must be specific enought to determine which mode or manner of operation applies to the TSF.

Additionally, there are many ways of determining compliance with a standard. It may be performed as part of the TOE evaluation, it might be a developer claim, or it might be verified by an independent party. In order to have consistency across evaluations, the PP/ST author should specify the means of determining compliance, so that consistency of interpretation across all uses of the PP/ST is achieved.

6.0 Appendix B - List of Acronyms

- ARCC Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security.
- CC Common Criteria version 2.1.
- CEM Common Evaluation Methodology version 0.6 for part 1 and 1.0 for part 2.
- PP Protection Profile.
- PSS Peripheral Sharing Switch for Human Interface Devices.
- TTAP Trust Technology Assessment Program.

7.0 Appendix C - Glossary of Terms

Assurance - Grounds for confidence that an entity meets its security objectives.

Class - A grouping of families that share a common focus.

Component - The smallest selectable set of elements that may be included in a PP, an ST, or a package.

Element - An indivisible security requirement.

Evaluation - Assessment of a PP, an ST or a TOE, against defined criteria.

Evaluation Assurance Level (EAL) - A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.

Package - A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.

Protection Profile (PP) - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Target of Evaluation (TOE) - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

1

8.0 Appendix D - References

- Common Criteria, version 2.1, Part 1, CCIMB-99-031.
- Common Criteria, version 2.1, Part 2, CCIMB-99-032.
- Common Criteria, version 2.1, Part 3, CCIMB-99-033.
- Common Evaluation Methodology, version 0.6, Part 1, CEM-97/017.
- Common Evaluation Methodology, version 1.0, Part 2, CEM-99/045.
- Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, version 1.0, 17 July 2000.
- http://www.radium.ncsc.mil/tpep/
- http://niap.nist.gov/
- http://niap.nist.gov/cc-scheme/
- http://www.commoncriteria.org/