CAFE LAB

Voltaire Advanced Data Security, Ltd.
2in1 PC™
Final Evaluation Report
Version 1.5

Robert J. West
Nicholas Pantiuk
Eric J. Grimes

June 7, 1999

COACT, Inc. Rivers Ninety-Five
9140 Guilford Road, Suite L
Columbia, Maryland 21046
Phone: 301-498-0150
Fax: 301-498-0855

Registration No. TTAP-CC-0004
Document No. CA-0299-011

TABLE OF CONTENTS

TABLE OF CONTENTS – CONTINUED

TABLE OF CONTENTS – CONTINUED

TABLE OF CONTENTS – CONTINUED

TABLE OF CONTENTS – CONTINUED

TABLE OF CONTENTS – CONTINUED

TABLES

TABLES – CONTINUED

APPENDICES

SECTION 1

EXECUTIVE SUMMARY

1 PRODUCT OVERVIEW

The Target of Evaluation (TOE) is the 2in1 PC™ card, the supporting software provided on the installation floppy diskettes, and the documentation provided as part of the 2in1 PC™ product developed by Voltaire that provides physical separation between two networks through the use of a hardware based security controller that is embedded on the 2in1 PC™ card. The 2in1 PC™ card is installed on a single host PC that conforms to the PC/AT standard and is configured by using the supplied installation diskettes. These diskettes partition the host PC's hard disk into three or four separate disk partitions and allow for the configuration of the security functions on 2in1 PC™ card itself. Once the 2in1 PC™ card has been configured, the security controller manages both the PC's connection between two networks and the access to the PC's configured disk partitions. This enables a single PC to securely connect to two physically separated network connections, while protecting the data stored on the PC's hard disk(s). Security is achieved by a state machine that allows the PC to access only the network connection and disk partition(s) associated with that machine state.

The 2in1 PC™ installation disks partition a PC into two distinct user domains (A and B). Each of the domains consists of a portion of the hard disk, a network connection, and, optionally, some other devices (e.g., floppy disk, SCSI interface, etc.). It also provides a capability for an administrator to set-up and configure the controls necessary to implement these functions.

The TOE recognises two types of users (roles), users and administrators, and two modes of operation, work mode and set-up mode. In work mode, there are three user machine states; A, B, and Transition (T), and four user visible functions that the TSF controls. They are:

1. Read or write access to disk partitions,

2. Connectivity to networks,

3. Connectivity to other (optional) TSF controlled devices, and

4. Switch user states.

In set-up mode, only the administrator function is recognised and permits the Initialisation or modification of parameters and configuration information. In this mode, I/O operations to the hard disk are not monitored and both network connections are severed. The administrator role is determined through the installation of an internal set-up

plug or the use of an external set-up plug in combination with an internal enabler plug inserted onto the 2in1 PC™ card. A user is identified by the absence of a set-up plug.

The TOE has four security policies. The first is the Partitioning Access Policy, which controls access between users and the protected objects that they access (i.e., disk partitions, network connections, and other interfaces). The second policy is the Administrator Access Policy, which controls write access to the EEPROM. The EEPROM is where many of the security parameters and attributes that are used to control the Partitioning Access Policy are stored. The third policy is the Identification and Authentication Policy, which specifies the two user types recognised by the 2in1 PC™ card. The fourth policy is the Floppy Disk Switching Policy, which controls the access to the floppy disk drive when switching through the Transition machine state.

The TOE configuration is accomplished using a standard PC that was not evaluated. The TOE is at the Evaluation Assurance Level 2 (EAL2). The EAL2 assurance requirements are augmented by an Informal Security Policy Model requirement (ADV_SPM.1). The TOE was evaluated against the requirements shown in Table 1-1, Security Functional Requirements, and Table 1-2, Assurance Requirements.

Security Functional Requirement	Description
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Security Attribute Based Access Control
FDP_ITC.1	Import of User Data Without Security Attributes
FIA_UID.2	User Identification Before Any Action
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_SMR.1	Security Roles
FMT_SMR.3	Assuming Roles
FPT_FLS.1	Failure with Preservation of Secure State
FPT_RCV.4	Function Recovery
FPT_RVM.1	Non-Bypassability of the TSP
FPT_SEP.3	Complete Reference Monitor

Table 1-1 Security Functional Requirements

Assurance Requirement	Description
ACM_CAP.2	Configuration Items
ADO_DEL.1	Delivery Procedures
ADO_IGS.1	Installation, Generation, and Start-Up Procedures
ADV_FSP.1	Informal Functional Specification
ADV_HLD.1	Descriptive High-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
ATE_COV.1	Evidence of Coverage
ATE_FUN.1	Functional Testing

Table 1-2 Assurance Requirements

ATE_IND.2	Independent Testing – Sample
AVA_SOF.1	Strength of TOE Security Function Evaluation
AVA_VLA.1	Developer Vulnerability Analysis

Table 1-2 Assurance Requirements (Cont.)

The CAFÉ Laboratory of COACT, Inc. evaluated the TOE against the security target as authorised by NSA under its Trust Technology Assessment Program. It was found that the TOE meets all the requirements defined in the Security Target and should be awarded a certificate at EAL2.

SECTION 2

IDENTIFICATION

2 IDENTIFICATION

This section provides product identification information.

2.1 TITLE

Voltaire 2in1 PC™

2.2 PRODUCT VERSION NUMBER

2in1 PC™ Version 1.21

2.3 VERSION NUMBERS FOR PRODUCT CONTENTS

2in1 PC™ card Version 1.21
Installation Disks Version 1.21
2in1 PC™ Installation Guide Version 1.21
2in1 PC™ Quick Installation Guide Version 1.21
2in1 PC™ User Guide Version 1.21
2in1 PC™ Application Notes Version 1.21

2.4 EVALUATION ASSURANCE LEVEL (EAL)

Functional and Assurance claims conform to EAL-2 (Version 2 Final of the Common Criteria, May 1998)

2.5 CONFORMANCE CLAIM

The 2in1 PC™ Version 1.21 TOE is compliant with the Common Criteria, Part 2, functional requirements specified in the Security Target and listed in Table 1-1.

The 2in1 PC™ Version 1.21 TOE is compliant with the Common Criteria, Part 3, assurance requirements for EAL2 augmented with ADV_SPM.1, Informal TOE Security Policy Model. This is consistent with the Security Target and the requirements are listed in Table 1-2.

The 2in1 PC™ Version 1.21 TOE does not claim conformance to any Common Criteria Protection Profiles (PP) as of the date of the development of this Security Target.

2.6 REGISTRATION

Registration No. TTAP-CC-0004

2.7 KEYWORDS

Multi-level security, COTS, access control, discretionary control, network security, network security hardware, networked information systems, data security, and information protection.

SECTION 3

SECURITY POLICY

3 SECURITY POLICY

This section describes the four security policies implemented in the TOE. Two of these policies are access policies, the Partitioning Access Policy and Administrator Access Policy. The Partitioning Access Policy controls access between users and the protected objects that they access (i.e., disk partitions, network connections, and other interfaces). The Administrator Access Policy controls write access to the EEPROM. The EEPROM is where many of the security parameters and attributes that are used to control the Partitioning Access Policy are stored. The other two policies deal with specific conditions. They are the Identification and Authentication Policy and the Floppy Disk Switching Policy.

3.1 PARTITIONING ACCESS POLICY

The Partitioning Access Policy is a role based policy intended to contain a user session to an authorised environment that includes a network connection, disk partition(s), and other local interfaces, depending on the local organisational security policy and the configuration settings set-up by the administrator. This policy applies to both the user roles and administrator roles, however the administrator is not subject to the rules relative to disk partitions and has no access to the controlled networks.

The subjects of the TOE Security Functions (TSF) are users and processes operating on behalf of users. The objects are disk partitions, network connections, and control of other external devices (optional). The operations between subjects and disk partitions are read and write. The operations between subjects and the other objects (i.e., network connections and hardware interfaces) are connected or not connected.

The TOE state machine implements three different user states with different access rules. Within each of these states, access is controlled to disk partitions, network connections, and other external devices (optional).

The administrator sets the parameters that control a part of the security policy during the initial set-up of the TSF. The administrator controllable parameters are:

1. Partition boundaries – A, B, T, and F(configurable – see Section 4);

2. If partition F exists, the access permissions (i.e., Read, Write, Read/Write, or No access) to partition F from each of the machine states (i.e., A, B, and T);

3. If a second disk is present in the configuration, the state in which it is available (i.e., A or B);

4. If access to other interfaces (e.g., floppy disk and SCSI interfaces) are controlled by the TSF, the state in which they are available (i.e., A, B, !A, or !B).

(Note: !A means available in all states except A. !B means available in all states except B. Either of these provides for the device to be available during the Transition state. Devices connected through !A or !B are also available in set-up mode.)

Table 9.1.5.1-1 lists all of the administrator dependent attributes and parameters.

Table 3.1-1 shows the access rules enforced in the Transition state (i.e., state T).

Objects	Allowable Access By Subjects
Four separate disk partitions	
Functional	Selectable* (Default – No access)
B	No access
Transition	Selectable* (Default – Read only)
A	No access
Two network connections	
B	No connection
A	No connection
Other hardware interfaces (e.g., Floppy and SCSI interfaces) – as configured	
A	No connection
!A	Connected
B	No connection
!B	Connected
* Access permissions as defined by the administrator.	

Table 3.1-1 Transition State Access Rules

The Transition state is considered to be secure because it allows no network connectivity, no access to the A, B, or F disk partitions, read only access to the Transition disk partition, and access only to other connected devices that are connected through the !A (Not A), or !B (Not B) jumper pins. A PC with the TOE installed (without the set-up plug installed on the 2in1 PC™ card), that has been shut down for any reason will always boot up into the controlled Transition state, where the environment is trusted and cannot be altered by either a user or an intruder. Table 3.1-2 shows the access rules enforced in user state A.

Objects	Allowable Access By Subjects
Four separate disk partitions	
Functional	Selectable* (Default – Read only)
B	No access
Transition	No access
A	Read/Write
Two network connections	
B	No connection
A	Connected

Table 3.1-2 State A Access Rules

Objects	Allowable Access By Subjects
Other hardware interfaces (e.g., Floppy and SCSI interfaces) – as configured	
A	Connected
!A	No connection
B	No connection
!B	Connected
* Access permissions as defined by the administrator.	

Table 3.1-2 State A Access Rules (Cont.)

Table 3.1-3 shows the access rules enforced in user state B.

Objects	Allowable Access By Subjects
Four separate disk partitions	
Functional	Selectable* (Default – Read/Write)
B	Read/Write
Transition	No access
A	No access
Two network connections	
B	Connected
A	No connection
Other hardware interfaces (e.g., Floppy and SCSI interfaces) – as configured	
A	No connection
!A	Connected
B	Connected
!B	No connection
* Access permissions as defined by the administrator.	

Table 3.1-3 State B Access Rules

3.1.1 Exceptions to the Partitioning Access Policy

When the administrator has identified himself by inserting the set-up plug into the 2in1 PC™ card the following exceptions are made to the Partitioning Access Policy:

1. Unconditional access is allowed to all disk partitions. Typically, the administrator accesses only partitions associated with the partition he is booted from, but that access is not monitored or controlled by the TSF.

2. No network connections are allowed.

3. Other device connections are allowed for devices associated with !A (Not A) or !B (Not B), and disallowed for devices associated with A and B.

4. Always boot into A, boot into T is bypassed.

3.2 ADMINISTRATOR ACCESS POLICY

The Administrator Access Policy provides the rules for write access to the EEPROM, where many of the security parameters and attributes that are used to control the

Partitioning Access Policy are stored. Other dynamic parameters, such as the current machine state, are stored in the Altera chip.

The Administrator Access Policy is a role-based policy intended to limit write access to the EEPROM to administrators. Like the Partitioning Access Policy, the subjects are users and processes operating on behalf of users, but the only object is the EEPROM and the only controlled operation is write. The Administrator Access Policy is very simple; administrators may write to the EEPROM, users may not.

3.3 IDENTIFICATION AND AUTHENTICATION POLICY

Another security policy covers identification and authentication. The TOE identifies only user roles (i.e., user and administrator), not users as individuals. By definition, any individual operating without the set-up plug in place is a user. Also by definition, any individual operating with the set-up plug in place is an administrator.

3.4 FLOPPY DISK SWITCHING POLICY

The final policy enforced by the TOE has to do with state switching after DMA2 activity has been detected. This detection is performed by the DMA controller receiving DMA2 activity from the ISA bus only. Since PCI devices do not interface with the DMA controller, their operation is not monitored by the TSF. The Floppy Disk Switching Policy states that, in the Transition state, once DMA2 activity has been detected, the state machine may not change without a reboot from the hard drive. Table 3.4-1 shows the rules enforced by the Floppy Disk Switching Policy.

State	DMA2 Activity Detected	Switching Allowed
T	No	Yes
T	Yes	No

Table 3.4-1 Floppy Disk Switching Policy Rules

SECTION 4

ASSUMPTIONS AND CLARIFICATION OF SCOPE

4 ASSUMPTIONS AND CLARIFICATION OF SCOPE

This section provides information about assumptions regarding organisational security policy and the operating environment used in the evaluation of the TOE, clarification of the scope of the evaluation, and clarification of some terminology used either by the vendor or the evaluators.

4.1 ORGANISATIONAL SECURITY POLICY ASSUMPTIONS

The following organisational security policies are beyond the scope of the Target of Evaluation (TOE) and were assumed to be implemented in the evaluation:

1. Users must be identified and authenticated before access to the TOE can be granted.
   Rationale: In some environments, identification and authentication mechanisms may be required and therefore must be supplied by the operational environment, as the TOE only requires identification for administrator privileges.

2. Administrators of the system will be adequately trained, enabling them to effectively implement organisational security policies.
   Rationale: Administrators are expected to use IT resources and information in accordance with the organisational security policy. In order for this to be possible, administrators must be adequately trained to understand the purpose and need for security controls, and to be able to make secure decisions with respect to their discretionary actions.

3. The organisation's IT resources must be used only for authorised purposes.
   Rationale: In conjunction with the TOE environment, users must ensure that the organisation's information technology is not used for unauthorised purposes.

4. The organisation's IT systems must be implemented and operated in a manner that represents due care and diligence with respect to any risks to the organisation.
   Rationale: It is important that the level of security afforded the IT system be in accordance with what is generally considered adequate within the business or government sector in which the organisation is placed.

4.2 ENVIRONMENTAL ASSUMPTIONS

The specific conditions listed below are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

1. The operating systems and supporting software stored in the Transition, A, and B disk partitions are not relied upon for security functionality.
   Rationale: These components are beyond the scope of the TSF.

2. Users of the TOE are trusted not to modify the hardware configuration.
   Rationale: Personnel security and determination of trusted users is beyond the scope of the TOE.

3. The TOE will be located in a controlled environment (i.e. basic physical security is assumed to prevent modification of the system hardware / software).
   Rationale: Physical security of the host system is beyond the scope of the TOE.

4. The Personal Computer (PC) platform fully complies with the PC/AT standard and uses an IDE controller for the primary system disk.
   Rationale: Standard compliance of the host system is beyond the scope of the TOE.

4.3 CLARIFICATION OF SCOPE

Administrator set-up software is not a part of the TSF and is not used in work mode. It exists on the 2in1 PC™ installation disks and should never be left available to a user. The administrator must use physical and procedural means to protect these disks. The first disk is a bootable floppy disk that will run only in set-up mode (i.e., with the administrator set-up plug installed on the 2in1 PC™ card).

There is a “SWITCH” process present in each machine environment (i.e., machine states A, B, and T, loaded with whatever TOE compatible operating system is loaded in their disk partitions). This “SWITCH” process is executed when the user initiates it, either by clicking the icon or by invoking the “SWITCH” command, depending on the operating system and/or user choice. The “SWITCH” process notifies the TOE of its intent to change user states on the next reset signal, and then causes a reset signal to be sent. This process is not part of the TSF. This process is provided for the convenience of the user, but the user could choose to provide the same functionality himself. The user interface to the TSF, for the purpose of a state change, is the combination of the two events from the user. If the user does not initiate the events, or initiates only one of the events, the state change does not occur and the user is left in his present state.

The TOE must be installed on a PC/AT compatible system with an IDE controller for the primary system drive. It does not rely on this system for any security functionality, and it

does not claim to provide any security functionality for any system that does not meet these standards.

4.4 TARGET OF EVALUATION

The TOE is the 2in1 PC™ card, the supporting software provided on the installation floppy diskettes, and the documentation provided as part of the TOE developed by Voltaire.

4.5 CLARIFICATION OF TERMINOLOGY

In this evaluation, the following terms and phrases have a specific meaning that may differ somewhat from common usage.

Control Access to External Devices (e.g., floppy disk and/or SCSI interface) – Access control to external devices is provided by controlling the passage of a control signal (e.g., "device ready" for the floppy disk) on the device ribbon cable. The wire carrying the control signal is physically interrupted and taken from the ribbon cable and connected to jumper pins on the 2in1 PC™ card. From the input jumper pin, the connection is routed through an electro-mechanical relay to the output jumper pin. Access is controlled to the device by allowing or not allowing the control signal through the electro-mechanical relay. No other command, address, or data line on the device cable is monitored by the TSF. By PC standard convention, the interface will not recognise any command, address, or data present on the device cable until the control signal is received.

Optional – The internal enabler plug, external set-up plug, and the cables provided to control external devices are additional elements that were not included as part of the TOE. These additional elements were ordered from the developer and their functionality was evaluated to verify that the jumper pins on the 2in1 PC™ card do provide the ability to control external devices and that the combination of the internal enabler plug and the external set-up plug is an equivalent to the internal set-up plug.

Detect Floppy Disk Usage – Floppy disk usage is associated and is based on the detection of DMA2 (DRQ2) signals on the ISA bus. This detection is performed by the DMA controller receiving DMA2 activity from the ISA bus only. Since PCI devices do not interface with the DMA controller, their operation is not monitored by the TSF.

Control Access to Networks – Access control to networks is provided by controlling the passage of the network connection through two electro-mechanical relays. Both relays must be closed for the network connection to be made.

Secure/Public – Various developer documents refer to the user (i.e., work mode) states, as well as disk partitions, network and external device connections, as "Secure" and "Public". These terms are merely labels the developer uses for the machine states and the protected assets associated with them. In this context, the term "Secure" does not imply that there is any inherent security associated with it. Some of the developer

documentation, and in this report, "A" and "B" have been used in lieu of "Secure" and "Public."

Disk Partitions – the 2in1 PC™ installation disks use POWERQUEST Partition Magic to partition the hard disk into either three or four partitions. The 2in1 PC™ card stores the partition boundary addresses of each of the partitions and controls access to the partitions based on these boundaries. The partitions are:

1. A – This is a user accessible disk partition associated with and available in machine state A. This partition is the first partition on the hard disk, starting at physical address 0,0,1. Whenever the TOE transitions into state A, the PC is rebooted from disk partition A. The A partition is not accessible in states B or T.

2. B – This is a user accessible disk partition associated with and available in machine state B. Whenever the TOE transitions into state B, the PC is rebooted from disk partition B. The B partition is not accessible in states A or T.

3. T – This disk partition is associated with and available in machine state T. The default access permission for the T partition is read only, but may be changed by the administrator. Whenever the TOE transitions into state T, the PC is rebooted from disk partition T. The T partition is not accessible in states A or B.

4. F – This is a configurable user accessible disk partition that is not automatically associated with or available in any machine state. It is intended to provide a controlled way of passing information between machine states A and B. If this disk partition is desired on a particular instantiation of the TOE, the administrator must set-up the access rules for it. The default access rules for the F disk partition are read only from state A, read/write from state B, and not accessible from state T. Assuming that state A is a more restrictive (e.g., higher) security level than state B, the default access rules would provide the ability for B to write up, through the F partition, to A. It would prevent a write down from A, through F, to B.

SECTION 5

ARCHITECTURE

5 ARCHITECTURE

This section describes the TOE architecture.

5.1 SYSTEM OVERVIEW

2in1 PC™ is an ISA PC card that is confined to a single host, intended to interface with a networked environment. It provides the ability to connect a host PC to two physically separate networks while providing secure connectivity to each network and data protection for each network by monitoring access to the host's hard disk partitions. This separation of networks and data defines the operating states that the TOE can operate in, i.e. Secure (A), Public (B) or Transition. These states are defined as:

1. Secure (A) – When the host PC is running in the Secure (A) operating state, connection is only made to the secure network. Access to the Secure (A) disk partition is allowed, access to the Functional disk partition is configurable (i.e. Read-only, Read/Write or No Access) and access to the other disk partitions is denied (i.e. the Transition and Public (B) disk partitions).

2. Public (B) – When the host PC is running in the Public (B) operating state, connection is only made to the public network. Access to the Public (B) disk partition is allowed, access to the Functional disk partition is configurable (i.e. Read-only, Read/Write, or No Access) and access to the other disk partitions is denied (i.e. the Transition and Secure (A) disk partitions).

3. Transition – When the host PC is running in the Transition operating state, all network connections are severed. Access to the Transition partition is configurable (i.e. Read-only or Read/Write access), access to the Functional disk partition is configurable (i.e. Read-only, Read/Write, or No Access) and access to the other disk partitions is denied (i.e. the Secure (A) and Public (B) disk partitions). The host PC is booted into the Transition state when the PC is powered on, when switching between the Secure (A) and Public (B) operating states and when the PC has been rebooted.

The TOE provides separation between the Secure and Public network connections and protects from access to disk partitions not related to the current operating state. Each of the two network connections are controlled by two electromechanical relays and these relays control the connectivity to each network based upon the current operating state stored in the Altera chip on the 2in1 PC™ card. The current operating state stored in the Altera chip also restricts access to the PC's hard disk partitions. The restrictions for hard

disk access in each operating state is read from the EEPROM during the beginning of each boot process. Once these access restrictions are stored in the Altera chip, all IDE traffic is filtered based upon the partition borders it read from the EEPROM. Traffic that is allowed based on the disk borders for the current operating state is allowed to pass. Traffic that is not allowed based on the disk borders for the current operating state is denied. The 2in1 PC™ card also provides the ability to control the access to peripheral devices. This is performed by purchasing an optional device cable available from Voltaire and then connecting the severed line on the cable to the jumpers on the 2in1 PC™ card. Access for up to two devices can be controlled by the 2in1 PC™ card (details of the jumper connections are located in Section 3.1 Partitioning Access Policy). Finally, when configuring the 2in1 PC™ card, the TOE provides the administrator the ability to install other software into the Transition partition. This software could include Identification and Authentication (I&A) mechanisms to prevent a user from being able to boot the PC into the Secure (A) or Public (B) operating states until the I&A has been successfully verified.

5.2 HARDWARE OVERVIEW

2in1 PC™ is an ISA slot PC card that provides the ability to monitor access to one or two IDE-ATA compatible hard drives on the host PC. The monitoring of disk access is performed by filtering all traffic on the IDE bus based upon the borders for each partition that the current operating state is restricted by. These borders are enforced for all of the disk partitions created after the installation of the TOE (i.e. Secure (A), Public (B), Transition and the configurable Functional disk partitions). Other TOE hardware used during the evaluation are identified as:

1. Internal set-up plug – included as part of the TOE to enable user identification to configure the card's Security Functions. Users that have the internal set-up plug are defined as an administrator. Users that do not have the internal set-up plug are defined as a user.

2. Internal enabler plug – optional device used in conjunction with the external set-up plug to enable user identification to configure the card's Security Functions. This device would remain on the 2in1 PC™ card and inserting the external set-up plug would then provide the same functions as if the internal set-up plug were installed. Users that have the external set-up plug are defined as an administrator. Users that do not have the external set-up plug are defined as a user.

3. External set-up plug – optional device used in conjunction with the internal enabler plug to enable user identification to configure the card's Security Functions. This device would be inserted into the external jack on the 2in1 PC™ card and would provide the same functionality offered by inserting the internal set-up plug (Note: the internal enabler plug must also be installed on the 2in1 PC™ card). Users that have the external set-up plug are defined as an administrator. Users that do not have the external set-up plug are defined as a user.

4. Y cable – included as part of the TOE to provide the connectivity from each of the networks connected to the 2in1 PC™ card to the Network Interface Card (NIC) on the host PC.

5. Two IDE cables – included as part of the TOE to connect the hard disk(s) to the 2in1 PC™ card and the 2in1 PC™ card to the IDE controller.

6. Floppy disconnection cable – optional device used to verify the disabling of the ability to send data to a floppy disk for each of the PC operating states (i.e. Transition, Secure (A) and Public (B)).

5.3 SOFTWARE OVERVIEW

The TOE includes software that is provided on diskettes one and two of the installation software. This software was used during the installation and reconfiguration of the 2in1 PC™ card. The details of the software components on the installation diskettes are defined in Section 9.2.1 ACM_CAP.2 Configuration Items. The details of other software used during the independent testing are defined in Section 9.2.12 Independent Testing – Sample.

SECTION 6

DOCUMENTATION

6 DOCUMENTATION

This section describes the user and administrator guidance documents and lists all of the documents that Voltaire provided to support this evaluation.

6.1 USER GUIDANCE

The User Guidance describes the Switching and Data Transfer functions permitted to the user. It also provides a description of the necessary actions and expected results when using the appropriate keyboard or mouse inputs for the Windows 95/98/NT 4, Windows 3.11/NT 3.51, MS-DOS, and Linux/SCO operating systems. (Ref. *Voltaire 2in1 PC™ User Guide*)

The User Guidance describes the two basic functions provided for the user when using the TOE. The Switching function enables the user to switch between the A and B machine states as required. The Data Transfer function is an option which allows the transfer of data from one machine state to another and will normally be only possible in one direction, e.g., data could be copied from machine state B to A but not from A to B. The configuration of the parameters for these functions is done by the administrator during installation of the TOE and cannot be accessed or modified by the user. The User Guidance also provides a description of the necessary actions and expected results when using the appropriate keyboard or mouse inputs for the Windows 95/98/NT 4, Windows 3.11/NT 3.51, MS-DOS, and Linux/SCO operating systems.

6.2 ADMINISTRATOR GUIDANCE

The Administrator Guidance is contained in the *2in1 PC™ Installation Guide* and is supplemented by *2in1 PC™ Application Notes*. The administrator function is invoked in the set-up mode through the use of an internal or external set-up plug as applicable.

The Administrator Guidance provides a detailed overview of the TOE security functionality available to the administrator in the set-up mode. It also provides step-by-step set-up mode procedures, configuration settings, and descriptions of the necessary actions and expected results when using the appropriate keyboard or mouse inputs for the Windows 3.1/95/NT, and MS-DOS operating systems.

The Administrator Guidance describes the use of security parameters and their secure values as appropriate. The administrator controls parameters for the following functions:

1. Configuring the 2in1 PC™ card
    a. Custom names for the state machines
    b. Disk space allocated to the A, B, and Functional partitions
    c. Size of A and/or B partitions
    d. Access to the Functional partition from the A, B, and Transition state machines
    e. Transition settings
        1) Power-up mode
    f. Advanced settings
        1) Reset signal
        2) Network mode
        3) Second hard drive
        4) Forced shutdown

2. Installing Special Software to the Transition Area
    a. Writing to the appropriate batch file

3. Installing a Reset Cable, if necessary

4. General Hardware Dependent Settings (Application Notes)
    a. BIOS Settings
    b. Hard Disk Settings
    c. Specific Platform Dependent Settings

6.2.1 Security-Relevant Events

The Administrator Guidance provides detailed descriptions and procedures for security-relevant events. Specifically, the following security-relevant administrative functions are described.

1. Changing to the 2in1 PC™ Set-up Mode
    a. Internal Set-up
    b. External Set-up

2. Configuring Your 2in1 PC™

3. Completing the Installation Flow

4. Installing Operating Systems

5. Installing 2in1 PC™ Drivers

6. Working with the 2in1 PC™

    a. Switching Machine States (rebooting)
    b. Shutting Down the 2in1 PC™ System

7. Reconfiguring, Reinstalling or Removing the 2in1 PC™ Card

8. Installing Special Software or Re-installing an Operating System

9. Advanced Configurations
   a. Dual Disk Configuration
   b. Configuring an Extended Partition in Windows NT

10. Application Notes
   a. General Hardware Dependent Settings
   b. Chip Sets
   c. BIOS Settings
   d. Hard Disk Settings
   e. Specific Platform Dependent Settings

6.3 VENDOR DOCUMENTS PROVIDED IN SUPPORT OF EVALUATION

The following is a list of documents provided by the vendor in support of this evaluation (the numbering system used for each document is defined as, digits one and two represent an EAL-2 level evaluation; digits three through six define the month and date the document was delivered to the evaluation lab; digits seven through nine define the specific control number assigned to every document; and the bracketed numbers identify the document as being revision one, revision two, and so on).

E20598004 – *2in1 PC™ Physical Data Security*
E20598005 – *2in1 PC™ Security Claims*
E20698006 – *2in1 PC™ Administrative Rights*
E20698007 – *2in1 PC™ Security Policy*
E20698008 – *2in1 PC™ Flow Policy*
E20698009 – *2in1 PC™ Hardware Design*
E20698010 – *2in1 PC™ Terminal Map*
E20598011 – *2in1 PC™ Product Approval Tests*
E20598012(2) – *2in1 PC™ Software Design Document (Windows 3.11 – DOS)*
E20598013 – *2in1 PC™ Software Design Document (Windows NT)*
E20598014 – *2in1 PC™ Software Design Document (Windows 95)*
E21098015 – *2in1 PC™ Software Design Document (Windows 98)*
E21098016 – *2in1 PC™ System Development Plan*
E21098017 – *2in1 PC™ Platform Qualifications Summary*
E20598018(2) – *2in1 PC™ Platform Tests Description*
E20598019(2) – *2in1 PC™ Install White Box Tests Sheet*
E20897020 – *2in1 PC™ Code Documentation*
E20898021 – *2in1 PC™ Hardware Failure*
E20898022 – *2in1 PC™ New Version Tests*
E20398023 – *2in1 PC™ White Paper*
E20598024 – *2in1 PC™ System Design Document*
E20498025 – *2in1 PC™ SPOCK Presentation*

E20198034 – *2in1 PC™ IDE Tests – Source Code*
E21198035(4) – *2in1 PC™ Informal Security Policy Model*
E20698036(3) – *2in1 PC™ Hacking Tests*
E21198037 – *Preliminary Evaluation of 2in1 PC™*
E21198038 – *2in1 PC™ Operating System QA Test*
E21198039(2) – *Evaluation of 2in1 PC™ Installation Guide, Version 1.21*
E21198040(2) – *2in1 PC™ Vulnerability Analysis*
E21198041(3) – *2in1 PC™ Configuration Items*
E21198042(3) – *2in1 PC™ Functional Testing*
E21198043(2) – *2in1 PC™ Tests Coverage*
E21197044 – *2in1 PC™ Product Requirements Document*
E21198045(3) – *2in1 PC™ Delivery Procedure*
E21198046 – *2in1 PC™ User Guide*
E21198047(2) – *2in1 PC™ Mapping of Assurance Elements*
E21198048 – *2in1 PC™ Claims*
E21198049 – *2in1 PC™ Relay Information*
E21298050 – *2in1 PC™ Software Components*
E21298053 – *2in1 PC™ Transition partition*
E21298054(4) – *2in1 PC™ Functional Specifications*
E21298056 – *2in1 PC™ Addendum to the 2in1 PC™ – Installation Software*
E21298057 – *2in1 PC™ IDE Tests – Output*
E21298058 – *2in1 PC™ Addendum to the 2in1 PC™ – The Transition partition*
E21298061 – *2in1 PC™ Updates to the SYD EEPROM Mapping Section*
E21298062 – *2in1 PC™ Application Notes*
E21298063 – *2in1 PC™ Installation Guide*
E21298064 – *2in1 PC™ Quick Installation Guide*
E21197065 – *2in1 PC™ IO Protocol Tests*
E20199066 – *2in1 PC™ Addendum to the 2in1 PC™ – System Design Document*

SECTION 7

PRODUCT TESTING

7 PRODUCT TESTING

The *Common Criteria, Part 3: Security assurance requirements,* Section 13, Class ATE: Tests, identifies the families of the "Tests" class and describes what the testing is intended to accomplish. Specifically, "Testing helps establish that the TOE security functional requirements are met. Testing provides assurance that the TOE satisfies at least the TOE security functional requirements, although it cannot establish that the TOE does no more than what was specified…" It also states that "The emphasis in this class is on the confirmation that the TSF operates according to its specification. …"

The developer's test documentation was checked and examined in accordance with the ATE_FUN.1C requirements identified in Section 9.2.11.1. The 2in1 PC™ functional test documents were developed to meet the content and presentation of evidence elements for ATE_FUN.1.

The developer test documentation included a test plan that provided enough information to fully satisfy the ATE_FUN.1, Functional Testing, element. The *2in1 PC Functional Testing* document clearly identifies the test approach and goals in the introductory section and provides a detailed analysis near the end of the document. The content of this document was reviewed by the evaluators and a selection of tests was made to be verified in section 9.2.12 ATE_IND.2 Independent Testing – Sample. Furthermore, the *Evaluation Test Plan for the 2in1 PC*™ was created to satisfy the ATE_IND.2 requirement. This document identifies the vendor tests that were selected and independent tests developed by the evaluators to confirm the TSF enforcement. These two test suites were identified by the evaluators to verify the validity of the developer's functional testing and provide correspondence to the functional specifications. Voltaire provided detailed test procedures for functional tests that could be replicated and verified by the evaluators, see Table 9.2.11.2.2-2. The second suite of tests was independently developed and performed by CAFÉ Lab evaluators, see Table 9.2.11.2.2-3. All of the test descriptions and results are contained in the *Evaluation Test Plan for the 2in1 PC™, Version 1.21*.

The EAL2 assurance that the TOE satisfies the security functional requirements is provided by analysis of all of the applicable Class ATE elements, i.e., ATE_COV (Evidence of Coverage), ATE_IND (Independent Testing - Sample), and ATE_FUN (Functional Testing). The evaluators determined that all of the elements were satisfied through a combination of developer test documentation, the CAFÉ LAB *Evaluation Test Plan for the 2in1 PC™, Version 1.21* and the tests performed and documented by the lab.

7.1 REPLICATED VENDOR TESTING

This section describes the vendor testing.

7.1.1 Details of the Test Suite

The platform used during the TOE vendor testing is defined as:

Computer: Twinbrook Systems, Intel 200Mhz Pentium-MMX
Mothercard: TX Chipset
Hard Disk: Seagate hard disk; model ST31720A, 1,705MB
BIOS Information: Award Modular BIOS Version 5.41PGM / Award Plug and Play BIOS Extension V1.0A
ISA Slot Cards: Voltaire 2in1 PC™, Version 1.21
Generic PIC Combo Network Interface Card (NIC)
Generic 16Bit SoundBlaster Compatible Sound Card
Diamond Stealth 4MB PCI Video Card / 3D 2000 Pro
Generic 33.6K Compatible Modem
Other: 32 MB SDRAM
24X LG CD-ROM Model CRD-8240B
Generic 3.5" 1.44MB NEC Floppy Diskette Drive
512K L2 Pipeline Burst Cache
Operating System Used for Evaluation: DOS 7, Windows 95
2in1 PC™ Drivers: Operating System Dependent
Other Software: 2in1 PC™ Configuration Information from the 2in1 PC™ Installation Diskettes, Version 1.21 (2 Disks)

The test suite used during the execution of the vendor performed tests included:

1. Twinbrook Systems, Intel 200Mhz Pentium-MMX – provided by the testing lab.

2. Fluke 75 Multi-meter – provided by the testing lab to evaluate the network connectors for test VT03 in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

3. llr.exe – source code was provided by the vendor and then compiled by the evaluation lab to test the low-level read access to the hard disk based on Cylinder, Head, Sector (CHS) and Logic Block Addressing (LBA) schemes. This application was used in test VT06 located in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

4. rwe2.exe – source code was provided by the vendor and then compiled by the evaluation lab to test the read and write permissions to the EEPROM on the 2in1 PC™ card. This application was used in tests VT01 and VT03 located in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

5. diskedit.exe (Norton) – provided by the vendor to read/write to specific addresses on the hard disk. This application was used in test VT05 (first and second sub-tests) located in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

The specific test details for the vendor tests performed are presented in Appendix A of the *Evaluation Test Plan for 2in1 PC™, Version 1.21*. Other applications installed on the system as part of the installation process (ref. 9.2.3 ADO_IGS.1 Installation, Generation, and Start-Up Procedures) were also used during the vendor testing. These applications were:

1. sense.exe – provided by installed files that were loaded onto the PC from installation disk 1. This application enables the administrator to verify that the configuration settings stored on the EEPROM have not been modified. A value is displayed in hexadecimal and reflects the current configuration settings, therefore any changes to the EEPROM's configuration will result in a different value being displayed. This application also displays the card's current working state (i.e. Secure (A), Public (B), or Transition).

2. report.exe – provided by installed files that were loaded onto the PC from installation disk 1. This application generates a report of the hard disk configuration (i.e. defining borders for each disk partition). This application works in conjunction with report.bat.

3. report.bat – provided by installed files that were loaded onto the PC from installation disk 1. This application executes report.exe and redirects the output to the display screen. This batch file was edited during the evaluation and renamed report2.bat so that the output could be redirected to a file for printing. The output of this file was used as a reference for other tests that were executed and is located after test VT02 in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

7.1.2 Test Configuration

The TOE was properly installed and configured in accordance with the steps provided in the *2in1 PC™ Installation Guide*. The configuration settings made during these steps are defined in the following tables.

Partition	Drive %	Total MB	Primary MB	Extended MB	File System	Access to Functional
Functional	3	49	----	----	FAT	----
Secure (A)	60	950	950	0	FAT	Read Only
Public (B)	37	592	592	0	FAT	Read/Write
Transition	----	9	----	----	FAT	No Access
Total: 100% 1600 MB						

Table 7.1.2-1 Partition Configuration

Transition Settings	Advanced Settings	
Power-Up Mode: Menu	Reset Signal	Advanced
	Network Mode	2in1 PC™
	2nd HD (if exists)	A only
	Force Shutdown	No

Table 7.1.2-2 Settings Configuration

Changes to the TOE configuration identified in the Tables above were performed for the following vendor tests:

1. VT05 (First Sub-test) – The TOE configuration was modified by changing the access to Functional to 'Read Only' when the PC is running in the Public (B) disk partition. This modification was performed to replicate the vendor supplied test procedures.

2. VT05 (Second Sub-test) – The TOE configuration was modified by changing the access to Functional to 'No Access' when the PC is running in either the Secure (A) or Public (B) disk partition. This modification was performed to replicate the vendor supplied test procedures.

3. VT06 – The TOE configuration was modified by changing the access to Functional to 'No Access' when the PC is running in either the Secure (A) or Public (B) disk partition. This modification was performed to replicate the vendor supplied test procedures.

7.1.3 Coverage and Depth Analysis

The developer test documentation evidence was evaluated as to the relevance of the identified security functions to be tested (ref. 9.2.11 ATE_FUN.1 Functional Testing). The selection of the developer tests was based upon a requirement to verify developer functional testing (see Section 9.2.11.2.3 Describe Scenarios) and correspondence to the tests mapped to the *2in1 PC™ Functional Specification*. With the confirmation of developer tests performed by the evaluators, a portion of the security functions within the TSC has been tested. Details of the vendor testing coverage are defined in Table 7.1.3-1 Developer Tests Correspondence to Functional Specifications.

Functional Specification	Developer Tests
1) Allow the setting up and configuration of the 2in1 PC™ attributes.	
2) Provide storage for configuration data (including card configuration and MBRs).	VT01
3) In WORK mode, provide a state machine with three distinct states of operation: A, B and T (Transition).	

Table 7.1.3-1 Developer Tests Correspondence to Functional Specifications

Functional Specification	Developer Tests
4) In WORK mode, provide a different MBR for each security state during boot.	
5) In WORK mode, control access to disk partitions based on the current security state and the access security policy.	VT05 VT06
6) In WORK mode, control access to networks based on the current security state and the access security policy.	VT02 VT04
7) In WORK mode, control the flow of state changes.	
8) Clear the PC's RAM during the Transition state.	Note: This function is not within the TSF.
9) In WORK mode, monitor access to the floppy disk during the Transition state and prevent state switching upon detection thereof.	VT07
10) In WORK mode, control access to external devices such as floppy drives and SCSI disks	
11) Detect the presence of a physical set-up plug in order to switch into Set-up mode and allow configuration.	VT03

Table 7.1.3-1 Developer Tests Correspondence to Functional Specifications (Cont.)

7.1.4 Testing Approach

The method of replicating the vendor tests was performed at the operating system interface level. The applications defined in Section 7.1.1, Details of the Test Suite, were relied upon by the operating system for all of the inputs and outputs from each of the vendor tests performed. Thus, in replicating the vendor tests the TSC included more than only the 2in1 PC™ card itself. This was due to the fact that all of the documented vendor test procedures were structured around a larger TSC, however in the independent testing of the product, the TSC was limited to only the 2in1 PC™ card, which is the defined TSC for this EAL2 evaluation.

7.1.5 Results of Vendor Testing

After the execution of all of the vendor tests, verification was made that each of the security functions performed as expected. Finally, with the inclusion of the replicated vendor tests defined in Section 7.1.3, Coverage and Depth Analysis, it was confirmed that all of the security functions within the TSC had been tested and performed as expected.

7.2 EVALUATOR TESTING

This section describes the evaluator testing.

7.2.1 Details of the Test Suite

The platform used during the TOE independent testing is defined as:

Computer: Twinbrook Systems, Intel 200Mhz Pentium-MMX
Mothercard: TX Chipset
Hard Disk: Seagate hard disk; model ST31720A, 1,705MB
BIOS Information: Award Modular BIOS Version 5.41PGM/Award Plug and Play BIOS Extension V1.0A
ISA Slot Cards: Voltaire 2in1 PC™, Version 1.21
Generic PIC Combo Network Interface Card (NIC)
Generic 16Bit SoundBlaster Compatible Sound Card
Diamond Stealth 4MB PCI Video Card / 3D 2000 Pro
Generic 33.6K Compatible Modem
Other: 32 MB SDRAM
24X LG CD-ROM Model CRD-8240B
Generic 3.5" 1.44MB NEC Floppy Diskette Drive
512K L2 Pipeline Burst Cache
Operating System Used for Evaluation: DOS 7, Windows 95
2in1 PC™ Drivers: Operating System Dependent
Other Software: 2in1 PC™ Configuration Information from the 2in1 PC™ Installation Diskettes, Version 1.21 (2 Disks)

The test suite used during the execution of the independent tests included:

1. Twinbrook Systems, Intel 200Mhz Pentium-MMX – provided by the testing lab.

2. Innotec ID520 IDE Analyzer – provided by Voltaire. This device was used in tests ET03 and ET04 that are defined in the *Evaluation Test Plan for 2in1 PC™, Version 1.21* Plan.

3. Faxconn ISA Slot Extension Card – provided by Voltaire. This device was used in all of the independent tests to provide easy access to the 2in1 PC™ card components.

4. HP 545A Logic Probe – provided by Voltaire. This device was used in conjunction with the *2in1 PC™ Hardware Design* document to verify connections on the 2in1 PC™ card. This device was used in independent evaluator tests as identified in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

5. HP 1660A Logic Analyzer (50/100-MHz State/500-MHz Timing) – provided by the testing lab. This device was used in test ET02 located in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

6. diskedit.exe (Norton) – provided by the vendor to read/write to specific addresses on the hard disk. This application was used in tests ET03 and ET04 located in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

The specific test details for the independent tests performed are presented in Appendix B and C of the *Evaluation Test Plan for 2in1 PC™, Version 1.21*. Other applications installed on the system as part of the installation process (ref. 9.2.3 ADO_IGS.1 Installation, Generation, and Start-Up Procedures) were also used during the independent testing. These applications were:

1. sense.exe – provided by installed files that were loaded onto the PC from installation disk 1. This application enables the administrator to verify that the configuration settings stored on the EEPROM have not been modified. A value is displayed in hexadecimal and reflects the current configuration settings, therefore any changes to the EEPROM's configuration will result in a different value being displayed. This application also displays the card's current working state (i.e. Secure (A), Public (B), or Transition).

2. report.exe – provided by installed files that were loaded onto the PC from installation disk 1. This application generates a report of the hard disk configuration (i.e. defining borders for each disk partition). This application works in conjunction with report.bat.

3. report.bat – provided by installed files that were loaded onto the PC from installation disk 1. This application executes report.exe and redirects the output to the display screen. This batch file was edited during the evaluation and renamed report2.bat so that the output could be redirected to a file for printing. The output of this file was used as a reference for other tests that were executed and is located after test VT02 in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

7.2.2 Test Configuration

The TOE was properly installed and configured in accordance with the steps provided in the *2in1 PC™ Installation Guide*. The configuration settings made during these steps are defined in the following tables:

Partition	Drive %	Total MB	Primary MB	Extended MB	File System	Access to Functional
Functional	3	49	----	----	FAT	----
Secure (A)	60	950	950	0	FAT	Read Only
Public (B)	37	592	592	0	FAT	Read/Write
Transition	----	9	----	----	FAT	No Access
Total: 100% 1600 MB						

Table 7.2.2-1 Partition Configuration

Transition Settings	Advanced Settings	
Power-Up Mode: Menu	Reset Signal	Advanced
	Network Mode	2in1 PC™
	2nd HD (if exists)	A only
	Force Shutdown	No

Table 7.2.2-2 Settings Configuration

Throughout the execution of the independent tests, there were no changes made to the configuration settings identified in the Tables above.

7.2.3 Coverage and Depth Analysis

After the successful verification of the replicated vendor test procedures, independent tests were developed to further evaluate the security functions that were above and beyond the tests selected from the developer test documentation (ref. 9.2.11 ATE_FUN.1 Functional Testing). With the confirmation of developer tests and the independent tests performed by the evaluators, every security function within the TSC has been tested. Details of the independent testing coverage are defined in Table 7.2.3-1 Independent Tests Correspondence to Functional Specifications

Functional Specification	Independent Tests
1) Allow the setting up and configuration of the 2in1 PC™ attributes.	ET01
2) Provide storage for configuration data (including card configuration and MBRs).	
3) In WORK mode, provide a state machine with three distinct states of operation: A, B and T (Transition).	ET02
4) In WORK mode, provide a different MBR for each security state during boot.	ET03
5) In WORK mode, control access to disk partitions based on the current security state and the access security policy.	ET04
6) In WORK mode, control access to networks based on the current security state and the access security policy.	
7) In WORK mode, control the flow of state changes.	ET02
8) Clear the PC's RAM during the Transition state.	Note: This function is not within the TSF.

Table 7.2.3-1 Independent Tests Correspondence to Functional Specifications

Functional Specification	Independent Tests
9) In WORK mode, monitor access to the floppy disk during the Transition state and prevent state switching upon detection thereof.	ET05
10) In WORK mode, control access to external devices such as floppy drives and SCSI disks	ET06
11) Detect the presence of a physical set-up plug in order to switch into Set-up mode and allow configuration.	ET01

Table 7.2.3-1 Independent Tests Correspondence to Functional Specifications (Cont.)

The selection of the independent tests identified in Table 7.2.3-1 was performed after identifying the obvious vulnerabilities the TOE could be subjected to. After reviewing these vulnerabilities, a selection was made to be included as part of the independent tests. The specific details of these vulnerabilities are defined in Section 9.2.14 AVA_VLA.1, Developer Vulnerability Analysis. The analysis and details for each test performed is identified in Section 9.2.10 ATE_COV.1 Evidence of Coverage.

7.2.4 Testing Approach

The method of conducting the independent tests was performed at the IDE interface level, using an IDE analyzer because the TSF has been identified as being only the 2in1 PC™ card. This method was selected to capture all of the IDE bus traffic on both the controller and hard disk side of the bus, thus allowing the ability to verify the card operated according to it's configured security state.

7.2.5 Results of Independent Testing

After the execution of all of the independent tests, verification was made that each of the security functions performed as expected. Finally, with the inclusion of the replicated vendor tests defined in Section 7.1.3, Coverage and Depth Analysis, it was confirmed that all of the security functions within the TSC had been tested and performed as expected. The details of this coverage are identified in Table 7.2.5-1 Overall Test Correspondence to Functional Specification.

Functional Specification	Developer Tests	Independent Tests
1) Allow the setting up and configuration of the 2in1 PC™ attributes.		ET01
2) Provide storage for configuration data (including card configuration and MBRs).	VT01	
3) In WORK mode, provide a state machine with three distinct states of operation: A, B and T (Transition).		ET02

Table 7.2.5-1 Overall Test Correspondence to Functional Specifications

Functional Specification	Developer Tests	Independent Tests
4) In WORK mode, provide a different MBR for each security state during boot.		ET03
5) In WORK mode, control access to disk partitions based on the current security state and the access security policy.	VT05 VT06	ET04
6) In WORK mode, control access to networks based on the current security state and the access security policy.	VT02 VT04	
7) In WORK mode, control the flow of state changes.		ET02
8) Clear the PC's RAM during the Transition state.	Note: This function is not within the TSF.	Note: This function is not within the TSF.
9) In WORK mode, monitor access to the floppy disk during the Transition state and prevent state switching upon detection thereof.	VT07	ET05
10) In WORK mode, control access to external devices such as floppy drives and SCSI disks		ET06
11) Detect the presence of a physical set-up plug in order to switch into Set-up mode and allow configuration.	VT03	ET01

Table 7.2.5-1 Overall Test Correspondence to Functional Specifications (Cont.)

SECTION 8

EVALUATED CONFIGURATION

8 EVALUATED CONFIGURATION

This section describes the evaluated configuration for the TOE. The purpose of an evaluated configuration is to define the hardware and software components that were examined by the evaluation team. Furthermore, based upon the assumptions defined in Section 4, Assumptions and Clarification of Scope, guidance on how to configure and operate the TOE in a secure manner is also identified.

8.1 EVALUATED HARDWARE AND SOFTWARE COMPONENTS

This section identifies the hardware and software components that were examined by the evaluation team (ref. Section 7 Product Testing). The examined hardware and software components are identified for both the vendor replicated tests and the independent evaluator tests performed. A rationale is also provided to explain the overall scope of the components selected.

8.1.1 Evaluated Hardware Components

The hardware component examined by the evaluators was the 2in1 PC™ ISA slot PC card. Table 8.1.1-1 Evaluated 2in1 PC™ Card List, identifies the evaluated components on the 2in1 PC™ card, provides a description of each element's security function and provides a rationale as to why the component was selected. The actions enforced by each component were verified by the evaluators, Section 7 Product Testing provides further details of this verification.

Card Element	Description	Evaluation Rationale
1 x Printed Circuit Card (PCB)	The fiberglass printed circuit card used to mount the electronic components.	This is the 2in1 PC™ card itself. The card logic was verified in all of the evaluator tests performed to ensure the correct operation of all of the individual card components.
1 x EEPROM chip	Used to store the 2in1 PC™ card configuration data.	The EEPROM was evaluated to ensure that when the administrator sets configuration parameters, they are actually being written to and read from the EEPROM. Furthermore, once these parameters had been defined, other tests were performed to verify that the 2in1 PC™ card enforced the defined security policy. The EEPROM has a hardware address assigned to it that can be referenced from the IDE bus, however the Altera chip blocks this write access if the machine is running in work mode. In order to write to the EEPROM, the machine must be in set-up mode, activating the write enable jumper pins where the set-up plug is installed.
1 x PROM chip	Used to store the code that operates the 2in1 PC™ card.	The PROM chip only stores the hard coded instruction set for the correct operation of the Altera chip. If the instruction set was not correct or fully adequate, then the card would not operate according to its defined security functions. Since the enforcement of the identified security functions was verified, this element was determined to be functioning properly.
6 x Electro-mechanical relays	Used to sever network connections to the 2in1 PC™ card and control the ability to enable/disable peripheral device control jumper connections.	The 6 electro-mechanical relays on the 2in1 PC™ card were evaluated to ensure their correct operation. Two relays control the Secure (A) network connection, two relays control the Public (B) network connection, one relay controls the peripheral device jumper connection for the Secure (A) machine state and the last relay controls the peripheral device jumper connection for the Public (B) machine state. The correct operation of all of the electromechanical relays was verified for every machine state (i.e. Secure (A), Public (B) and Transition). Furthermore, the relays that control access to the Secure (A) and Public (B) networks were verified not only at the network connection interface level, but also by physically connecting two networks to the card to verify the ability to transfer data to and from each network.
1 x Altera chip	Used to perform processing and logical operations on the card. The instruction set for this components operation is read from the PROM element.	The evaluators did not directly evaluate this component because it is the logic core of the 2in1 PC™ card. All of the card components are controlled by the data stored in the Altera chip and since the enforcement of the security functions was verified, this component was determined to be functioning properly. Furthermore, the Altera chip does not have a machine address assigned to it, therefore it cannot be referenced by the IDE bus.

Table 8.1.1-1 Evaluated 2in1 PC™ Card List

Card Element	Description	Evaluation Rationale
2 x IDE connectors	Used to route the IDE cables through the 2in1 PC™ card.	The evaluators examined the IDE interfaces as described in Section 7, Product Testing. These interfaces were thoroughly examined to verify that the 2in1 PC™ card enforced its security functions as expected. This examination was performed in both the replications of vendor performed tests and also the independent tests performed. In the replications of vendor performed tests, verification of the enforcement of the security functions was verified at the operating system level. In the independent tests, verification of the enforcement of the security functions was verified at the IDE interface level on both the controller and hard disk side of the IDE connections to the 2in1 PC™ card.
4 x Network connectors	Used to route the network/telephone cables through the 2in1 PC™ card.	The evaluators examined the four network connections on the 2in1 PC™ card. All four connections are independently controlled by an electromechanical relay. Two of the network connections are associated with the Secure (A) network, and the other two network connections are associated with the Public (B) network. The purpose of having two network connections for each network is to have a network input into the card and an output to the NIC card on the host PC. These network connections were tested to verify the ability to connect to each network and transfer data to and from each network based upon the machine states, Secure (A) and Public (B).
6 x Floppy disconnection jumpers	Used to provide the ability to sever the ability to access a peripheral device.	The evaluators verified the correct operation of the floppy disconnection jumpers as defined in Section 9.1.2.1 Partitioning Access Policy.

Table 8.1.1-1 Evaluated 2in1 PC™ Card List (Cont.)

The correct operation of other hardware elements, all of which are complements to the 2in1 PC™ ISA slot PC card, was also verified. These elements are identified in Table 8.1.1-2 Evaluated Elements Complementing the 2in1 PC™ Card.

Card Element	Description	Evaluation Rationale
1 x Internal Set-up plug	Used to enable the write function to alter the EEPROM configuration settings and allows for full unmonitored IDE access to the hard disk(s).	This component was used during the installation procedure to configure the 2in1 PC™ card on the host PC. It was also used to reconfigure the 2in1 PC™ card to verify the expected results from the replicated vendor tests (ref. Section7, Product Testing).
1 x Internal Enabler Plug (Note: This is an optional device, however its functionality was verified).	Used in conjunction with the external set-up plug to enable the write function to alter the EEPROM configuration settings and to allow full unmonitored IDE access to the hard disk(s). With the internal enabler plug inserted on the 2in1 PC™ card, the external set-up plug can be used in lieu of the internal set-up plug.	This component, used in conjunction with the external set-up plug, was examined to verify that the functionality provided is the same as with the internal set-up plug.
1 x External Set-up Plug (Note: This is an optional device, however its functionality was verified).	Used in conjunction with the internal enabler plug to enable the write function to alter the EEPROM configuration settings and to allow for full unmonitored IDE access to the hard disk(s). With the internal enabler plug inserted on the 2in1 PC™ card, the external set-up plug can be used in lieu of the internal set-up plug.	This component, used in conjunction with the internal enabler plug, was examined to verify that the functionality provided is the same as with the internal set-up plug.
1 x Floppy Disk Control Cable (Note: This is an optional device, however its functionality was verified).	This cable replaces the floppy drive cable on the host PC. This cable is installed on the host PC in the same manner as the old cable, however it has a spliced control signal wire that is connected to the peripheral device control jumpers on the 2in1 PC™ card. These jumpers are controlled by two electro-mechanical relays. One relay controls the jumpers for the Secure (A) machine state and the other relay controls the jumpers for the Public (B) machine state.	This component was examined to verify the ability to enable/disable access to the floppy diskette drive. This was performed by connecting the floppy disk control cable onto the host PC and then connecting the severed control signal wire to the floppy disconnection jumpers.

Table 8.1.1-2 Evaluated Elements Complementing the 2in1 PC™ Card

8.1.2 Evaluated Software Components

The software components examined by the evaluators were the two installation diskettes provided as part of the TOE for the installation and configuration of the card on the host PC. The extent of this examination was limited to only the verification of a secure configuration of the TOE as defined in Section 9.2.3 ADO_IGS.1 Installation, Generation, and Start-up Procedures. The individual software elements stored on each disk (ref. 9.2.1.2.3 Configuration List) were not independently evaluated in Section 7 Product Testing, because they were defined to be outside the scope of the TSF. The area

where these elements were evaluated was in Section 9.2.3 ADO_IGS.1 - Installation, Generation, and Start-Up Procedures. The software elements that were copied from the installation diskettes to the hard disk during the installation and configuration of the 2in1 PC™ card were also beyond the scope of the TSF; however, some of these elements were used in conducting the tests identified in Section 7 Product Testing. The specific software elements that were used during the replication of vendor performed tests are identified in Section 7.1.1 Details of the Test Suite. The specific software elements that were used during the execution of the independent evaluator tests are identified in Section 7.2.1 Details of the Test Suite.

8.2 CONFIGURATION AND USAGE NOTES

The 2in1 PC™ card can be configured in accordance with specific organisational security policies. This section identifies which of the configuration settings were examined as part of the TOE evaluation and also identifies other configurable settings that the TOE supports, but were not included as part of the evaluation. Section 8.2.3, Incorrect Installation of the Evaluated Configuration, addresses the incorrect configuration settings that could be made when installing the TOE. The input of incorrect configuration settings has been mitigated based upon the assumptions identified in Section 4, Assumptions and Clarification of Scope.

8.2.1 Required and Allowed Configuration Settings

2in1 PC™ requires specific configuration settings for the following:

1. During installation, the percent, or size in MB, of hard disk space allocated for the Secure (A), and Public (B) disk partitions must be defined. The percent or size in MB for the Functional disk partition is not required since it is a disk partition that can be created depending upon the TOE's configured environment.
   Note: This partition was created for the EAL-2 evaluation of the TOE.

A number of TOE configuration settings are available to the administrator and are implemented in accordance with the organisational security policy the TOE is to enforce. These configuration settings are defined in Table 8.2.1-1 Allowed Configuration Settings.

Setting	Allowable Values	Default Value	Discussion
Name	Any	'Secure' for the A partition and 'Public' for the B partition	Disk partitions A and B can be assigned unique names rather than accepting the default value.
Functional	Numeric Inputs	None	The administrator must define the size in percentage of disk space or the size in MB if this disk partition is created.

Table 8.2.1-1 Allowed Configuration Settings

Setting	Allowable Values	Default Value	Discussion
Access to Functional, Secure (A)	Read/Write, Read Only, or No Access	Read Only	Read/Write-Sets the Secure (A) machine to have the ability to write data to and read data from the Functional disk partition. Read Only-Sets the Secure (A) machine to only have the ability to read data from the Functional disk partition. No Access-Sets the Secure (A) machine to have no ability to access the data stored in the Functional disk partition.
Access to Functional, Public (B)	Read/Write, Read Only, or No Access	Read/Write	Read/Write-Sets the Public (B) machine to have the ability to write data to and read data from the Functional disk partition. Read Only-Sets the Public (B) machine to only have the ability to read data from the Functional disk partition. No Access-Sets the Public (B) machine to have no ability to access the data stored in the Functional disk partition.
Access to Functional, Transition	Read/Write, Read Only, or No Access	No Access	Read/Write-Sets the Transition machine to have the ability to write data to and read data from the Functional disk partition. Read Only-Sets the Transition machine to only have the ability to read data from the Functional disk partition. No Access-Sets the Transition machine to have no ability to access the data stored in the Functional disk partition.
Power-Up Mode	A, B, or Menu	A	A-Sets the PC during first power on to boot into Transition and then reboot into the Secure (A) machine state. B-Sets the PC during first power on to boot into Transition and then reboot into the Public (B) machine state. Transition-Sets the PC during first power on to boot into Transition and then displays a menu for the user to select whether to reboot the PC into the Secure (A) or Public (B) machine state.

Table 8.2.1-1 Allowed Configuration Settings (Cont.)

Setting	Allowable Values	Default Value	Discussion
Reset Signal	Advanced or AT Compatible	Advanced	Advanced-Set to match the reset signal method used on the host PC (IDE Reset). AT Compatible-Set to match the reset signal method used on the host PC (ISA64 Reset). Note: If this setting is not properly configured, the TOE will ignore the reset signal that has been sent.
Network Mode	2in1 PC, or 2in1 Net	2in1 PC	2in1 PC-Set if to allow the user on the host PC to control the machine states. 2in1 Net-Set if the optional (not evaluated) 2in1 Net device will be used to control the machine states of a group of host PC's that have the 2in1 PC™ card installed on them.
2nd HD (if exists)	A Only, B Only.	A	A Only-Set to allow only the Secure (A) machine state the ability to access the secondary slave hard disk. B Only-Set to allow only the Public (B) machine state the ability to access the secondary slave hard disk.
Force Shutdown	Yes, or No	No	Yes-Sets the Host PC to fully power down when switching between machine states Secure (A) and Public (B). No-Sets the host PC to perform a soft-boot when switching between machine states Secure (A) and Public (B).

Table 8.2.1-1 Allowed Configuration Settings (Cont.)

The configuration settings defined in Table 8.2.1-1 Allowed Configuration Settings only apply to the configuration of the 2in1 PC™ card during the installation of the TOE. After the installation has been completed, the only parameters that cannot be modified without reinstalling the TOE on the host system are the partition sizes on the master disk for the Secure (A), Public (B), Transition and Functional disk partition. These configuration settings only apply to the 2in1 PC™ card itself.

The operating environment must address other devices or connections that are to be controlled by the 2in1 PC™ card. This includes:

1. Proper connection of the network wires to the 2in1 PC™ card. If the network connections are not connected to the 2in1 PC™ card as defined in the *2in1 PC Installation Guide*, then the result will be no network connectivity.

2. Proper connection of the peripheral device control cables to the jumper connections on the 2in1 PC™ card (these cables are optional and supplied by

Voltaire). If the cable connections are not properly inserted onto the correct jumpers on the 2in1 PC™ card as defined in the *2in1 PC Installation Guide*, then the controlled device on the host PC will be disabled/enabled for the wrong machine states.

3. Proper connection of the IDE cables from the motherboard to the 2in1 PC™ card and from the 2in1 PC™ card to the hard disk(s). If the IDE cables are not properly installed on the 2in1 PC™ card, then the host PC will not function.

8.2.2 Evaluated Configuration Settings

The following TOE configuration settings were not tested in Section 7 Product Testing and Section 9.2.3 ADO_IGS.1 – Installation, Generation, and Start-Up Procedures (ref Table 8.2.1-1 Allowed Configuration Settings):

1. Name- Names were not reassigned to the 'Secure' (A) or 'Public' (B) disk partitions.

2. Functional- The creation of the Functional disk partition was not omitted during the installation process (ref. 9.2.3 ADO_IGS.1 Installation, Generation, and Start-up Procedures).

3. Access to Functional, Secure (A)- 'Read/Write' access to the Functional disk partition while running in the Secure (A) machine state was not tested.

4. Access to Functional, Transition- 'Read/Write' and 'Read Only' access to the Functional disk partition while running in the Transition machine state was not tested.

5. Power-Up Mode- During first power on of the PC, Power-Up Mode 'B' was not tested.

6. Reset Signal- The 'AT Compatible' reset signal was not tested.

7. 2nd HD (if exists)- The configuration of the TOE did not include the existence of a second hard disk, therefore the selections 'A Only' and 'B Only' were not tested.

8. Force Shutdown- The selection 'Yes' was not tested.

8.2.3 Non-Evaluated Configuration Settings

The following TOE configuration settings were not evaluated:

1) Network Mode- The '2in1 Net' selection was not evaluated.

8.2.4 Incorrect Installation of the Evaluated Configuration

The administrator must select the appropriate TOE configuration settings in order to enforce their organisational security policy. The specific TOE configuration settings that, if not properly configured, will result in a violation of any organisational security policy include:

1. Defining incorrect values for the Secure (A) machine's ability to pass data to and/or from the Functional disk partition.

2. Defining incorrect values for the Public (B) machine's ability to pass data to and/or from the Functional disk partition.

The operational environment must address the incorrect installation of other devices or connections that are to be controlled by the 2in1 PC™ card. These connections include:

1. Network Connections: If the network connections are not connected to the 2in1 PC™ card as defined in the *2in1 PC Installation Guide*, then the result will be no network connectivity.

2. Peripheral device control cables: If the cable connections are not properly inserted onto the correct jumpers on the 2in1 PC™ card as defined in the *2in1 PC Installation Guide*, then the controlled device on the host PC will be disabled/enabled for the wrong machine states.

3. IDE Cables: If the IDE cables are not properly installed on the 2in1 PC™ card as defined in the *2in1 PC Installation Guide*, then the host PC will not function.

8.3 TARGET ENVIRONMENT

The TOE is a COTS system that is intended to be installed on a PC that is located in a controlled environment. The operational environment must provide basic physical security. Other requirements for the target environment include:

1. Users of the TOE must recognise the need for a secure IT environment.

2. Administrators must be adequately trained to competently administer the security features of the TOE during set-up and reconfiguration.

3. Users of the TOE system must be trusted not to modify the hardware configuration.

8.4 RESIDUAL VULNERABILITIES

The TOE vulnerabilities are identified in Section 9.2.14, Developer Vulnerability Analysis. Along with the identification of residual vulnerabilities, this section also

defines how each vulnerability is mitigated by either environmental assumptions or policies, or how each vulnerability is mitigated based upon the logic used on the 2in1 PC™ card.

SECTION 9

RESULTS OF EVALUATION

9 RESULTS OF EVALUATION

This section provides descriptions of how the TOE meets each of the Security Functional Requirements and Assurance Requirements of the *2in1 PC™ Security Target Report*.

9.1 SECURITY FUNCTIONAL REQUIREMENTS

Table 9.1-1 lists the security functional requirements from the *2in1 PC™ Security Target Report*.

Security Functional Requirement	Description
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Security Attribute Based Access Control
FDP_ITC.1	Import of User Data Without Security Attributes
FIA_UID.2	User Identification Before Any Action
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_SMR.1	Security Roles
FMT_SMR.3	Assuming Roles
FPT_FLS.1	Failure with Preservation of Secure State
FPT_RCV.4	Function Recovery
FPT_RVM.1	Non-Bypassability of the TSP
FPT_SEP.3	Complete Reference Monitor

Table 9.1-1 Security Functional Requirements

9.1.1 FDP_ACC.1 Subset Access Control

Subset access control requires that each identified access control SFP be in place for a subset of the possible operations, on a subset of the objects in the TOE.

9.1.1.1 FDP_ACC.1.1 – Partitioning Access Policy

The TSF shall enforce the [*Partitioning Access Policy*] on [*the user's current machine state: "A", "B" and "T"; disk partitions: Transition, Functional, "A", and "B"; network connections: "A" and "B"; and other devices controlled by the Partitioning Access Policy*].

This element was satisfied by the TOE. In the Partitioning Access Policy, the only subjects are users and processes running on behalf of users. The objects are disk partitions, network connections, and other devices controlled by the TSF. The

Partitioning Access Policy described in Section 3.1 is enforced by a combination of security functions specified in the *2in1 PC™ Functional Specification*. A state machine is maintained that provides three user states: A, B, and Transition. While in any given state, the IDE bus monitor permits only IDE hard disk addresses that are within the boundaries of disk partitions to which the user is allowed access, according to the Partitioning Access Policy. The IDE bus monitor also permits only IDE hard disk operations (e.g., read/write) that are allowed for the partition, according to the Partitioning Access Policy. The TSF sets and resets relays that control network access in accordance with the Partitioning Access Policy. Other optional interfaces may be controlled by the TSF. The administrator may configure the optional interfaces with special ribbon cables supplied by Voltaire. These ribbon cables have a jumper that connects to pins on the 2in1 PC™ card to enable or disable their use in specific user states. Devices so connected are controlled by the TSF.

9.1.1.2 FDP_ACC.1.1 – Administrator Access Policy

The TSF shall enforce the [*Administrator Access Policy*] on [*the user roles: administrator and user; for write access to the EEPROM*].

This element was satisfied by the TOE. The TOE implements a role based access policy providing the administrator the ability to set-up and modify some of the attributes and parameters used by the Partitioning Access Policy. The Administrator Access Policy is described in Section 3.2. Write access to the EEPROM is physically prohibited while in work mode. When the administrator has been identified, by detection of the set-up plug being inserted on the 2in1 PC™ card, they are put into set-up mode and write access to the EEPROM is physically enabled (the PC must be powered off to insert the set-up plug, then powered back on to enter set-up mode).

9.1.1.3 Dependencies

9.1.1.3.1 FDP_ACF.1 – Security Attribute Based Access Control

The TSF meets the requirement for this condition by providing security attribute based access control. (See Section 9.1.2.)

9.1.2 FDP_ACF.1 Security Attribute Based Access Control

This element was satisfied by the TSF. The TSF has two access control policies that are enforced by the TSF. The first is the Partitioning Access Policy, which controls access between users and the objects that they normally access (i.e., disk partitions, network connections, and other interfaces) while in work mode. The second policy is the Administrator Access Policy, which controls write access to the EEPROM. The EEPROM is where many of the security parameters and attributes that are used to control the Partitioning Access Policy are stored.

9.1.2.1 Partitioning Access Policy

The following requirements apply to the Partitioning Access Policy.

9.1.2.1.1 FDP_ACF.1.1 – Partitioning Access Policy

The TSF shall enforce the [*Partitioning Access Policy*] to objects based on [*the user's currently active machine state, disk partition address, network connection type, and pin connection for external devices controlled by the TOE*].

This element was satisfied by the TSF. The allowable attributes are as follows:

1.	Machine state	A, B, or T
2.	Disk partition addresses	Address ranges for A, B, T, or F
3.	Network connection	A or B
4.	External Devices (Floppy or SCSI)	A, B, !A, or !B.

(Note: !A means available in all states except A. !B means available in all states except B. Either of these provides for the device to be available during the Transition state.)

9.1.2.1.2 FDP_ACF.1.2 – Partitioning Access Policy

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*users in a given state have access only to disk partitions, network connections, and other TOE controlled interfaces authorised for their current state*].

This element was satisfied by the TSF. In state A, users have access only to disk partition A, and possibly F (depending on the security policy settings selected by the administrator), network connection A, and possibly other external devices (e.g., floppy disk and SCSI interfaces), depending on the security policy settings and cables connecting the devices selected by the administrator. In state B, users have access only to disk partition B, and possibly F (depending on the security policy settings selected by the administrator), network connection B, and possibly other external devices (depending on the security policy settings selected by the administrator and cables connecting the devices). In state T, users have read only access to disk partition T, and possibly access to F (depending on the security policy settings selected by the administrator), no network connections, and access to other external devices (e.g., floppy disk and SCSI interfaces) connected on !A (Not A) and !B (Not B). The external devices (e.g., floppy disk and SCSI interfaces), if configured as part of the TSC, can be available in A, B, !A (Not A), or !B (Not B) (see Section 9.1.2.1.1). The existence of, and access policy for, disk partition F is selectable by the administrator. If partition F exists, the default settings are read access from state A and read/write access from state B. An administrator selectable setting of read only from state A and read/write from state B would allow the passing of information from state B to state A, but not from state A to state B.

The TSF enforces its Partitioning Access Policy, as shown in Table 9.1.2.1.2-1. This policy is more fully discussed in Section 3, Security Policy.

	State A	State B	State T
Disk Partitions			
A	R/W	No access	No access
B	No access	R/W	No access
T	No access	No access	R*
F	R*	R/W*	No access*
Network Connections			
A	Connected	Not Connected	Not Connected
B	Not Connected	Connected	Not Connected
Other Interface			
External devices	A & !B**	B & !A **	!A, & !B
* Administrator selectable. ** Administrator configurable as A, B, !A (Not A), or !B (Not B)			

Table 9.1.2.1.2-1 Partitioning Access Policy Rules

9.1.2.1.3 FDP_ACF.1.3 – Partitioning Access Policy

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*when the administrator has entered set-up mode, unconditional access is granted to the entire hard disk and to other controlled devices connected to the !A (Not A) and !B (Not B) jumper pins*].

This element was satisfied by the TSF. The administrator role, and set-up mode, are identified by the set-up plug being inserted onto the 2in1 PC™ card. In this role, access is allowed to all disk partitions. Typically, the administrator accesses only partitions associated with the partition he is booted from, but that access is not monitored or controlled by the TSF. Relays are set to allow access to any devices connected to the !A (Not A) and !B (Not B) jumper pins.

9.1.2.1.4 FDP_ACF.1.4 – Partitioning Access Policy

The TSF shall explicitly deny access of subjects to objects based on the [*administrator having entered set-up mode, then no network connections are allowed and other controlled device access is not allowed to devices connected to the A and B jumper pins*].

This element was satisfied by the TSF. Entering set-up mode causes relays to be opened, disconnecting both A and B networks and to any devices connected to the A and B jumper pins.

9.1.2.2 Administrator Access Policy

The Administrator Access Policy provides the rules for write access to the EEPROM by the user roles. The following requirements apply to the Administrator Access Policy.

9.1.2.2.1 FDP_ACF.1.1 – Administrator Access Policy

The TSF shall enforce the [*Administrator Access Policy*] to objects based on [*the user role: user or administrator, for write access to the EEPROM*].

This element was satisfied by the TSF. For the Administrator Access Policy, the attributes are the user roles: user or administrator.

9.1.2.2.2 FDP_ACF.1.2 – Administrator Access Policy

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*administrators are allowed to write to the EEPROM; users are denied write access to the EEPROM*].

This element was satisfied by the TSF. Being in set-up mode identifies the administrator role. When the set-up plug is in place, and the system has been rebooted in set-up mode, write access is physically enabled to the EEPROM. Typically, the administrator uses utilities provided on the 2in1 PC™ installation disks to manage EEPROM information. These utilities are not a part of the TSF and have not been included in Section 7 Product Testing, because they were defined to be outside the scope of the TSF. The area where these elements were evaluated was in Section 9.2.3 ADO_IGS.1 - Installation, Generation, and Start-Up Procedures.

9.1.2.2.3 FDP_ACF.1.3 – Administrator Access Policy

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

This element was satisfied by the TSF. There are no other rules that apply to write access to the EEPROM.

9.1.2.2.4 FDP_ACF.1.4 – Administrator Access Policy

The TSF shall explicitly deny access of subjects to objects based on the [*none*].

This element was satisfied by the TSF. There are no other rules that apply to write access to the EEPROM.

9.1.2.3 Dependencies

9.1.2.3.1 FDP_ACC.1 Subset Access Control

The TSF meets the requirement for this condition by providing subset access control. (See Section 9.1.1.)

9.1.2.3.2 FMT_MSA.3 Static Attribute Initialisation

The TSF meets the requirement for this condition by providing static attribute Initialisation. (See Section 9.1.6.)

9.1.3 FDP_ITC.1 Import of User Data Without Security Attributes

Import of user data without security attributes requires that the security attributes correctly represent the user data and are supplied separately from the object.

9.1.3.1 FDP_ITC.1.1

The TSF shall enforce the [*Partitioning Access Policy*] when importing user data, controlled under the SFP, from outside of the TSC.

This element was satisfied by the TSF. In work mode, data may be imported only from devices that are authorised for the particular machine state, and will be stored in a disk partition appropriate for that machine state. For example: In machine state B, data may only be imported from network B or external devices (e.g., floppy drive, SCSI disk) that have been properly set up for state B by the administrator. That data may be stored in disk partition B or, depending on the administrator provided security policy selections, in disk partition F.

9.1.3.2 FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

This element was satisfied by the TSF. External security attributes, such as security labels, are not recognised by TSF. The only security attributes recognised by the TSF are the assignments associated with machine state, disk partition, or other devices controlled by the TSF (i.e., A, B, T, or F).

9.1.3.3 FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [*user data imported under the control of the TSF is assigned the security attribute of the current machine state (i.e., A or B)*].

This element was satisfied by the TSF. In work mode, all data imported under control of the TSF is assigned the security attribute of the current machine state.

9.1.3.4 Dependencies

9.1.3.4.1 FDP_ACC.1 Subset Access Control

The TSF meets the requirement for this condition by providing subset access control. (See Section 9.1.1.)

9.1.3.4.2 FMT_MSA.3 Static Attribute Initialisation

The TSF meets the requirement for this condition by providing static attribute Initialisation. (See Section 9.1.6.)

9.1.4 FIA_UID.2 User Identification Before Any Action

User identification before any action requires that users identify themselves before any action will be allowed by the TSF.

9.1.4.1 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.

This element was satisfied by the TSF. The requirement for the identification before any action is derived from the FMT_SMR.1, Security Roles, security functional requirement. The TOE makes no claim of individual identification of users. The TSF identifies only user roles (i.e., user and administrator), not users as individuals. By definition, any individual operating in work mode is a user. Also by definition, any individual operating in set-up mode is an administrator. A user may become an administrator, and enter set-up mode, by powering off the PC, opening the PC case, inserting the set-up plug on the 2in1 PC™ card, and turning the machine back on. Alternately, if the optional, internal enabler plug is already inserted on the 2in1 PC™ card, the user need only turn the PC off, insert the external set-up jack, and turn the power back on. To become a user again, and return to work mode, the administrator reverses the process, removing the set-up plug and restarting the machine in work mode. The TSF checks for the presence or absence of the set-up plug (in one of its two forms), thus identifying the user role, before performing any functions on behalf of the user.

9.1.4.2 Dependencies

This requirement has no dependencies.

9.1.5 FMT_MSA.1 Management of Security Attributes

Management of security attributes allows authorised users (roles) to manage the specified security attributes.

9.1.5.1 FMT_MSA.1.1

The TSF shall enforce the [*Administrator Access Policy*] to restrict the ability to [*change_ default and modify*] the security attributes [*partition boundary addresses, MBRs, access rights, switching policies, and internal set-up information*] to [*the administrator that has entered set-up mode*].

This element was satisfied by the TSF. In work mode, no write access is allowed to the EEPROM, where most of the security attribute information, including partition boundary addresses, access rights, and switching policies, is stored. When in set-up mode, the administrator may modify these attributes.

Table 9.1.5.1-1 shows the information stored on the EEPROM that is modifiable by the administrator or set by the installation software.

Attribute	Allowable Values	Default	Set By*	Discussion
Power On Mode	A, B, Ta, Tb**	Ta**	Adm	The administrator may select the initial user state. The installation software allows only Ta or Tb.**
Access to Functional disk partition in T	N – No access R – Read Only R/W – Read & write	N	Adm	Access policy for the Functional disk partition while in T.
Access to Functional disk partition in B	N – No access R – Read Only R/W – Read & write	R/W	Adm	Access policy for the Functional disk partition while in B.
Access to Functional disk partition in A	N – No access R – Read Only R/W – Read & write	R	Adm	Access policy for the Functional disk partition while in A.
Slave disk usage	A or B	A	Adm	The second disk, if present, may be accessible in either state A or B, not both.
Reset signal	IDE reset ISA 64	ISA 64	Inst	There are two ways to detect a reset on a PC – by detecting the actual associated electrical activity on the ISA or IDE bus, or by monitoring the CPU reset command itself. As certain PCs don't display the aforementioned bus electrical activity during reset, the only way to verify a reset on them is to monitor the CPU reset command.

Table 9.1.5.1-1 Administrator Dependent Attributes and Parameters

Attribute	Allowable Values	Default	Set By*	Discussion
Forced power off	E – Enabled D – Disabled	D	Adm	2in1 PC™ installation disk software (not a part of the TSF) provides for the clearing of RAM during state transition. Some local policies may also require the PC to cycle through power off to ensure that all volatile memory is cleared.
2in1 PC™ /NET mode	2in1 PC™ 2in1 NET™	2in1 PC™	Adm	There are currently two different 2in1 products available from Voltaire, 2in1 PC™ and 2in1 NET. These products share a great deal of their design and implementation. This bit allows the identification of the product. NOTE: The evaluated version is only 2in1 PC™ .
Functional partition start address	Logical and physical disk addresses	N/A	Inst	This is the start address of the Functional disk partition given in both LBA and physical formats. It is the last partition on the disk and the end of the disk is the end of the Functional partition.
Disk characteristics	Heads/Cylinder Sectors/Head	N/A	Inst	Default geography of the disk – sectors/head and heads/cylinder.
Disk partition start and end addresses for A, B, and T	Logical and physical disk addresses	N/A	Inst	These are the start and end addresses for the A, B, and T disk partitions given in both LBA and physical formats.
Installation signature	"2in1 PC™ "	N/A	Inst	This is used to verify that the EEPROM is not blank.
Installation version	Installation software version number.	N/A	Inst	Used for upgrades to the installation software.
Installation unique number	Globally Unique Identifier (GUID)	N/A	Inst	A value assigned to bind the disk and the 2in1 PC™ card together.
Data CRC32	CRC of the EEPROM.	N/A	Inst	Used to verify the integrity of the EEPROM.
Install state	C – Completed I – In progress	C	Inst	There is a reboot required during the set-up process. This flag indicates the status of the set-up (i.e., before or after the reboot).
Stash BIOS cylinder	Physical cylinder address	N/A	Inst	Location of the backup of the EEPROM. This is located between partitions and is not accessible. ***

Table 9.1.5.1-1 Administrator Dependent Attributes and Parameters (Cont.)

Attribute	Allowable Values	Default	Set By*	Discussion
MBRs for A, B, and T	Boot loader and system tables	N/A	Inst	These are the actual MBR to be used for booting from the A, B, and T disk partitions.

* Adm means specifically set by the administrator. Inst means the value is determined by the set-up software, depending on administrator selected parameters.
** Ta and Tb are the Transition state where the next state has been identified as A or B, respectively.
*** The stash is a mirror image of the EEPROM that is saved to facilitate recovery from a damaged or malfunctioning 2in1 PC card. It has no security function. Without this information, much of the data on the hard disk would be difficult to recover and my be completely lost, in the event of a failure. The stash resides in a gap between partitions, and therefore is never accessible in WORK mode (when you're in partition A it is above your highest accessible sector, when you're in T and B, it's below your lowest accessible sector). The "Stash BIOS cylinder" item in the EEPROM is the address of the cylinder in which the stash is located. It's used to assist in locating the stash when it needs to be updated (and not having to sequentially search the entire disk for it - a lengthy process).

Table 9.1.5.1-1 Administrator Dependent Attributes and Parameters (Cont.)

9.1.5.2 Dependencies

9.1.5.2.1 FDP_ACC.1 Subset Access Control

The TSF meets the requirement for this condition by providing subset access control. (See Section 9.1.1.)

9.1.5.2.2 FMT_SMR.1 Security Roles

The TSF meets the requirement for this condition by providing security roles. (See Section 9.1.7.)

9.1.6 FMT_MSA.3 Static Attribute Initialisation

Static attribute Initialisation ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.

9.1.6.1 FMT_MSA.3.1

The TSF provides two different types of default access policies for the Functional partition, if one exists. For the Transition state, the defaults are restrictive. For states A and B, the default is for a “read down” access policy, where state B may read and write to the Functional partition and state A may only read from the Functional partition. Table 9.1.6.1-1 shows the access rule attributes that have selectable values, the possible selections, and the default selection.

Attribute	Allowable Selections	Default Selection
First power on state	States A, B, T (where the next state is B), or T (where the next state is A). (Note – Installation software allows only Ta or Tb.)	State T (where the next state is A)
Access to the F disk partition from state T	No access, read only access, or read/write access	No access
Access to the T partition from state T	Read only or read/write	Read only
Access to the F partition from state B	No access, read only access, or read/write access	R/W
Access to the F partition from state A	No access, read only access, or read/write access	R
Slave disk state	State A or B	State A

Table 9.1.6.1-1 Administrator Selectable Partitioning Access Policy Security Attributes

9.1.6.1.1 FMT_MSA.3.1 – Transition state

The TSF shall enforce the [*Partitioning Access Policy*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

This element was satisfied by the TSF. The SFP is enforced in the Transition state. Administrator selectable access rules for the Transition state default to the most restrictive case, as shown in the access security policy (see Section 3). From the Transition state, the T partition is read only and no other partitions are accessible.

9.1.6.1.2 FMT_MSA.3.1 – States A and B

The TSF shall enforce the [*Partitioning Access Policy*] to provide [*read down*] default values for security attributes that are used to enforce the SFP.

This element was satisfied by the TSF. The SFP is enforced in the Transition state. Administrator selectable access rules for states A and B default to a “read down” case, as shown in the access security policy (see Section 3). Where state A is assumed to be a more restrictive state than state B, state B may read and write to the Functional partition and state A may only read from the Functional partition. This will allow the flow of information from state B to state A, but not from A to B.

9.1.6.2 FMT_MSA.3.2

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

This element was satisfied by the TSF. In set-up mode, write access is logically and physically enabled to the EEPROM, and the administrator has the capability to specify alternative initial values to override default values. Typically, the administrator uses utilities provided on the 2in1 PC™ installation disks to set initial values and/or override default values in the EEPROM. These utilities are not a part of the TSF and are not

included in Section 7 Product Testing, because they were defined to be outside the scope of the TSF. The area where these elements were evaluated was in Section 9.2.3 ADO_IGS.1 - Installation, Generation, and Start-Up Procedures.

9.1.6.3 Dependencies

9.1.6.3.1 FMT_MSA.1 Management of Security Attributes

The TSF meets the requirement for this condition by management of security attributes. (See Section 9.1.5.)

9.1.6.3.2 FMT_SMR.1 Security Roles

The TSF meets the requirement for this condition by providing security roles. (See Section 9.1.7.)

9.1.7 FMT_SMR.1 Security Roles

FMT_SMR.1 Security roles specifies the roles with respect to security that the TSF recognises.

9.1.7.1 FMT_SMR.1.1

The TSF shall maintain the roles [a*dministrator and user*].

This element was satisfied by the TSF. There are two roles recognised by the 2in1 PC™ TSF, the user role and the administrator role. There are specific actions that may only occur in one or the other of the recognised roles.

9.1.7.2 FMT_SMR.1.2

The TSF shall be able to associate users with roles.

This element was satisfied by the TSF. All users operating the TOE in work mode are in the user role. Anyone operating the TOE in set-up mode is considered to be in the administrator role.

9.1.7.3 Dependencies

9.1.7.3.1 FIA_UID.1 Timing of Identification

The TSF meets the requirement for this condition by providing user identification before any action (See Section 9.1.4.). Administrators are required to be in set-up mode before they can perform any administrator functions. Being in work mode (i.e., the set-up plug not being inserted on the 2in1 PC™ card) identifies the user role.

9.1.8 FMT_SMR.3 Assuming Roles

Assuming roles requires that an explicit request be given to the TSF to assume a role.

9.1.8.1 FMT_SMR.3.1

The TSF shall require an explicit request to assume the following roles: [*administrator*].

This element was satisfied by the TSF. Installation of the set-up plug in the TSF, and power up in set-up mode, is the explicit action necessary to assume the administrator role. Anyone operating the TOE without being in set-up mode is considered to be a user.

A user may become an administrator by powering off the PC, opening the PC case, inserting the set-up plug on the 2in1 PC™ card, and turning the machine back on. Alternately, if the optional, internal enabler plug is already inserted on the 2in1 PC™ card, the user need only turn the PC off, insert the external set-up jack, and turn the power back on. To become a user again, the administrator reverses the process, removing the set-up plug and restarting the machine in work mode. The TSF checks for the presence of the set-up plug (in one of its two forms), thus identifying the user role, before performing any functions on behalf of the user.

9.1.8.2 Dependencies

9.1.8.2.1 FMT_SMR.1 Security Roles

The TOE meets the requirement for this condition by providing security roles (See Section 9.1.7.).

9.1.9 FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1 Failure with preservation of secure state requires that the TSF preserve a secure state in the face of the identified failures.

9.1.9.1 FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [*forced shutdown, power failure, or system failure*].

This element was satisfied by the TSF. Under forced shutdown, power failure, or system failure in work mode, the TSF does not respond until it has reached the Transition state. The Transition state is defined in the *2in1 PC™ Informal Security Policy Model* as being a secure state. It allows no network connections, no access to either the A or B disk partitions, read only access to the Transition disk partition, and access only to other connected devices that are connected through the !A (not A) or !B (not B) jumper pins.

9.1.9.2 Dependencies

9.1.9.2.1 ADV_SPM.1 Informal TOE Security Policy Model

The TOE meets the requirement for this condition by providing an informal TOE security policy model (ref. Section 3). Upon failure in the work mode, the TSF always transitions to, or through, the Transition state, described in the informal TOE security policy model.

9.1.10 FPT_RCV.4 Function Recovery

Function recovery, provides for recovery at the level of particular SFs, ensuring either successful completion or rollback of TSF data to a secure state.

9.1.10.1 FPT_RCV.4.1

The TSF shall ensure that [*forced shutdown, power failure, or system failure while in work mode*] have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

This element was satisfied by the TSF. In work mode, the TSF recovers to, or through, the Transition state after any forced shutdown, power failure, or system failure. The Transition state is defined in the *2in1 PC™ Informal Security Policy Model* as being a secure state. It allows no network connections, no access to either the A or B disk partitions, read only access to the Transition disk partition, and access only to other connected devices that are connected through the !A (not A) or !B (not B) jumper pins.

9.1.10.2 Dependencies

9.1.10.2.1 ADV_SPM.1 Informal TOE Security Policy Model

The TOE meets the requirement for this condition by providing an informal TOE security policy model. (See Section 3.) Upon failure in the work mode, the TSF always transitions to, or through, the secure (i.e., transition) state, described in the informal TOE security policy model.

9.1.11 FPT_RVM.1 Non-Bypassability of the TSP

FPT_RVM.1 requires non-bypassability for all SFPs in the TSP.

9.1.11.1 FPT_RVM.1.1

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

This element was satisfied by the TSF. In work mode, there are four user visible functions that the TSF controls. They are:

1. Read or write access to disk partitions,

2. Connectivity to network connections,

3. Connectivity to other (optional) TSF controlled devices, and

4. Switch user states.

The TSF controls each of these functions and allows them to proceed only if they comply with the Partitioning Access Policy. Additionally, the user state switch may occur only if it does not violate the Floppy Disk Switching Policy.

9.1.11.2 Dependencies

This requirement has no dependencies.

9.1.12 FPT_SEP.3 Complete Reference Monitor

Complete reference monitor, requires that there be distinct domain(s) for TSP enforcement, a domain for the remainder of the TSF, as well as domains for the non-TSF portions of the TOE.

9.1.12.1 FPT_SEP.3.1

The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

This element was satisfied by the TSF. The TOE security policy is enforced entirely by the 2in1 PC™ card. The TSF is isolated from interference or modification. The state machine implementation is in the Altera chip that is loaded from ROM and is not accessible by untrusted subjects. The EEPROM is not writeable without the set-up plug, and therefore not writeable by untrusted subjects. The IDE checking is also implemented in the Altera chip that is loaded from ROM, and its security attributes are on the EEPROM. The Altera chip has no input interface open to outside of the TSF.

9.1.12.2 FPT_SEP.3.2

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

This element was satisfied by the TSF. The user security domains are maintained by a combination of the security features implemented on the 2in1 PC™ card. The Partitioning Access Policy is intended to contain a user session to an authorised environment that includes a network connection, disk partition(s), and other local

interfaces, depending on the local organisation security policy and the administrator controlled settings. Each user state has it's own domain that includes disk partitions, network connections, and other device connections. Separation of these domains is provided by the TSF.

9.1.12.3 FPT_SEP.3.3

The TSF shall maintain the part of the TSF that enforces the access control and/or information flow control SFPs in a security domain for its own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to the TSP.

This element was satisfied by the TSF. The access control SFPs covered in this requirement are the Partitioning Access Policy and the Administrator Access Policy. There are no information flow control policies for this TOE. The TOE security policy is enforced entirely by the 2in1 PC™ card. The card is isolated from interference or modification. The state machine, IDE checking, and network and other hardware interface access control implementation is in the Altera chip that is loaded from ROM. The Altera chip has no input interface open to outside of the TSF. Object security attributes are on the EEPROM and are not writeable without the set-up plug, and therefore not writeable by untrusted subjects.

9.1.12.4 Dependencies

This requirement has no dependencies.

9.2 ASSURANCE REQUIREMENTS

The assurance requirements for the TOE are the EAL2 assurance requirements, augmented by the informal TOE security policy model requirement. Table 9.2-1 lists the assurance requirements from the *2in1 PC™ Security Target Report.*

Assurance Requirement	Description
ACM_CAP.2	Configuration Items
ADO_DEL.1	Delivery Procedures
ADO_IGS.1	Installation, Generation, and Start-Up Procedures
ADV_FSP.1	Informal Functional Specification
ADV_HLD.1	Descriptive High-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
ATE_COV.1	Evidence of Coverage
ATE_FUN.1	Functional Testing
ATE_IND.2	Independent Testing – Sample
AVA_SOF.1	Strength of TOE Security Function Evaluation
AVA_VLA.1	Developer Vulnerability Analysis

Table 9.2-1 Assurance Requirements

9.2.1 ACM_CAP.2 Configuration Items

9.2.1.1 Evidence Elements

This section addresses the individual content and presentation evidence elements as defined in the CC Version 2, May 1998. Specifically, these elements consist of the unique identification and description of the TOE configuration items. These uniquely identified configuration items provide a definition of the TOE hardware and software elements that lead to an overall unique version number for the TOE. Furthermore, the configuration management system used in the assignment of the identification of hardware items, software items, and the TOE itself is also provided.

9.2.1.2 Evaluator Action Elements and Findings

9.2.1.2.1 Unique Version Numbers

The *2in1 PC™ Configuration Items* satisfies this element by defining a unique version for the TOE. The version defined for the TOE is 1.21. The *2in1 PC™ Configuration Items* further defines the TOE contents, software elements and card components identifying the manufacturer version numbers and in some cases, the reassigned version numbers by the vendor.

9.2.1.2.2 Labeled With Reference

The *2in1 PC™ Configuration Items* satisfies this element by listing labeled version numbers for the TOE such that the consumer can identify the TOE at the point of purchase. Verification that these procedures are in place and that the configuration item version numbers match the evaluated TOE was performed in Section 9.2.2.2.1, Description of Delivery Procedures.

9.2.1.2.3 Configuration List

The *2in1 PC™ Configuration Items* satisfies this element by providing a list of the unique version numbers for the container items of the TOE. The container items define the unique version numbers assigned by the vendor to the contents of the TOE as follows:

Container Item	Version Number
2 x IDE cable	1.21
1 x 2in1 PC™ –Network cable	1.21
1 x 2in1 PC™ –Modem cable	1.21
1 x Y cable	1.21
1 x reset cable	1.21
1 x 2in1 PC™ Installation Guide (Administrator Use)	1.21
1 x 2in1 PC™ Quick Installation Guide (Administrator Use)	1.21
1 x 2in1 PC™ Application Notes (Administrator Use)	1.21
1 x 2in1 PC™ User Guide (End-User Document)	1.21
2 x installation diskettes (disk 1 of 2 and disk 2 of 2)	1.21
1 x 2in1 PC™ card	1.21

Table 9.2.1.2.3-1 Container Items

The software elements define what files are used or are installed on the user's PC during the installation and configuration of the TOE. Some of these elements have been assigned a version number from the other software developers. The rest of the software elements were developed by the vendor and each element has been assigned a reference number to signify the association to the version number of the installation diskettes. These files are uniquely identified in Tables 9.2.1.2.3-2 and Table 9.2.1.2.3-3:

Diskette #1 Item	Version Number / Manufacturer
INSTALL.EXE	Voltaire: 1.21
MEMCLR.EXE	Voltaire: 1.21
PQ.EXE	Voltaire: 1.21 PQ: 3.04.259
REPUI.EXE	Voltaire: 1.21
SENSE.EXE	Voltaire: 1.21
SWITCH.EXE	Voltaire: 1.21
MESSAGES.BM	Voltaire: 1.21
FACTORY.INI	Voltaire: 1.21
INSTALL.INI	Voltaire: 1.21
PCI.DAT	Voltaire: 1.21
INSTALL.HLP	Voltaire: 1.21
2IN1PC.MBR	Voltaire: 1.21
DOS.MBR	Voltaire: 1.21
TRANS.MBR	Voltaire: 1.21
AUTOEXEC.BAT	Voltaire: 1.21
COMPLETE.BAT	Voltaire: 1.21
N.BAT	Voltaire: 1.21
NK.BAT	Voltaire: 1.21
REPORT.BAT	Voltaire: 1.21
UNINST.BAT	Voltaire: 1.21
AUTOEXEC.PUB	Voltaire: 1.21
CONFIG.SYS	Voltaire: 1.21
AUTOEXEC.TRN	Voltaire: 1.21
MSDOS.TRN	Voltaire: 1.21 MS-DOS: 7.0

Table 9.2.1.2.3-2 Software Elements Disk 1

Diskette #1 Item	Version Number / Manufacturer
COMMAND.COM	MS-DOS: 7.0
IO.SYS	MS-DOS: 7.0
ATTRIB.EXE	MS-DOS: 7.0
CHOICE.COM	MS-DOS: 7.0
MORE.COM	MS-DOS: 7.0
MOUSE.COM	MS-DOS: 7.0
SYS.COM	MS-DOS: 7.0
MSDOS.SYS	MS-DOS: 7.0
RAMDRIVE.SYS	MS-DOS: 7.0
HIMEM.SYS	MS-DOS: 7.0

Table 9.2.1.2.3-2 Software Elements Disk 1 (Cont.)

Diskette #2 Item	Version Number / Manufacturer
\DOS\2IN1TSR3.COM	Voltaire: 1.21
\DOS\INSTALL.COM	Voltaire: 1.21
\DOS\TSR.DAT	Voltaire: 1.21
\OS2\AUTOEXEC.BAT	Voltaire: 1.21
\OS2\INSTALL.BAT	Voltaire: 1.21
\UNIX\LINUX\README.TXT	Voltaire: 1.21
\UNIX\LINUX\ V2IN1DRV-0.39.TAR.GZ	Voltaire: 1.21
\UNIX\LINUX\ V2IN1DRV-0.39-LINUX.BIN.TAR.GZ	Voltaire: 1.21
\UNIX\SCO\README	Voltaire: 1.21
\UNIX\SCO\V2I1SCO.TAR	Voltaire: 1.21
UNIX\SCO\V2IN1DRV-0.39-SCO.BIN.TAR.GZ	Voltaire: 1.21
\UTILS\APM.EXE	Voltaire: 1.21
\UTILS\CONFIG.PSW	Voltaire: 1.21
\UTILS\ENCRYPT.EXE	Voltaire: 1.21
\UTILS\PASSWORD.SYS	Voltaire: 1.21
\UTILS\PSW.BAT	Voltaire: 1.21
\UTILS\FILE2E2.EXE	Voltaire: 1.21
\UTILS\RE2.EXE	Voltaire: 1.21
\UTILS\RWE2.EXE	Voltaire: 1.21
\WIN\SETUP.EXE	Voltaire: 1.21
DEBUG.EXE	MS-DOS: 7.0
EDIT.COM	MS-DOS: 7.0
FORMAT.COM	MS-DOS: 7.0
MORE.COM	MS-DOS: 7.0

Table 9.2.1.2.3-3 Software Elements Disk 2

The card components define the low-level components the TOE is comprised of. These components are assigned unique version numbers from the manufacturer and in some cases, the vendor has reassigned the numbers as follows:

Card Component	Version Number / Manufacturer
1 x PCB	Voltaire: Rev. B
1 x EEPROM chip	ATMEL: AT28C16-15SC or Xicor: X2816CS-15 Voltaire: 1.21
1 x PROM chip	Altera: EPC1441 LC20 Voltaire: 12A
6 x Electro-mechanical relays	NaiS: TQ2SA-5V
1 x Internal Set-up plug	None
1 x Altera chip	Altera Flex EPF6016TC144-3
2 x IDE connectors	None
4 x Network connectors	None
6 x Floppy disconnection jumpers	None

Table 9.2.1.2.3-4 Card Components

9.2.1.2.4 Description of Configuration Items that Comprise the TOE

The *2in1 PC™ Configuration Items* satisfies this element by providing a description of each configuration item the TOE is comprised of. These items are defined as follows:

Container Item	Version Number	Description
2 x IDE cable	1.21	Used to connect the hard disk(s) to the 2in1 PC™ card, and the 2in1 PC™ card to the IDE controller.
1 x 2in1 PC™ –Network cable	1.21	Used to connect one 2in1 PC™ network connector to a network interface card.
1 x 2in1 PC™ –Modem cable	1.21	Used to connect one 2in1 PC™ network connector to a modem.
1 x Y cable	1.21	Used to connect both 2in1 PC™ network connectors to one NIC.
1 x reset cable	1.21	Used to connect the 2in1 PC™ card to the motherboard's reset pins (necessary only with certain platforms).
1 x 2in1 PC™ Installation Guide (Administrator Use)	1.21	Provide detailed installation and administration instructions for the installer/administrator.
1 x 2in1 PC™ Quick Installation Guide (Administrator Use)	1.21	Provide quick and simple installation reference for the installer/administrator.
1 x 2in1 PC™ Application Notes (Administrator Use)	1.21	Provide information to the installer/administrator about special problematic hardware platforms, and troubleshooting.
1 x 2in1 PC™ User Guide (End-User Document)	1.21	Provide operating instructions for the end user.
2 x installation diskettes (disk 1 of 2 and disk 2 of 2)	1.21	Used to configure the PC on which the 2in1 PC™ is installed.
1 x 2in1 PC™ card	1.21	(See Table 9.2.1.2.4-4)

Table 9.2.1.2.4-1 Container Items

The software elements define what files are used or installed on the user's PC during the installation and configuration of the TOE. Some of these elements have been assigned a version number from the other software developers. The rest of the software elements

were developed by the vendor and each element has been assigned a reference number to signify the association to the version number of the installation diskettes. These files are described in Table 9.2.1.2.4-2 and Table 9.2.1.2.4-2 as follows:

Diskette #1 Item	Version Number / Manufacturer	Description
INSTALL.EXE	Voltaire: 1.21	2in1 PC™ installation program
MEMCLR.EXE	Voltaire: 1.21	RAM clearing utility, copied to T partition.
PQ.EXE	Voltaire: 1.21 PQ: 3.04.259	PowerQuest Partition Magic disk partitioning utility (compressed)

Table 9.2.1.2.4-2 Software Elements Disk 1

Diskette #1 Item	Version Number / Manufacturer	Description
REPUI.EXE	Voltaire: 1.21	Report and diagnostics utility
SENSE.EXE	Voltaire: 1.21	Card state output utility. Copied to all partitions.
SWITCH.EXE	Voltaire: 1.21	State switching utility. Gets copied to all partitions.
MESSAGES.BM	Voltaire: 1.21	Installation messages file.
FACTORY.INI	Voltaire: 1.21	Factory settings INI file.
INSTALL.INI	Voltaire: 1.21	User specified settings (or default) INI file.
PCI.DAT	Voltaire: 1.21	PCI database used to determine the appropriate reset method.
INSTALL.HLP	Voltaire: 1.21	Installation help file.
2IN1PC.MBR	Voltaire: 1.21	Message file. Used as the disk based MBR if the AMO option is disabled.
DOS.MBR	Voltaire: 1.21	DOS 7.0 MBR bootstrap code
TRANS.MBR	Voltaire: 1.21	MBR for read only disks. Copied to the T partition.
AUTOEXEC.BAT	Voltaire: 1.21	Auto-execute file for the installation diskette.
COMPLETE.BAT	Voltaire: 1.21	Batch file for copying files into the A, B and T partitions. In addition to copying files, two files are created on the fly in the T partition: TR_TO_A.BAT and TR_TO_B.BAT (empty placeholder files that are executed in Ta and Tb, respectively. Can be used to call one set of programs in Ta and another in Tb).
N.BAT	Voltaire: 1.21	Quick installation batch file.
NK.BAT	Voltaire: 1.21	Quick installation batch file (allows additional parameters).
REPORT.BAT	Voltaire: 1.21	Report generation batch file.
UNINST.BAT	Voltaire: 1.21	Uninstallation batch file.
AUTOEXEC.PUB	Voltaire: 1.21	Auto-execute file for the A and B partitions. Appended to existing AUTOEXEC.BAT file in A, copied to B.
CONFIG.SYS	Voltaire: 1.21	Driver loading and settings for the installation diskette.
AUTOEXEC.TRN	Voltaire: 1.21	Auto-execute file for T partition. Copied to T partition.
MSDOS.TRN	Voltaire: 1.21 MS-DOS: 7.0	DOS Configuration file for T partition (disables Windows logo and boot stopping).
COMMAND.COM	MS-DOS: 7.0	DOS 7.0 shell.
IO.SYS	MS-DOS: 7.0	DOS 7.0 I/O and hardware interface.
ATTRIB.EXE	MS-DOS: 7.0	DOS 7.0 file attribute editing utility.
CHOICE.COM	MS-DOS: 7.0	DOS 7.0 utility for enabling menu choice. Gets copied to T
MORE.COM	MS-DOS: 7.0	DOS 7.0 utility for pausing when screen is full (used for REPORT).
MOUSE.COM	MS-DOS: 7.0	DOS 7.0 mouse driver
SYS.COM	MS-DOS: 7.0	DOS 7.0 utility for making partitions bootable.
MSDOS.SYS	MS-DOS: 7.0	DOS 7.0 configuration file.
RAMDRIVE.SYS	MS-DOS: 7.0	DOS 7.0 RAM drive driver.
HIMEM.SYS	MS-DOS: 7.0	DOS 7.0 high-memory driver.

Table 9.2.1.2.4-2 Software Elements Disk 1 (Cont.)

Diskette #2 Item	Version Number / Manufacturer	Description
\DOS\2IN1TSR3.COM	Voltaire: 1.21	2in1 PC™ DOS driver
\DOS\INSTALL.COM	Voltaire: 1.21	DOS driver installation batch file
\DOS\TSR.DAT	Voltaire: 1.21	DOS Driver path file
\OS2\AUTOEXEC.BAT	Voltaire: 1.21	OS2 Auto-execute batch file
\OS2\INSTALL.BAT	Voltaire: 1.21	2in1 PC™ OS2 installation batch file
\UNIX\LINUX\README.TXT	Voltaire: 1.21	2in1 PC™ Linux installation instructions
\UNIX\LINUX\ V2IN1DRV-0.39.TAR.GZ	Voltaire: 1.21	2in1 PC™ Linux driver source
\UNIX\LINUX\ V2IN1DRV-0.39-LINUX.BIN.TAR.GZ	Voltaire: 1.21	2in1 PC™ Linux driver installation
\UNIX\SCO\README	Voltaire: 1.21	2in1 PC™ SCO driver installation instructions
\UNIX\SCO\V2I1SCO.TAR	Voltaire: 1.21	2in1 PC™ SCO driver source
UNIX\SCO\V2IN1DRV-0.39-SCO.BIN.TAR.GZ	Voltaire: 1.21	2in1 PC™ SCO driver installation
\UTILS\APM.EXE	Voltaire: 1.21	Check whether the PC supports Advanced Power Management.
\UTILS\CONFIG.PSW	Voltaire: 1.21	CONFIG.SYS file for password in T partition (optional use)
\UTILS\ENCRYPT.EXE	Voltaire: 1.21	Utility for changing T password
\UTILS\PASSWORD.SYS	Voltaire: 1.21	T partition password driver
\UTILS\PSW.BAT	Voltaire: 1.21	T partition password installation batch file
\UTILS\FILE2E2.EXE	Voltaire: 1.21	Utility for writing a file to the EEPROM
\UTILS\RE2.EXE	Voltaire: 1.21	Utility for outputting the EEPROM content to the screen
\UTILS\RWE2.EXE	Voltaire: 1.21	Utility for reading and writing to the EEPROM
\WIN\SETUP.EXE	Voltaire: 1.21	2in1 PC™ Windows (All versions) driver installation program
DEBUG.EXE	MS-DOS: 7.0	DOS 7.0 debugger
EDIT.COM	MS-DOS: 7.0	DOS 7.0 text editor
FORMAT.COM	MS-DOS: 7.0	DOS 7.0 disk formatting utility
MORE.COM	MS-DOS: 7.0	DOS 7.0 utility for pausing when screen is full.

Table 9.2.1.2.4-3 Software Elements Disk 2

The card components describe the low-level components the TOE is comprised of. These components are defined as follows:

Card Component	Version Number / Manufacturer	Description
1 x PCB	Voltaire: Rev. B	The actual fiberglass printed circuit card used to mount the electronic components.
1 x EEPROM chip	ATMEL: AT28C16-15SC or Xicor: X2816CS-15 Voltaire: 1.21	Used to store configuration data.

Table 9.2.1.2.4-4 Card Components

Card Component	Version Number / Manufacturer	Description
1 x PROM chip	Altera: EPC1441 LC20 Voltaire: 12A	Used to store the code that operates the 2in1 PC™ card.
6 x Electro-mechanical relays	NaiS: TQ2SA-5V	Used to sever network and telephone wires connected to the 2in1 PC™ card.
1 x Internal Set-up plug	None	Used to Enable EEPROM alteration and full disk access.
1 x Altera chip	Altera Flex EPF6016TC144-3	Used to perform processing and logic operations.
2 x IDE connectors	None	Used to route the IDE cables through the 2in1 PC™ card.
4 x Network connectors	None	Used to route the network/telephone cables through the 2in1 PC™ card.
6 x Floppy disconnection jumpers	None	Used to provide the ability to sever peripheral devices' cables.

Table 9.2.1.2.4-4 Card Components (Cont.)

9.2.1.2.5 Method of Unique Identification of Configuration Items

The *2in1 PC™ Configuration Items* satisfies this element by defining a unique method of identification. Both the installation diskettes and the 2in1 PC™ card are clearly marked as version 1.21. The following is a list of the uniquely identified TOE elements:

Container Item	Version Number	Description
2 x installation diskettes (disk 1 of 2 and disk 2 of 2)	1.21	Voltaire's version number is incremented by 0.01 every time a minor change, such as a bug fix, is implemented. Incremented by 0.1 when a major change, such as new logic design is implemented.
1 x 2in1 PC™ card	1.21	Voltaire's version number is incremented by 0.01 every time a minor change, such as a bug fix, is implemented. It is incremented by 0.1 when a major change, such as new logic design or card architecture is implemented.

Table 9.2.1.2.4-1 Container Items

Container Item	Version Number	Description
1 x 2in1 PC™ Installation Guide (Administrator Use)	1.21	Voltaire's version number is incremented by 0.01 every time a minor change, such as a documentation correction, is made. It is incremented by 0.1 when a major change, such as a minor change to the product's design has been made.
1 x 2in1 PC™ Quick Installation Guide (Administrator Use)	1.21	Voltaire's version number is incremented by 0.01 every time a minor change, such as a documentation correction, is made. It is incremented by 0.1 when a major change, such as a minor change to the product's design has been made.
1 x 2in1 PC™ Application Notes (Administrator Use)	1.21	Voltaire's version number is incremented by 0.01 every time a minor change, such as a documentation correction, is made. It is incremented by 0.1 when a major change, such as a minmr change to the product's design has been made.
1 x 2in1 PC™ User Guide (End-User Document)	1.21	Voltaire's version number is incremented by 0.01 every time a minor change, such as a documentation correction, is made. It is incremented by 0.1 when a major change, such as a minor change to the product's design has been made.

Table 9.2.1.2.4-1 Container Items (Cont.)

The 2in1 PC™ card components specify the method of identification used for the following items:

Card Component	Version Number / Manufacturer	Description
1 x PCB	Voltaire: Rev. B	Version number incremented by one letter every time the PCB is reedited.
1 x EEPROM chip	ATMEL: AT28C16-15SC Or Xicor: X2816CS-15 Voltaire: 1.21	Atmel and Xicor are identical 2K EEPROMs used interchangeably during manufacturing. They both offer the same functionality. Their use is determined by manufacturing prices. The Voltaire version number is identical to the overall product version number, and changes with it.
1 x PROM chip	Altera: EPC1441 LC20 Voltaire: 12A	Voltaire's version number is incremented by one letter every time a minor change, such as a bug fix, is implemented. It is incremented by one number when a major change, such as a new logic design or card architecture is implemented.

Table 9.2.1.2.5-2 Card Components

The EEPROM component of the TOE is manufactured by either AMTEL or Xicor and the vendor has assigned version number of 1.21 to identify either chip. The selection of the EEPROM chip is based on manufacturer pricing, however both chips offer the same functionality (i.e., to store the 2in1 PC™ card configuration data). The PROM chip has been assigned a vendor number 12A. A unique vendor number has been assigned to this component due to the fact that future versions of the 2in1 PC™ card may share the same PROM but have different instruction sets hard coded during production.

9.2.1.2.6 Unique Identification of Configuration Items

The *2in1 PC™ Configuration Items* satisfies this element by uniquely identifying each configuration item of the TOE. This list of items was used to verify that the TOE

delivered in Section 9.2.2 ADO_DEL.1 Delivery Procedures was properly marked with the specified manufacturer and vendor version numbers.

9.2.1.2.7 Configuration Items Evidence

The following vendor documentation was referenced to satisfy this assurance component.

- E21198041(4), *2in1 PC™ Configuration Items*

9.2.2 ADO_DEL.1 Delivery Procedures

9.2.2.1 Evidence Elements

This section addresses the vendor delivery procedures when delivering the TOE to the user's location. The system controls and distribution facility procedures are defined to provide assurance that the recipient receives the TOE without any modifications. The established procedures define the steps the developer is enforcing to guarantee that the recipient receives the version that corresponds precisely to the TOE master copy, thus avoiding any tampering with the actual version, or substitution of a false version.

9.2.2.2 Evaluator Action Elements and Findings

9.2.2.2.1 Description of Delivery Procedures

The delivery procedures implemented by Voltaire satisfy this element by defining the steps for the secure delivery of the TOE to the user's site. The specific steps followed by Voltaire are:

1. Every 2in1 PC™ card undergoes a full final test before being packaged and shipped. This test ensures that the card is in working order (functionality-wise and security-wise), ensures that the PROM version and the software on the installation diskette are correct. (See *2in1 PC™ Product Approval Tests* for further information regarding this procedure).

2. A sticker with the product's overall version number is placed on the card itself.

3. Every TOE package is individually sealed using a sticker displaying the Voltaire logo, thereby preventing the possibility of opening the box and tampering with its contents without being noticed.

4. A sticker with the product's overall version number is placed on the package.

5. The TOE is stored in a controlled environment prior to shipment, i.e., a guarded office building, inside a locked office protected by an alarm system.

6. Cards are shipped to their final destination either by courier or by public mail.

After reviewing the vendor delivery procedure documentation, an order for the TOE was placed to verify that the documented delivery procedures were being enforced. After receipt of the TOE, these delivery procedures were verified. This verification was performed in the following manner:

1. Physically inspecting the package upon receipt to confirm that the TOE was properly sealed.

2. Confirming that the TOE received matched the configuration items listed in Section 9.2.1.

   Note: Version numbers on the card and package were not confirmed upon receipt of the TOE (items 2 and 4 of the vendor delivery procedures). This was due to the fact that when the order for the TOE was made, these procedures were not specified. The requirement for these procedures was identified and has been incorporated into Voltaire's delivery procedures.

3. Installing and configuring the TOE to confirm that the 2in1 PC™ card operated as specified. Section 9.2.12 defines the independent testing that was conducted and provides details on the tests performed.

9.2.2.2.2 Delivery Procedures Evidence

The following vendor documentation was referenced to satisfy this assurance component.

- E20598011, *2in1 PC™ Product Approval Tests*
- E21198045, *2in1 PC™ Delivery Procedure*

9.2.3 ADO_IGS.1 Installation, Generation, and Start-Up Procedures

9.2.3.1 Evidence Elements

9.2.3.2 Evaluator Action Elements and Findings

This section addresses the installation, generation, and start-up procedures after receipt of the TOE from the vendor. These procedures provide assurance that the documentation provided as part of the TOE is sufficient in detail to securely configure the TOE in its target environment.

9.2.3.2.1 Description of Installation, Generation, and Start-Up

Verification of the vendor's installation, generation, and start-up procedures for the TOE satisfies this element. These one-time procedures were verified using only the supporting documentation, the installation software, and other package contents that was provided

with the TOE in order to configure it to a secure operational state. Before the installation of the TOE commenced, the *2in1 PC Installation Guide* was used to verify that all of the TOE components have been received. Once this verification was made, Chapter 9 of the *2in1 PC Installation Guide* was also examined. This Chapter addresses the reconfiguration, reinstallation, or removal of the 2in1 PC™ card. For the specific evaluation details of the TOE documentation, please refer to the COACT, Inc. document entitled *Evaluation of the 2in1 PC Installation Guide, Version 1.21.* This document defines areas expressed to the vendor that should be included in future versions of the installation guide, however do not directly affect the procedures necessary for the secure installation, generation, and start-up of the TOE. When performing the installation, generation, and start-up procedures, the TOE provided a Graphical User Interface (GUI) so that the administrator could verify that the TOE security functions were properly configured.

9.2.3.2.2 Determination of Resulting Configuration

Verification of the vendor-supplied installation, generation, and start-up procedure documentation has satisfied this element. This verification was performed by installing the TOE using the included product documentation and by performing a trial run to confirm that the TOE security functions were being enforced. Once the enforcement of the TOE security functions was verified, the security functions were further evaluated through the replication of vendor tests and the execution of independent evaluator tests defined in Section 9.2.12 ATE_IND.2, Independent Testing - Sample.

9.2.3.2.3 Installation, Generation, and Start-Up Evidence

The following vendor documentation was referenced to satisfy this assurance component.

- E21298062, *2in1 PC™ App. Notes – Special Settings*
- E21298063, *2in1 PC™ Installation Guide*
- E21298064, *2in1 PC™ Quick Installation Guide*
- E21198039(2), *Evaluation of the 2in1 PC™ Installation Guide, Version 1.21*

9.2.4 ADV_FSP.1 Informal Functional Specification

9.2.4.1 Documentation Included in the Functional Specification

The following documents were considered part of the 2in1 PC™ functional specification:

- E21198024, *2in1 PC™ System Design Document*
- E21298054, *2in1 PC™ Functional Specifications*
- E21198061, *2in1 PC™ Updates to the SYD EEPROM Mapping Section*

9.2.4.2 Evidence Elements

This section addresses the informal functional specification that completely represents the TSF. The informal functional specification provides a high-level description of the user-visible interfaces and the behavior of the TSF. It is an instantiation of the TOE security

functional requirements. The functional specification shows that all the TOE security functional requirements have been addressed.

9.2.4.3 Evaluator Action Elements and Findings

9.2.4.3.1 Description of the TSF and External Interfaces

The TOE satisfies this element. The TOE functional specification is in an informal style, written in English. All documents listed in Section 9.2.4.1 were considered in making this determination.

9.2.4.3.2 Internally Consistent

The TOE satisfies this element. The functional specification is internally consistent. It contains no contradictory statements. The initial documentation, the *2in1 PC™ System Design Document*, is incomplete, sometimes vague, and has a few errors in it. These problems have been corrected with supplemental documentation, including the *2in1 PC™ Functional Specification* and *Updates to the SYD EEPROM Mapping Section.* The new functional specification is consistent with the *2in1 PC™ System Design Document*, but organises and defines the functions differently and adds more detail. The *Updates to the SYD EEPROM Mapping Section* provide corrections to Appendix A – 2in1 PC™ Configuration Summary in the *2in1 PC™ System Design Document.* All documents listed in Section 9.2.4.1 were considered in making this determination.

9.2.4.3.3 Purposes and Uses of External Interfaces

The TOE satisfies this element. The *2in1 PC™ Functional Specification* provides sufficient information on the purposes and uses of the interfaces to the TSF. An examination of the 2in1 PC™ card reveals the existence of the following physical connections:

1. ISA edge connector to the PC motherboard,
2. IDE bus connector to the PC motherboard (or the hard disk controller card, as appropriate),
3. IDE bus connector to the hard disk drive,
4. 2 RJ-45 network connector sockets,
5. 2 RJ-11 network connector sockets,
6. Set-up plug connector pins,
7. 26 jumper pins, and an

8. External set-up connector jack.

Additionally, there are 6 electro-mechanical relays that, while they are not external interfaces, provide the access control mechanism that enforces the security policy on some of the external interfaces (see Sections 9.2.4.3.3.4 and 9.2.4.3.3.6).

The uses of each of these interfaces are described in the *2in1 PC™ Functional Specification* and are more fully explained in other supporting documentation (e.g., *2in1 PC™ Installation Guide*).

All of the TSFIs listed in the following sections can be derived, directly or indirectly, from the security functional requirements presented in Section 9.1. All interfaces mandated or implied in the security functional requirements are discussed in the *2in1 PC™ Functional Specifications.*

As described in the following sections, the available documentation identifies all interfaces to the TSF and correctly and completely describes the behavior of the TOE at each external interface. All security relevant input parameters, or a characterisation of those parameters, have been described. The following sections provide specific references to documentation, in addition to the *2in1 PC™ Functional Specification,* that was used in determining the purpose and use of all of the external interfaces to the TSF.

9.2.4.3.3.1 ISA Bus

The ISA bus is used to receive reset signals and detect DMA2 activity. It is used in the following security functions, as described in the *2in1 PC™ Functional Specification*:

1. In work mode, control the flow of state changes (Function 7)

2. In work mode, monitor DMA2 activity during the Transition state and prevent state switching upon detection thereof (Function 9)

Detection of DMA2 activity affects the enforcement of the Floppy Disk Switching Policy in that the TSF will not allow any state switching if DMA2 activity has been detected in the Transition state. This detection is performed by the DMA controller receiving DMA2 activity from the ISA bus only. Since PCI devices do not interface with the DMA controller, their operation is not monitored by the TSF. This condition may only be cleared by a reboot. (Ref. *2in1 PC™ System Design Document,* Sections 3.1 & 4.2.2.)

The ISA bus reset signal is used as a part of state switching, but does not directly affect the enforcement of the security policy. It indirectly affects the enforcement of the Partitioning Access Policy in that it can affect the machine state. However, the TSF will continue to enforce the Partitioning Access Policy for whatever state the machine is in. (Ref. *2in1 PC™ System Design Document,* Sections 3.1, 3.4, 3.5 & 4.2.2.)

9.2.4.3.3.2 IDE Bus – PC

The IDE connection from the PC motherboard (or the hard disk controller card, as appropriate) is used in several of the security functions described in the *2in1 PC™ Functional Specification.* Those uses are shown in Table 9.2.4.3.3-1.

Function (*2in1 PC™ Functional Specification)*	**Use of the IDE Interface**
1 – Allow the setting up and configuration of the 2in1 PC™ attributes.	Inputs are attributes and parameters from the PC during set-up. This input includes many of the attributes and parameters used to enforce the Partitioning Access Policy and the Floppy Disk Switching Policy. (Ref. *2in1 PC™ System Design Document,* Sections 3.1, 3.4 & 4.2.4.)
2 – Provide storage for configuration data (including card configuration and MBRs).	Inputs are requests from the PC for configuration information contained on the EEPROM and reads for MBR addresses. Outputs are MBR data and configuration data (including security attributes and parameters) to the PC. These inputs and outputs include many of the attributes and parameters used to enforce the Partitioning Access Policy and the Floppy Disk Switching Policy. (Ref. *2in1 PC™ System Design Document,* Sections 3.1, 3.4 & 4.2.4.)
3 – In work mode, provide a state machine with three distinct states of operation: A, B, and T.	Outputs state information to the PC. This external output does not directly affect the enforcement of security policy. (Ref. *2in1 PC™ System Design Document,* Sections 3.1, 3.4, 3.5 & 4.2.2.)
4 – In work mode, provide a different MBR for each security state during boot.	Inputs are read requests for the MBR address (sector 0,0,1). Output is MBR data to the PC. These inputs and outputs are used to enforce the Partitioning Access Policy. As the state machine changes state, the PC is booted, or rebooted, from the new state's assigned disk partitions. (Ref. *2in1 PC™ System Design Document,* Sections 3.1, 3.4, 3.5 & 4.2.4.)
5 – In work mode, control access to disk partitions based on the current machine state and the access security policy.	Inputs are disk commands, addresses, and data from the PC. Disk addresses are checked to see if they are within the partition boundaries for the partition associated with the current state or the "Functional" partition. Disk commands are checked to see that they are legal operations (e.g., read, write) to the partition for which they are addressed. IDE commands and addresses are used to enforce the Partitioning Access Policy on access to disk partitions. (Ref. *2in1 PC™ System Design Document,* Sections 3.1, 3.2, 3.4, 4.2.1 & 4.2.3.)
7 – In work mode, control the flow of state changes.	Inputs are the switch command and the reset signal. The reset signal and the switch command are used as a part of state switching, but do not directly affect the enforcement of security policy. The TSF will enforce the Partitioning Access Policy for whatever state the machine is in. (Ref. *2in1 PC™ System Design Document,* Sections 3.1, 3.4, 3.5 & 4.2.2.)

Table 9.2.4.3.3-1 Uses of the IDE Interface

9.2.4.3.3.3 IDE Bus – Disk

The IDE bus connector to the hard disk drive is used to send valid commands, addresses, and data to the hard disk and return information from the hard disk. The validity of the commands and addresses is determined in Function 5, as described in the *2in1 PC™ Functional Specification.* IDE outputs from the TSF to the hard disk drive are the results of the enforcement of the Partitioning Access Policy. (Ref. *2in1 PC™ System Design Document,* Sections 3.1, 3.2, 3.4, 3.5, 4.2.1, & 4.2.3.)

Note: The flow of IDE commands, addresses, and data from the hard disk drive back to the PC are not covered by the TSP, and are not monitored by the TSF.

9.2.4.3.3.4 Network Connectors

The 2in1 PC™ card has two RJ-45 network connection sockets and two RJ-11 network connection sockets. One RJ-45 and one RJ-11 network connection socket is used to provide connectivity to each of the two networks (networks A and B). The connectivity to each of the two networks is enforced by the TSF controlling two electro-mechanical relays for each of the two networks. The A network cable is connected into the 'Net A' RJ-45 connection socket on the 2in1 PC™ card. This socket is connected to an electro-mechanical relay, is routed through a second (redundant) electro-mechanical relay, and is then routed out to the 'Net A' RJ-11 network connector for the A network. The B network cable is connected into the 'Net B' RJ-45 connection socket on the 2in1 PC™ card. This socket is connected to an electro-mechanical relay, is routed through a second (redundant) electro-mechanical relay, and is then routed out to the 'Net B' RJ-11 network connector for the B network. The network connector sockets themselves are not a direct interface to the TSF, but are controlled by another interface (i.e., the electro-mechanical relays). The RJ-45 sockets connect to the external networks and the RJ-11 sockets connect to the PC's NIC card or modem. There are two electro-mechanical relays between each of the RJ-45 sockets and RJ-11 sockets. The TSF controls the electro-mechanical relays, allowing or disallowing these network connections to be made. There are two relays on each circuit to provide redundant backup. Both must be closed for the circuit to be complete. The use of this interface is described in Function 6, in the *2in1 PC™ Functional Specification.* (Ref. *2in1 PC™ System Design Document,* Sections 3.1, 3.4, & 4.2.1. Additional details on the network connections are also provided in the *2in1 PC™ Installation Guide,* Chapter 7.)

The electro-mechanical relays are used to enforce the Partitioning Access Policy on access to external networks.

9.2.4.3.3.5 Set-up Pins/Plugs

The set-up plug connector pins accept the 2in1 PC™ set-up plug that identifies a user as being in the administrator role and that the machine is in set-up mode. The PC must be powered off to insert or remove the set-up plug on the 2in1 PC™ card. This must be performed since the TSF only checks for the presence of the set-up plug after powering

on the PC. Inserting or removing the set-up plug while the machine has not been powered off will not change the mode (set-up or work) that the 2in1 PC™ card is running in. The presence of the 2in1 PC™ set-up plug also physically and logically enables the write operations to the EEPROM, causes the network electro-mechanical relays to be opened (i.e., disconnecting all networks), causes the other connected device electro-mechanical relays associated with A and B to be opened (i.e., disconnecting all devices connected through the A and B jumpers), causes the other connected device electro-mechanical relays associated with !A (Not A) and !B (Not B) to be closed (i.e., connecting all devices connected through the !A (Not A) and !B (Not B) jumpers), and allows all IDE commands to pass without being monitored. There are two methods of using the set-up pins to place the 2in1 PC™ card into setup mode. The first, and recommended, method is with the standard, black, set-up plug. When this plug is inserted on the set-up pins, set-up mode is activated. The second method is to attach the gray, internal enabler plug to the set-up pins, and leave it in place. The PC must also be powered off to insert or remove the external set-up plug. This enables the use of an external, phone jack type, plug to enter set-up mode. This external set-up plug is inserted in the external set-up connector jack. This second method is not recommended because it allows the TSF to be put into set-up mode without removing the cover of the host PC to insert a plug for which the user does not have access. This could allow a user to enter set-up mode with only an easily obtainable microphone jack plug. Although the users are assumed to be trusted not to modify the TOE, it should not be that easy to assume the administrator role.

Table 9.2.4.3.3-2 shows how the functions specified in the *2in1 PC™ Functional Specification* use the set-up pins/plug.

Function (*2in1 PC™ Functional Specification*)	**Use of the Set-up Pins/Plug**
1 – Allow the setting up and configuration of the 2in1 PC™ attributes.	If the set-up plug is installed on the set-up pins, the EEPROM is made writeable and security attributes and parameters may be stored. (Ref. *2in1 PC™ System Design Document*, Sections 3.1, 3.4, & 4.2.4.)
11 – Detect the presence of a physical set-up plug in order to switch into set-up mode and allow configuration.	If the set-up plug is installed on the set-up pins, and the PC is powered back on, the Altera chip senses the presence of the set-up plug and places the TOE in set-up mode, and establishes the user as being in the administrator role. This allows all disk access, breaks all network connections, and other device connections are broken or established. (Ref. *2in1 PC™ System Design Document*, Sections 3.1, 3.4, & 4.2.4.)

Table 9.2.4.3.3-2 Set-up Pins/Plug Uses

The set-up pins/plugs are used in the enforcement of all of the security policies. The Identification and Authentication Policy assigns user roles and machine modes based on the presence or absence of the set-up plug. When the plug is in place, the TOE is in set-up mode and the user is in the administrator role. Otherwise, the TOE is in work mode and the user is in the user role. Based on the user role, different rules are applied in the Partitioning Access Policy. Administrator Access Policy rules are based on the user's

role. The Floppy Disk Switching Policy is enforced only in work mode. (See Section 3 for a detailed description of these security policies.)

9.2.4.3.3.6 Jumper Pins

The external device pins (i.e., pins 1-6) provide the attributes (i.e., A or !A and B or !B) used in the Partitioning Access Policy for the attached devices. The Partitioning Access Policy is enforced on the attached devices using the electro-mechanical relays. The indicator pins (i.e., pins 7-12) provide an externally available indication of the state of the state machine, but are not used for any security functionality. The reset pins (i.e., pins 13-14) can be used to provide a reset signal to older-style PCs. If they were used when not needed, they may have no affect, depending on the configured reset signal. If not used when required, switching would be prevented. In either case, the Partitioning Access Policy continues to be enforced. Pins 15-16 are reserved for future Voltaire use, and were not used in the evaluated configuration. The switch disable pins (i.e., pins 17-18) may prevent state switching, but will not affect the correct enforcement of security policy. The net select pins (i.e., pins 19-26) are jumpered in specified patterns to indicate the type of networks that are connected through the A and B network connector sockets (see *2in1 PC™ Installation Guide,* Appendix C for the correct settings). These pins do not provide or affect any security relevant functionality. The RJ-45 connectors provide for a total of 8 wires to come in from an attached network. Ethernet uses wires 1,2,3, and 6. Token-Ring uses wires 3,4,5, and 6. The pins map the correct network wires to the PC side of the connection. Incorrect settings will make connected networks inaccessible, but do not effect security policy. Jumper pins usage is shown in Table 9.2.4.3.3-3.

Pins	**Use**	***2in1 PC™ Functional Specification* Reference**
1 - 6	Control up to two external devices (one each in states A and B). The system administrator applies jumper wires to two pins, connecting to/from the external devices, allowing connectivity in accordance with local policy. Control of the external device(s) is achieved by routing the one of the control signals (e.g., "Device Ready" signal for a floppy disk) from the peripheral device cable through an electro-mechanical relay. Allowable settings are A or !A (not A) and B or !B (not B). (See Note 1) (Ref. *2in1 PC™ System Design Document,* Sections 3.1, & 4.2.1. Additional details on the use of these pins are provided in the *2in1 PC™ Installation Guide,* Chapter 1 & Appendix B.)	Function 10
7 - 12	State indicator outputs from the TSF. Pins 8, 10, & 12 provide +5V when in states A, B, & T, respectively. Otherwise 0V are present. Pins 7, 9, & 11 provide a logical "0" for the active state and logical "1" for inactive states for states A, B, & T, respectively. (Ref. *2in1 PC™ System Design Document,* Sections 3.1, & 4.2.2. Additional details on the use of these pins are provided in the *2in1 PC™ Installation Guide,* Appendix B.)	Function 3

Table 9.2.4.3.3-3 2in1 PC™ Jumper Pins

Pins	Use	*2in1 PC™ Functional Specification* Reference
13 - 14	If jumper wires are connected to the reset pins on the motherboard, the TSF provides a reset signal for computers that use a non-standard reset scheme (Ref. *2in1 PC™ System Design Document,* Sections 3.1, 3.4, & 4.2.2. Additional details on the use of these pins are provided in the *2in1 PC™ Installation Guide,* Appendices B & C.)	Function 7
15 - 16	Reserved for future Voltaire add-ons. (Ref. *2in1 PC™ Installation Guide,* Appendix B.)	
17 - 18	If jumper wires connecting the pins to an external device (not part of the TSF) are present, a "switch disable" signal can be received by the TSF (See Note 2). (Ref. *2in1 PC™ System Design Document,* 4.2.2. Additional details on the use of these pins are provided in the *2in1 PC™ Installation Guide,* Chapter 1 & Appendix B.)	Function 7
19 - 22 and 23 - 26	These pins are jumpered in specified patterns to indicate the type of networks that are connected through the A and B network connector sockets. (Ref. *2in1 PC™ Installation Guide,* Chapter 7 & Appendix B.)	Not security function related.

Table 9.2.4.3.3-3 2in1 PC™ Jumper Pins (Cont.)

Note 1: These pins connect to two electro-mechanical relays (one for each circuit) that are controlled by the TSF, as specified in Function 10 of the *2in1 PC™ Functional Specification.* They are not a direct interface to the TSF, but are controlled by another interface (i.e., the electro-mechanical relays), just as are the RJ-45 and RJ-11 network connectors. The jumper pins provide the attributes (i.e., A or !A and B or !B) used in the Partitioning Access Policy for the attached devices.

Note 2: These pins may be used by an optional, external device (e.g., biometric I&A device) to disallow transition to an operational machine state until this signal is asserted. Improper use of this signal will not violate the TOE security policy, but will prevent state switching.

9.2.4.3.4 Complete Representation of the TSF

The TOE satisfies this element. All security functions contained in the TOE summary specification of the ST are fully represented in the documentation that makes up the TOE functional specifications. However, there are some security relevant functions described in the user and administrator guidance, as well as elsewhere in the documentation, that are outside of the TSF. The TSF is contained entirely on the 2in1 PC™ card. Several of the vendor supplied documents describe software support provided on the host PC. This software is complimentary to the TSF and provides assistance to the administrator in setting-up and configuring the TSF, and to the user in switching states, but is not necessary for the correct function of the TSF. This software is all outside the TSC. It provides user-friendly support, but adds no additional security functionality or interfaces to the TSF. Included in this category of support is a process that runs in the Transition state that clears PC RAM between user states. While this is a desirable function, it is outside of the TSC. Likewise, there are processes that run in each of the user states (i.e.,

A and B) that show the current state of the state machine or can cause the commands to be sent to the TSF to change to the other user state. These processes are also outside of the TSC. Therefore, while providing some useful functionality, none of these processes can be trusted.

Similarly, there is a recommendation, and instructions for adding identification and authentication (I&A) mechanisms into the Transition state in the PC (see *2in1 PC™ Installation Guide*). That I&A mechanism is outside of the TSC.

All documents listed in Sections 9.2.4.1 and 9.2.4.6 were considered in determining that the TSF is completely represented in the 2in1 PC™ functional specifications.

9.2.4.3.5 Accurate and Complete Instantiation of TOE Security Functional Requirements

The TOE satisfies this element. The *2in1 PC™ Functional Specifications* completely and accurately cover the security functional requirements from the ST. Table 9.2.4.3.5-1 shows the mapping from the security functional requirements to the security functions presented in the *2in1 PC™ Functional Specifications.*

Security Functional Requirements from ST	*2in1 PC™ Functional Specification* References
FDP_ACC.1	3 – State Machine, 4 – Provide different MBRs, 5 – Control Access to Disk Partitions, 6 – Control Access to Networks, 7 – Control State Changes, 9 – Monitor Floppy Disk Usage in Transition state, & 10 – Control Access to External Devices
FDP_ACF.1	3 – State Machine, 4 – Provide different MBRs, 5 – Control Access to Disk Partitions, 6 – Control Access to Networks, 7 – Control State Changes, 9 – Monitor Floppy Disk Usage in Transition state, & 10 – Control Access to External Devices
FDP_ITC.1	3 – State Machine, 5 – Control Access to Disk Partitions, 6 – Control Access to Networks, & 10 – Control Access to External Devices
FIA_UID.2	11 – Detect the Set-up Plug
FMT_MSA.1	1 – Set-up & Configuration & 2 – Storage for Configuration Data
FMT_MSA.3	1 – Set-up & Configuration & 2 – Storage for Configuration Data
FMT_SMR.1	11 – Detect the Set-up Plug
FMT_SMR.3	11 – Detect the Set-up Plug
FPT_FLS.1	3 – State Machine, 4 – Provide different MBRs, 5 – Control Access to Disk Partitions, 6 – Control Access to Networks, 7 – Control State Changes, & 10 – Control Access to External Devices
FPT_RCV.4	3 – State Machine, 4 – Provide different MBRs, 5 – Control Access to Disk Partitions, 6 – Control Access to Networks, 7 – Control State Changes, & 10 – Control Access to External Devices
FPT_RVM.1	All
FPT_SEP.3	All

Table 9.2.4.3.5-1 Security Functional Requirements to Functional Specification Mapping

The TSF does not provide any error or success indicators back to the end user except for indications of state change. Operations permitted by the TSF are allowed to occur.

Prohibited operations (e.g., read from a disk address outside the user's allowed partitions) are not allowed to pass through the TSF to the hard disk, and no indication of success or failure, and no data, are passed back to the user. The user visible indication of state information is not trusted, so state change information presented to the user is also not trusted. Regardless of what state the user thinks the TOE is in, the TSF enforces the security policy for the actual state of the state machine.

9.2.4.6 Functional Specification Evidence

The following additional documentation was reviewed during the analysis of the functional specification:

- *Voltaire 2in1 PC™ Security Target Report*
- E21198006, *2in1 PC™ Administrative Rights*
- E21198021, *2in1 PC™ Hardware Failure*
- E21198035, *2in1 PC™ Informal Security Policy Model*
- E21198046, *2in1 PC™ User Guide*
- E21198047, *2in1 PC™ Mapping of Assurance Elements*
- E21198063, *2in1 PC™ Installation Guide*
- E21198064, *2in1 PC™ Quick Installation Guide*

9.2.5 ADV_HLD.1 Descriptive High-Level Design

9.2.5.1 Evidence Elements

This section addresses the high-level design of the TOE, provides a description of the TSF in terms of major structural units (i.e. subsystems), and relates these units to the functions that they provide. For each subsystem of the TSF, the high-level design describes every function, the purpose of each function, and identifies the security functions contained in the subsystem. The interrelationships of all subsystems are also defined in the high-level design. These interrelationships are represented as external interfaces for data flow, control flow, etc., as appropriate.

9.2.5.2 Documentation Included in the High-Level Design

The following documentation was considered a part of the high-level design for the TOE:

- E21198024, *2in1 PC™ System Design Document*
- E21198061, *2in1 PC™ Updates to the SYD EEPROM Mapping Section*
- E21199066, *2in1 PC™ Addendum to the System Design Document – High-Level Design*

9.2.5.3 Evaluator Action Elements and Findings

9.2.5.3.1 Informal High-Level Design

The TOE satisfies this element. The high-level design is in an informal style, written in English.

9.2.5.3.2 Internal Consistency

The TOE satisfies this element. The high-level design is internally consistent. It contains no contradictory statements. The initial documentation, the *2in1 PC™ System Design Document*, is incomplete, sometimes vague, and has a few errors in it. These problems have been corrected with supplemental documentation provided by the developer, primarily the *Addendum to the 2in1 PC™ System Design Document – High Level Design*. The Addendum is consistent with the *2in1 PC™ System Design Document*, and adds more detail.

9.2.5.3.3 Structure of the TSF in Terms of Subsystems

The TOE satisfies this element. The high-level design is described in terms of blocks. There are four blocks described in the high-level design. They are the Main Block, IDE Block, EEPROM Block, and the State Machine Block. Each of the blocks implements a part, or all, of the functions described in the functional specifications. The number and composition of the blocks is appropriate for the security functionality provided by the TOE. The functional decomposition into subsystems, and their descriptions, provided in the high-level design is sufficient to provide a high-level understanding of design of the TSF. (Ref. *2in1 PC™ System Design Document*, Section 4; *Addendum to the 2in1 PC™ System Design Document – High-Level Design*; and *2in1 PC™ Functional Specifications*.)

9.2.5.3.4 Security Functionality Provided by Each Subsystem of the TSF

The TOE satisfies this element. The high-level design provides a description of the functional behavior of each of the four blocks. The following sections describe the blocks.

9.2.5.3.4.1 Main Block

The Main Block provides the external interface to the entire card. All external inputs and outputs are channeled through the Main Block. Other blocks deal with externally visible inputs and outputs, but they all pass through the Main Block. The other primary security functions of the Main Block are:

- Manage security arbitration – allow or disallow IDE disk commands based on the results of determinations made by the IDE Block (Function 5) and open and close electro-mechanical relays that control access to network connections (Function 6) and external devices (Function 10) based on mode and state information from the State Machine Block. (Ref. *2in1 PC™ System Design Document*, Section 4.2.1;

Addendum to the 2in1 PC™ System Design Document – High-Level Design, Main Block, Sections 3.1, 3.5, and 3.6; and *2in1 PC™ Functional Specifications.*)

- Manage the reset mechanism – Monitor the IDE and ISA buses for any of the possible reset signals or commands. When a reset is received, the Main Block notifies the State Machine Block (Function 7). (Ref. *2in1 PC™ System Design Document*, Section 4.2.1; *Addendum to the 2in1 PC™ System Design Document – High-Level Design*, Main Block, Sections 3.3 and 3.4; and *2in1 PC™ Functional Specifications.*)

9.2.5.3.4.2 IDE Block

The IDE Block monitors IDE bus activity. The IDE Block looks for four specific conditions on the IDE bus and acts accordingly.

First, it looks for a read MBR (0,0,1). When a read MBR has been detected, the IDE Block signals the EEPROM Block of the occurrence (Function 4). This process is functional only in work mode. When the TOE is in set-up mode, the MBR at physical disk location 0,0,1 (normally the MBR for the A partition) is used. (Ref. *2in1 PC™ System Design Document*, Section 4.2.3; *Addendum to the 2in1 PC™ System Design Document – High-Level Design*, IDE Block, Section 3.1; and *2in1 PC™ Functional Specifications.*)

The IDE Block also looks for 2in1 PC™ commands. When the "SWITCH" command is detected, the IDE Block notifies the State Machine Block (Function 7). (Ref. *2in1 PC™ System Design Document*, Section 4.2.3; *Addendum to the 2in1 PC™ System Design Document – High-Level Design*, IDE Block, Section 3.1; and *2in1 PC™ Functional Specifications.*)

When a read or write command to the EEPROM is detected, the IDE Block notifies the EEPROM Block (Functions 1 and 2). (Ref. *2in1 PC™ System Design Document*, Section 4.2.3; *Addendum to the 2in1 PC™ System Design Document – High-Level Design*, IDE Block, Section 3.1; and *2in1 PC™ Functional Specifications.*)

The IDE Block also looks for any I/O command for the disk (Function 5). When a disk I/O command is detected, the IDE Block compares the disk address provided with the disk boundary addresses for the different disk partitions. Then, based on the current machine state provided by the State Machine Block and partition boundary information provided by the EEPROM block, the IDE Block does the following checks and resulting notifications:

1. Is the disk address within the partition associated with the current state or within the Functional partition?
   a. If not, signal the Main Block to block the command.
   b. Otherwise, is the access type (i.e., read or write) authorised for that partition by the current machine state?

1) If so, signal the Main Block to let the command pass.
2) Otherwise, signal the Main Block to block the command.

(Ref. *2in1 PC™ System Design Document*, Section 4.2.3; *Addendum to the 2in1 PC™ System Design Document – High-Level Design*, IDE Block, Sections 3.1 and 3.2; and *2in1 PC™ Functional Specifications.*)

9.2.5.3.4.3 EEPROM Block

The primary function of the EEPROM Block is to store and retrieve security and configuration parameters and attributes for the TOE (Functions 1 and 2). The EEPROM Block functions differently in set-up mode than in work mode.

In set-up mode, the EEPROM Block write enables the EEPROM chip. This allows the input and storage of the security and configuration parameters and attributes that are maintained on the EEPROM chip. Vendor supplied utilities are provided to support the set-up of parameters and attributes, but that software is outside the TSC.

Table 9.2.5.3.4-1 shows the information stored on the EEPROM that is configurable by the administrator or determined by the set-up software.

Attribute	Allowable Values	Default	Set By*	Discussion
Power On Mode	A, B, Ta, Tb**	Ta	Adm	The administrator may select the initial user state. The installation software allows only Ta or Tb.
Access to T disk partition in T	R – Read Only R/W – Read & write	R	Adm	Access policy for the T disk partition while in T.
Access to Functional disk partition in B	N – No access R – Read Only R/W – Read & write	R/W	Adm	Access policy for the Functional disk partition while in B.
Access to Functional disk partition in A	N – No access R – Read Only R/W – Read & write	R	Adm	Access policy for the Functional disk partition while in A.
Slave disk usage	A or B	A	Adm	The second disk, if present, may be accessible in either state A or B, not both.
Reset signal	IDE reset ISA 64	ISA 64	Inst	There are two ways to detect a reset on a PC – by detecting the actual associated electrical activity on the ISA or IDE bus, or by monitoring the CPU reset command itself (out 64, FE). As certain PCs don't display the aforementioned bus electrical activity during reset, the only way to verify a reset on them is to monitor the CPU reset command.

Table 9.2.5.3.4-1 Administrator Dependent Attributes and Parameters

Attribute	Allowable Values	Default	Set By*	Discussion
Forced power off	E – Enabled D – Disabled	D	Adm	2in1 PC™ installation disk software (not a part of the TSF) provides for the clearing of RAM during state transition. Some local policies may also require the PC to cycle through power off to ensure that all volatile memory is cleared.
2in1 PC™ /NET mode	2in1 PC™ 2in1 NET	PC	Adm	There are currently two different 2in1 products available from Voltaire, 2in1 PC™ and 2in1 NET. These products share a great deal of their design and implementation. This bit allows the identification of the product. NOTE: The evaluated version is only 2in1 PC™ .
Functional partition start address	Logical and physical disk addresses	N/A	Inst	This is the start address of the Functional disk partition given in both LBA and physical formats. It is the last partition on the disk and the end of the disk is the end of the Functional partition.
Disk characteristics	Heads/Cylinder Sectors/Head	N/A	Inst	Default geography of the disk – sectors/head and heads/cylinder.
Disk partition start and end addresses for A, B, and T	Logical and physical disk addresses	N/A	Inst	These are the start and end addresses for the A, B, and T disk partitions given in both LBA and physical formats.
Installation signature	"2in1 PC™ "	N/A	Inst	This is used to verify that the EEPROM is not blank.
Installation version	Installation software version number	N/A	Inst	Used for upgrades to the installation software.
Installation unique number	Globally Unique Identifier (GUID)	N/A	Inst	A value assigned to bind the disk and the 2in1 PC™ card together.
Data CRC32	CRC of the EEPROM.	N/A	Inst	Used to verify the integrity of the EEPROM.
Install state	C – Completed I – In progress	C	Inst	There is a reboot required during the set-up process. This flag indicates the status of the set-up (i.e., before or after the reboot).
Stash BIOS cylinder	Physical cylinder address	N/A	Inst	Location of the backup of the EEPROM. This is located between partitions and is not accessible. ***

Table 9.2.5.3.4-1 Administrator Dependent Attributes and Parameters (Cont.)

Attribute	Allowable Values	Default	Set By*	Discussion
MBRs for A, B, and T	Boot loader and system tables.	N/A	Inst	These are the actual MBRs to be used for booting from the A, B, and T disk partitions.

* Adm means specifically set by the administrator. Inst means the value is determined by the set-up software, depending on administrator selected parameters.
** Ta and Tb are the Transition state where the next state has been identified as A or B, respectively.
*** The stash is a mirror image of the EEPROM that is saved to facilitate recovery from a damaged or malfunctioning 2in1 PC card. It has no security function. Without this information, much of the data on the hard disk would be difficult to recover and my be completely lost, in the event of a failure. The stash resides in a gap between partitions, and therefore is never accessible in WORK mode (when you're in partition A it is above your highest accessible sector, when you're in T and B, it's below your lowest accessible sector). The "Stash BIOS cylinder" item in the EEPROM is the address of the cylinder in which the stash is located. It's used to assist in locating the stash when it needs to be updated (and not having to sequentially search the entire disk for it - a lengthy process).

Table 9.2.5.3.4-1 Administrator Dependent Attributes and Parameters (Cont.)

(Ref. *2in1 PC™ System Design Document*, Section 4.2.4 and Appendices A and B; *Addendum to the 2in1 PC™ System Design Document – High-Level Design*, EEPROM Block, Sections 3.1 and 3.3; and *2in1 PC™ Functional Specifications*.)

When the IDE Block notifies the EEPROM Block that a read MBR has been detected, and based on machine state obtained from the State Machine Block, the EEPROM Block provides MBR data appropriate for that state, to the IDE bus (Function 4). This provides the capability to boot the operating system from the appropriate disk partition for the machine state. For example, when the TOE transitions into state A, the system is booted from the A partition. (Ref. *2in1 PC™ System Design Document*, Section 4.2.4; *Addendum to the 2in1 PC™ System Design Document – High-Level Design*, EEPROM Block, Sections 3.2 and 3.4; and *2in1 PC™ Functional Specifications*.)

The IDE Block also responds to requests for data both internal to the TSF and to external sources. External requests for EEPROM data come through the IDE Block (Function 2). (Ref. *2in1 PC™ System Design Document*, Section 4.2.4; *Addendum to the 2in1 PC™ System Design Document – High-Level Design*, EEPROM Block, Section 3.2; and *2in1 PC™ Functional Specifications*.)

9.2.5.3.4.4 State Machine Block

The State Machine Block provides the state machine for the TOE. It controls and maintains both the mode (i.e., set-up or work) and the state (i.e., A, B, or T) of the TOE.

When the system (i.e., PC and TOE) is powered-on, the State Machine Block checks the set-up pins for the presence of a set-up plug. If the set-up plug is detected, the TOE is put into set-up mode (Function 11). In set-up mode, the machine states (i.e., A, B, and T) do not apply, and that part of the state machine is not active. (Ref. *2in1 PC™ System Design Document*, Section 4.2.2; *Addendum to the 2in1 PC™ System Design Document – High-Level Design*, State Machine Block, Section 3.1; and *2in1 PC™ Functional Specifications*.)

When the TOE is not in set-up mode, it is in work mode. In work mode, the machine states (i.e., A, B, and T) are maintained by the state machine (Functions 3 and 7). A change of machine state requires two specific events to occur. First, a "SWITCH" command must be received from the IDE block. The next state is determined based on the current machine state, an internal flag that indicates the next user state, and the direction of the switch (i.e., switching from A or from B). The state will actually change when the next reset signal is received from the Main Block. (Ref. *2in1 PC™ System Design Document*, Section 4.2.2; *Addendum to the 2in1 PC™ System Design Document – High-Level Design*, State Machine Block, Sections 3.4 and 3.5; and *2in1 PC™ Functional Specifications*.) There are three conditions that may prevent state switching, depending on the administrator defined and configured options. They are:

1. Forced Shutdown – There is an administrator selectable option that requires a full, hard boot, between user states (i.e., A and B). When this option is selected, only one state transition is allowed (e.g., T –> A or T –> B) before state switching is disabled (Function 7). When the State Machine Block determines that it was a hard boot (i.e., power-on), a flag is cleared to indicate initial state. The first power-on state is determined from configuration information obtained from the EEPROM Block (bits 1-2 of the first word on the EEPROM chip). At the next reset signal, the flag will be set, indicating that the one allowed switch has taken place. No additional state switches will be honored after the flag is set. (Ref. *2in1 PC™ System Design Document*, Section 4.2.2; *Addendum to the 2in1 PC™ System Design Document – High-Level Design*, State Machine Block, Sections 3.2, 3.4 and 3.6; and *2in1 PC™ Functional Specifications*.)

2. DMA2 (DRQ2) Activity – There is an administrator selectable option that prevents the state machine from leaving the transition (T) state if any DMA2 activity has been detected during that state (Function 9). DMA2 (DRQ2) activity is generally associated with the floppy disk. (Note: There is a possibility that DMA2 could be associated with another device (e.g., sound card). If that were to occur, switching would also be prevented by access to the sound card, and would still not violate the security policy.) This detection is performed by the DMA controller receiving DMA2 activity from the ISA bus only. Since PCI devices do not interface with the DMA controller, their operation is not monitored by the TSF. When DMA2 activity is detected during the Transition state, the system (PC & TOE) must be rebooted, through Transition state again, without any further DMA2 activity, before it is allowed to continue on to a user state (i.e., A or B). (Ref. *2in1 PC™ System Design Document*, Section 4.2.2; *Addendum to the 2in1 PC™ System Design Document – High-Level Design*, State Machine Block, Sections 3.3 and 3.4; and *2in1 PC™ Functional Specifications*.)

3. Switch Disable – There are jumper pins (i.e., 17-18) on the 2in1 PC™ card that may disable switching. As long as a signal is asserted (i.e., +5v) on these pins, switching is disabled (Function 7). This feature was included in the TOE to provide an optional, external device, such as a biometric I&A device, to be used

to restrict a user's ability to gain access to one, or more, of the machine's three states. Any such device is outside of the TSC. (Ref. *2in1 PC™ System Design Document,* Section 4.2.2; *Addendum to the 2in1 PC™ System Design Document – High-Level Design,* State Machine Block, Section 3.8; and *2in1 PC™ Functional Specifications.*)

In some older PCs, software generated resets do not send a reset signal on either the ISA or IDE busses. Such a reset signal is required by the TOE to verify that a reboot occurred. In such cases, an optional reset jumper must be connected from the reset pins (i.e., pins 13-14) to the PC motherboard's reset pins (Function 7). (Ref. *2in1 PC™ System Design Document,* Section 4.2.2; *Addendum to the 2in1 PC™ System Design Document – High-Level Design,* State Machine Block, Section 3.4; and *2in1 PC™ Functional Specifications.*)

9.2.5.3.5 Underlying Hardware, Firmware, and/or Software

This element is satisfied because the *Voltaire 2in1 PC™ Security Target Report* contains no IT security requirements on the IT environment. (See Section 4.3.)

9.2.5.3.6 Identify All Interfaces to the Subsystems

The TOE satisfies this element. The *2in1 PC™ High-Level Design* provides the required information on the internal and external interfaces to the four blocks. Table 9.2.5.3.6-1 identifies each of the security relevant interfaces to the blocks and shows which are internal and which are external.

Block	Internal Interfaces	Externally Visible Interfaces
Main Block	IDE Block – Allow/disallow signals for disk I/O EEPROM Block – Configuration data State Machine Block – Machine state, Machine mode, Reset notification	IDE Bus (PC) – Reset signals, Hard disk I/O commands IDE Bus (Disk) – Hard disk I/O commands ISA Bus – Reset signals and commands Electro-mechanical relays – Network connectivity Electro-mechanical relays – External device connectivity Jumper pins – External devices
IDE Block	Main Block – Hard disk I/O commands, Allow/disallow signals for disk I/O EEPROM Block – Configuration data, Read MBR notice, Read/write EEPROM commands State Machine Block – Machine state, Machine mode, Switch command	IDE Bus (PC) – Hard disk I/O commands

Table 9.2.5.3.6-1 Interfaces to the Blocks

Block	Internal Interfaces	Externally Visible Interfaces
EEPROM Block	Main Block – Configuration data IDE Block – Configuration data, Read MBR notice, Read/write EEPROM commands State Machine Block – Configuration data, Machine state, Machine mode	IDE Bus (PC) – Read & write requests
State Machine Block	Main Block – Machine state, Machine mode, Reset notification IDE Block – Machine state, Machine mode, Switch command EEPROM Block – Configuration data, Machine state, Machine mode	ISA Bus – DMA2 activity IDE Bus – State indicator Set-up Pins/Plug – Set-up/work mode Jumper Pins – Switch Disable, State indicator, Reset signal

Table 9.2.5.3.6-1 Interfaces to the Blocks (Cont.)

9.2.5.3.7 Accurate and Complete Instantiation of the TOE Security Functional Requirements

The TOE satisfies this element. The security functions in the functional specification are accurately and completely represented in the high-level design. Table 9.2.5.3.7-1 shows the mapping from functional specifications to high-level design. It further shows, for each function, to which block it is primarily allocated and other blocks that provide supporting functionality. Table 9.2.5.3.7-2 shows the reverse mapping, from high-level design to functional specifications. It demonstrates that each of the blocks provides support for several functions.

	High-Level Design	
Functional Specification	**Primary**	**Support**
1 – Set-up & Configuration	EEPROM Block	IDE Block
2 – Storage for Configuration Data	EEPROM Block	IDE Block
3 – State Machine	State Machine Block	
4 – Provide different MBRs	EEPROM Block	IDE Block
5 – Control Access to Disk Partitions	IDE Block	Main Block
6 – Control Access to Networks	Main Block	
7 – Control State Changes	State Machine Block	Main Block and IDE Block
8 – N/A (see note)		
9 – Monitor Floppy Disk Usage in Transition state	State Machine Block	
10 – Control Access to External Devices	Main Block	
11 – Detect the Set-up Plug	State Machine Block	
Note: This function is not within the TSC.		

Table 9.2.5.3.7-1 Mapping of Functional Specification to High-Level Design

High-Level Design	Functional Specification
Main Block	5 – Control Access to Disk Partitions, 6 – Control Access to Networks, 7 – Control State Changes, and 10 – Control Access to External Devices
IDE Block	1 – Set-up & Configuration , 2 – Storage for Configuration Data, 4 – Provide different MBRs, 5 – Control Access to Disk Partitions, and 7 – Control State Changes
EEPROM Block	1 – Set-up & Configuration , 2 – Storage for Configuration Data, 4 – Provide different MBRs
State Machine Block	3 – State Machine, 7 – Control State Changes, 9 – Monitor Floppy Disk Usage in Transition state, and 11 – Detect the Set-up Plug

Table 9.2.5.3.7-2 Mapping of High-Level Design to Functional Specification

9.2.5.4 High-Level Design Evidence

The following additional documentation was reviewed during parts of the analysis of the High-Level Design:

- *Voltaire 2in1 PC™ Security Target Report*
- E21198047, *2in1 PC™ Mapping of Assurance Elements*
- E21298054, *2in1 PC™ Functional Specifications*

9.2.6 ADV_RCR.1 Informal Correspondence Demonstration

9.2.6.1 Evidence Elements

This section addresses the correspondence between the various TSF representations. These representations include the TOE summary specification, functional specification, and high-level design. A correct and complete instantiation of the requirements to the least abstract TSF representation is also provided. This conclusion is achieved by step-wise refinement and the cumulative results of correspondence determinations between all adjacent abstractions of representation.

9.2.6.2 Evaluator Action Elements and Findings

9.2.6.2.1 Correspondence Demonstration

The TOE satisfies this element. The TOE Summary Specification, provided in *Voltaire 2in1 PC™ Security Target Report*, is directly derived from the 2in1 PC™ functional specification. The mappings presented in this section were taken from *the 2in1 PC™ Mapping of Assurance Elements.* Table 9.2.6.2.1-1 shows the mapping between the TOE Summary Specification and the functional specification.

Functions	Functional Specification
SET-UP	1 – Set-up & Configuration
STORE	2 – Storage for Configuration Data
STATE	3 – State Machine
BOOT	4 – Provide different MBRs
AC_DISK	5 – Control Access to Disk Partitions
AC_NW	6 – Control Access to Networks
CHANGE	7 – Control State Changes
FLOPPY	9 – Monitor Floppy Disk Usage in Transition state
AC_DEV	10 – Control Access to External Devices
MODE	11 – Detect the Set-up Plug

Table 9.2.6.2.1-1 Functions to Security Functional Requirements Mapping

Table 9.2.6.2.1-2 shows the mapping of the security functional requirements from the ST to the security functions presented in the *2in1 PC™ Functional Specifications.*

Security Functional Requirements	*2in1 PC™ Functional Specification* References
FDP_ACC.1	3 – State Machine, 4 – Provide different MBRs, 5 – Control Access to Disk Partitions, 6 – Control Access to Networks, 7 – Control State Changes, 9 – Monitor Floppy Disk Usage in Transition state, & 10 – Control Access to External Devices
FDP_ACF.1	3 – State Machine, 4 – Provide different MBRs, 5 – Control Access to Disk Partitions, 6 – Control Access to Networks, 7 – Control State Changes, 9 – Monitor Floppy Disk Usage in Transition state, & 10 – Control Access to External Devices
FDP_ITC.1	3 – State Machine, 5 – Control Access to Disk Partitions, 6 – Control Access to Networks, & 10 – Control Access to External Devices
FIA_UID.2	11 – Detect the Set-up Plug
FMT_MSA.1	1 – Set-up & Configuration, & 2 – Storage for Configuration Data
FMT_MSA.3	1 – Set-up & Configuration, & 2 – Storage for Configuration Data
FMT_SMR.1	11 – Detect the Set-up Plug
FMT_SMR.3	11 – Detect the Set-up Plug
FPT_FLS.1	3 – State Machine, 4 – Provide different MBRs, 5 – Control Access to Disk Partitions, 6 – Control Access to Networks, 7 – Control State Changes, & 10 – Control Access to External Devices
FPT_RCV.4	3 – State Machine, 4 – Provide different MBRs, 5 – Control Access to Disk Partitions, 6 – Control Access to Networks, 7 – Control State Changes, & 10 – Control Access to External Devices
FPT_RVM.1	All
FPT_SEP.3	All

Table 9.2.6.2.1-2 Security Functional Requirements to Functional Specification Mapping

Table 9.2.6.2.1-3 shows the mapping of functional specifications to high-level design. It further shows, for each function, to which block it is primarily allocated and other blocks that provide supporting functionality. Table 9.2.6.2.1-4 shows the reverse mapping, from high-level design to functional specifications. It demonstrates that each of the blocks provides support for several functions.

Functional Specification	High-Level Design (Primary)	High-Level Design (Support)
1 – Set-up & Configuration	EEPROM Block	IDE Block
2 – Storage for Configuration Data	EEPROM Block	IDE Block
3 – State Machine	State Machine Block	
4 – Provide different MBRs	EEPROM Block	IDE Block
5 – Control Access to Disk Partitions	IDE Block	Main Block
6 – Control Access to Networks	Main Block	
7 – Control State Changes	State Machine Block	Main Block and IDE Block
8 – N/A (see note)		
9 – Monitor Floppy Disk Usage in Transition state	State Machine Block	
10 – Control Access to External Devices	Main Block	
11 – Detect the Set-up Plug	State Machine Block	
Note: This function is not within the TSC.		

Table 9.2.6.2.1-3 Mapping of Functional Specification to High-Level Design

High-Level Design	Functional Specification
Main Block	5 – Control Access to Disk Partitions, 6 – Control Access to Networks, 7 – Control State Changes, and 10 – Control Access to External Devices
IDE Block	1 – Set-up & Configuration , 2 – Storage for Configuration Data, 4 – Provide different MBRs, 5 – Control Access to Disk Partitions, and 7 – Control State Changes
EEPROM Block	1 – Set-up & Configuration , 2 – Storage for Configuration Data, 4 – Provide different MBRs
State Machine Block	3 – State Machine, 7 – Control State Changes, 9 – Monitor Floppy Disk Usage in Transition state, and 11 – Detect the Set-up Plug

Table 9.2.6.2.1-4 Mapping of High-Level Design to Functional Specification

9.2.6.3 Informal Correspondence Evidence

The following additional documentation was reviewed during the analysis of the Informal Correspondence Demonstration:

- *Voltaire 2in1 PC™ Security Target Report*
- E21198024, *2in1 PC™ System Design Document*
- E21298054, *2in1 PC™ Functional Specifications*
- E21198061, *2in1 PC™ Updates to the SYD EEPROM Mapping Section*
- E21199066, *2in1 PC™ Addendum to the System Design Document – High-Level Design*

9.2.7 ADV_SPM.1 Informal TOE Security Policy Model

9.2.7.1 Evidence Elements

This section addresses the informal TOE security policy model. This model is defined in a consistent manner and fully describes the TSP rules, characteristics, and provides a correspondence between the TSP and the functional specification. This correspondence demonstrates that all of the security functions defined in the functional specification are consistent and complete with respect to the TSP model.

9.2.7.2 Evaluator Action Elements and Findings

9.2.7.2.1 Informal TSP Model

The TOE satisfies this element. The security policy model is in an informal style, written in English and includes tables and explanatory text.

9.2.7.2.2 Description of Rules and Characteristics

A security policy model is required by the inclusion of the FPT_FLS.1, Failure with Preservation of Secure State, and FPT_RCV.4, Function Recovery, security functional requirements. For that purpose, only the definition of a "secure state" need be made. However, for reasons of clarity and completeness, the vendor has chosen to also include access control, I&A, and floppy disk switching policies.

The TOE satisfies this element. The ST identifies two access control TSPs in the FDP_ACC.1 and FDP_ACF.1 security functional requirements, the Partitioning Access Policy and the Administrator Access Policy. Both of these access policies are represented in the *2in1 PC™ Informal Security Policy Model.*

The four security policies modeled in the *2in1 PC™ Informal Security Policy Model* are fully described in Section 3 of this report. Both access control models clearly state the rules to be enforced by identifying the subjects, objects, and operations to which they apply. The I&A and floppy disk switching policy models also clearly state the rules to be enforced.

9.2.7.2.3 Consistent and Complete Model

The TOE satisfies this element. Three of the policies modeled, the Administrator Access Policy, the Identification and Authentication Policy, and the Floppy Disk Switching Policy are relatively simple policies with trivial models. The Identification and Authentication Policy states that once the set-up plug is installed on the 2in1 PC™ card and the PC has been powered on, the user has assumed the administrator role. Otherwise he is a user. The Administrator Access Policy states that if a user is acting in the administrator role, they may have write access to the EEPROM. Otherwise he may not. The Floppy Disk Switching Policy states that, once DMA2 activity has been detected in Transition state, no further switching is permitted during the current session. Removing the floppy disk (if present) and rebooting the system can reset this condition. If any other device uses DMA2, it also can not be used during transition. The Partitioning Access Policy has a much more complex set of rules, and is more fully described below.

There are two modes of operation for the TOE, set-up and work. Each mode is directly coupled with a user role. All actions in set-up mode are in the administrator role. All actions in work mode are in the user role. Table 9.2.7.2.3-1 shows the effects of each of these modes/roles on the application or enforcement of each of the four security policies.

	Mode/Role	
Policy	**Set-up/Administrator**	**Work/User**
Partitioning Access	Exceptions apply *	Policy fully enforced
Administrator Access	Write access granted	Write access denied
Identification and Authentication	Administrator role	User role
Floppy Disk Switching	Does not apply	Policy fully enforced
* Exception rules are identified in Table 9.2.7.3-3.		

Table 9.2.7.2.3-1 Mode/Role Use By Policies

Enforcement of the Partitioning Access Policy is the primary purpose of the product. This policy controls access to disk partitions, network connections and other devices under it's control, depending on the current state of the state machine. Table 9.2.7.2.3-2 shows the rules for the Partitioning Access Policy. Exceptions are shown in Table 9.2.7.2.3-3.

	State A	State B	State T
Disk Partitions			
A	R/W	No access	No access
B	No access	R/W	No access
T	No access	No access	R
F	* (default R)	* (default R/W)	* (default No access)
Network Connections			
A	Connected	Not Connected	Not Connected
B	Not Connected	Connected	Not Connected
External Devices			
A	Connected	Not Connected	Not Connected
!A	Not Connected	Connected	Connected
B	Not Connected	Connected	Not Connected
!B	Connected	Not Connected	Connected
* Administrator selectable (R, R/W, or No access)			

Table 9.2.7.2.3-2 Partitioning Access Policy Rules

When the user is acting in the administrator role (i.e., they have entered set-up mode by installing the set-up plug on the 2in1 PC™ card and powering back on) there are exceptions to the Partitioning Access Policy. The rules that are applied under this exception are shown in Table 9.2.7.2.3-3.

Disk Partitions	Set-up Mode
A	Not monitored
B	Not monitored
T	Not monitored
F	Not monitored
Network Connections	
A	Not Connected
B	Not Connected

Table 9.2.7.2.3-3 Partitioning Access Policy Exception Rules

Other Interface	
A	Not Connected
!A	Connected
B	Not Connected
!B	Connected

Table 9.2.7.2.3-3 Partitioning Access Policy Exception Rules (Cont.)

In the Partitioning Access Policy, the Transition state is considered to be secure since it has no active network connections, no access to either A or B disk partitions, read only access to the Transition disk partition, and only has access to other controlled external devices connected through the !A (Not A) or !B (Not B) jumper pins. Access to the functional partition is an administrator selectable parameter. The TSF will assure that a PC with the 2in1 PC™ card correctly installed, and without the set-up plug installed on the card, that has been shut down for any reason will always boot up into, or through, the Transition state, where the environment is restricted and cannot be altered.

9.2.7.2.4 Correspondence Between TSP Model and Functional Specification

The TOE satisfies this element. The *2in1 PC™ Informal Security Policy Model* is fully represented in the *2in1 PC™ Functional Specification.* Identified functions implement the rules of each of the policies included in the model. The functional descriptions identify the same attributes and characteristics as found in the model. The policy descriptions are consistent with user and administrator guidance. Table 9.2.7.2.4-1 maps the Informal Security Policy Model to the Functional Specification.

Informal Security Policy Model	Functional Specification
Partitioning Access Policy	
Disk Partitions	5 – Control Access to Disk Partitions
Networks	6 – Control Access to Networks
Other Devices	10 – Control Access to External Devices
Partitioning Access Policy Exception	
Disk Partitions	11 – Detect the Set-up Plug
Networks	11 – Detect the Set-up Plug
Other Devices	11 – Detect the Set-up Plug
Administrator Access Policy	
EEPROM	1 – Set-up & Configuration & 11 – Detect the Set-up Plug
Identification and Authentication Policy	
Set-up Pins	11 – Detect the Set-up Plug
Floppy Disk Switching Policy	
Floppy Disk	9 – Monitor DMA2 Usage in Transition state

Table 9.2.7.2.4-1 Security Policy Model to Functional Specification Mapping

9.2.7.2.5 Informal Security Policy Model Evidence

The following documentation was reviewed during the analysis the Informal Security Policy Model:

- E21198035, *2in1 PC™ Informal Security Policy Model*
- E21298054, *2in1 PC™ Functional Specifications*

- E21198046, *2in1 PC™ User Guide*
- E21198063, *2in1 PC™ Installation Guide*
- E21198064, *2in1 PC™ Quick Installation Guide*

9.2.8 AGD_ADM.1 Administrator Guidance

9.2.8.1 Evidence Elements

This section presents the results of the evaluation of administrator guidance provided with the TOE. The administrator guidance is contained in the *2in1 PC™ Installation Guide* and is supplemented by *2in1 PC™ Application Notes.* The administrator function is invoked in the set-up mode through the use of an internal or external set-up plug as applicable.

9.2.8.2 Evaluator Action Elements and Findings

9.2.8.2.1 Describe Administrative Functions and Interfaces

The administrator guidance satisfies this element by providing a detailed overview of the TOE security functionality available to the administrator in the set-up mode (Ref. *2in1 PC™ Installation Guide*, Chapter 1). It also provides step-by-step set-up mode procedures, configuration settings, and descriptions of the necessary actions and expected results when using the appropriate keyboard or mouse inputs for the Windows 3.1/95/NT, and MS-DOS operating systems (Ref. *2in1 PC™ Installation Guide*, Chapter 3, Chapter 4, Chapter 5, Chapter 6, Chapter 9, Appendix B, Appendix C, and Appendix D).

9.2.8.2.2 Describe How to Administer the TOE in a Secure Manner

The administrator guidance satisfies this element by describing the required administrator actions and procedures while in the set-up mode with the set-up plug inserted and is consistent with the security management requirements specified in the *Voltaire 2in1 PC™ Security Target Report* (Ref. *2in1 PC™ Installation Guide*, Chapter 3, Chapter 4, Chapter 5, Chapter 6, Chapter 9, and Appendix D). Specifically:

- FMT_MSA.1 Management of Security Attributes
- FMT_MSA.3 Static Attribute Initialisation
- FMT_SMR.1 Security Roles
- FMT_SMR.3 Assuming Roles

9.2.8.2.3 Warnings About Functions and Privileges that Should Be Controlled

This element is satisfied because there are no user-accessible functions and privileges, i.e., running the 2in1 PC™ installation program, keeping or erasing existing data, configuring the 2in1 PC™ card, and completing the installation flow, (Ref. *2in1 PC™ Installation Guide*, Chapter 4) available to the user in the work mode (Ref. *2in1 PC™ Installation Guide*, Chapter 8). Consequently, there are no specific warnings about these

items. The administrator guidance does provide highlighted warnings and informational notes regarding the installation and configuration of the TOE (Ref. *2in1 PC™ Installation Guide*, Chapter 3, Chapter 4, Chapter 5, Chapter 6, Chapter 9, and Appendix D).

9.2.8.2.4 Assumptions Regarding User Behavior

This element is satisfied because the user is unable to access, modify, or otherwise affect the TOE security functions and privileges from the work mode. Consequently, the administrator guidance contains no assumptions regarding user behavior. Specific user behavior assumptions are contained in the *Voltaire 2in1 PC™ Security Target Report*, namely, that users recognise the need for a secure IT environment (A.E.USER-NEED).

9.2.8.2.5 Security Parameters Under the Control of the Administrator

The administrator guidance satisfies this element through the description of security parameters and their secure values as appropriate. The administrator controls parameters for the following functions (REF. *2in1 PC™ Installation Guide*, Chapter 4, Chapter 10, Appendix C, and Application Notes):

1. Configuring the 2in1 PC™
    a. Custom names for the state machines
    b. Disk space allocated to the A, B, and Functional partitions
    c. Size of A and/or B partitions
    d. Access to the Functional partition from the A, B, and Transition state machines
    e. Transition settings
        1) Power-up mode
    f. Advanced settings
        1) Reset signal
        2) Network mode
        3) Second hard drive
        4) Forced shutdown
2. Installing Special Software to the Transition Area
    a. Writing to the appropriate batch file
3. Installing a Reset Cable, if necessary
4. General Hardware Dependent Settings (Application Notes)
    a. BIOS Settings
    b. Hard Disk Settings
    c. Specific Platform Dependent Settings

9.2.8.2.6 Security-Relevant Events

The administrator guidance satisfies this element through detailed descriptions and procedures for security-relevant events. Specifically, the following events were examined to determine that the guidance described each type of security-relevant event relative to

the administrative functions that need to be performed, including the changing of entities under the control of the TSF (REF. *2in1 PC™ Installation Guide*, Chapter 4, Chapter 5, Chapter 6, Chapter 8, Chapter 9, Chapter 10, Appendix D, and Application Notes):

1. Changing to the 2in1 PC™ Set-up Mode
    a. Internal Set-up
    b. External Set-up
2. Configuring Your 2in1 PC™
3. Completing the Installation Flow
4. Installing Operating Systems
5. Installing 2in1 PC™ Drivers
6. Reconfiguring, Reinstalling or Removing the 2in1 PC™ Card
7. Installing Special Software or Re-installing an Operating System
8. Advanced Configurations
    a. Dual Disk Configuration
    b. Configuring an Extended Partition in Windows NT
9. Application Notes
    a. General Hardware Dependent Settings
    b. Chip Sets
    c. BIOS Settings
    d. Hard Disk Settings
    e. Specific Platform Dependent Settings

9.2.8.2.7 Consistency of Documentation

Administrator guidance contained in the *2in1 PC™ Installation Guide* and supplemented by *2in1 PC™ Application Notes* is consistent with other applicable deliverables and satisfies this element. The following documentation was reviewed in making the consistency analysis determination:

- *Voltaire 2in1 PC™ Security Target Report*
- E21298054(2), *2in1 PC™ Functional Specifications*
- E20598024, *2in1 PC™ System Design Document* (Section 3)
- E21298056, *Addendum to the 2in1 PC™ High Level Design –INSTALLATION Software*
- E21298058, *Addendum to the 2in1 PC™ High Level Design – The Transition partition*
- E21198046, *2in1 PC™ User Guide*
- E21198040(2), *2in1 PC™ Vulnerability Analysis*
- E20698006, *2in1 PC™ Administrative Rights*
- E20698007, *2in1 PC™ Security Policy*
- E21198035(2), *2in1 PC™ Informal Security Policy Model*
- E20598004, *2in1 PC™ Physical Data Security*

9.2.8.2.8 Security Requirements for the IT Environment

This element is satisfied because the *Voltaire 2in1 PC™ Security Target Report* contains no IT security requirements on the IT environment.

9.2.9 AGD_USR.1 User Guidance

9.2.9.1 Evidence Elements

This section presents the results of the evaluation of user guidance provided with the TOE. The user guidance is supplied with the TOE as a separate document (Ref. *Voltaire 2in1 PC™ User Guide*) and addresses only the functions available to the non-administrative user. The user is restricted to two basic actions, Switching and Data Transfer, as determined by the administrator during the installation of the TOE. As such, the user guidance only contains information relevant to these two functions.

9.2.9.2 Evaluator Action Elements and Findings

9.2.9.2.1 User Functions and interfaces

The user guidance satisfies this element by providing an overview of the TOE security functionality and describing the Switching and Data Transfer functions permitted to the user. It also provides a description of the necessary actions and expected results when using the appropriate keyboard or mouse inputs for the Windows 95/98/NT 4, Windows 3.11/NT 3.51, MS-DOS, and Linux/SCO operating systems. (Ref. *Voltaire 2in1 PC™ User Guide*)

9.2.9.2.2 Use of User Functions

The user guidance satisfies this element by providing a description of the methods (e.g., menu selection, command line, or command button) and expected results for the functions available to the user.

The user is restricted to two basic functions when using the TOE. The Switching function enables the user to switch between the A and B machine states as required. The Data Transfer function is an option which allows the transfer of data from one machine state to another and will normally be only possible in one direction, e.g., data could be copied from machine state B to A but not from A to B. The configuration of the parameters for these functions is accomplished by the administrator during installation of the TOE and cannot be accessed or modified by the user. (Ref. *Voltaire 2in1 PC™ User Guide*)

9.2.9.2.3 Warnings About User Functions and Privileges

Parameters and privileges for the two user functions are configured by the administrator during installation of the TOE and cannot be accessed or modified by the user. Consequently, no warnings are required in the user guidance.

9.2.9.2.4 User Responsibilities

User responsibilities are not included in the user guidance because of the limited functions available to the user. Various aspects of user responsibilities are addressed in the *Voltaire 2in1 PC™ Security Target Report.* Specifically:

1. A.E.ACCESS – The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorised, physical access.

2. A.E.USER-NEED – Users recognise the need for a secure IT environment.

3. P.E.KNOWN – Users of the TOE must be identified and authenticated before TOE access can be granted.

4. P.E.USAGE – The organisation's IT resources must be used only for authorised purposes.

5. P.E.DUE-CARE – The organisation's IT systems must be implemented and operated in a manner that represents due care and diligence with respect to any risks to the organisation.

9.2.9.2.5 Consistency with Other Documentation

User guidance contained in the *Voltaire 2in1 PC™ User Guide* is consistent with other applicable deliverables and satisfies this element. The following documentation was reviewed in making the consistency analysis determination:

- *Voltaire 2in1 PC™ Security Target Report*
- E21298054(4), *2in1 PC™ Functional Specifications*
- E20598024, *2in1 PC™ System Design Document* (Section 3)
- E21298056, *Addendum to the 2in1 PC™ High Level Design –INSTALLATION Software*
- E21298058, *Addendum to the 2in1 PC™ High Level Design – The Transition partition*
- E21298063, *2in1 PC™ Installation Guide*
- E21198040(2), *2in1 PC™ Vulnerability Analysis*
- E20698006, *2in1 PC™ Administrative Rights*
- E20698007, *2in1 PC™ Security Policy*
- E21198035(4), *2in1 PC™ Informal Security Policy Model*

- E20598004, *2in1 PC™ Physical Data Security*

9.2.9.2.6 User Relevant Environmental Security Requirements

This element is satisfied because the *Voltaire 2in1 PC™ Security Target Report* contains no IT security requirements on the IT environment.

9.2.10 ATE_COV.1 Evidence of Coverage

9.2.10.1 Evidence Elements

This section presents the results of the test coverage evidence check for a mapping between the test documentation and the functional specification. Correspondence is presented in table format and includes both developer functional tests and independent lab tests. Specific test descriptions and results are contained in the *Evaluation Test Plan for the 2in1 PC™, Version 1.21.*

9.2.10.2 Evaluator Action Elements and Findings

9.2.10.2.1 Correspondence Between Tests and Functional Specification

This element has been satisfied through the evaluation of the developer functional tests and identifies the independent lab tests performed. Correspondence between tests and the functional specification is provided in Table 9.2.10.2.1-1. Developer tests are identified in Table 9.2.10.2.1-2. Independent lab tests are identified in Table 9.2.10.2.1-3.

Functional Specification	Developer Tests	Independent Tests
1) Allow the setting up and configuration of the 2in1 PC™ attributes.	VT12	ET01
2) Provide storage for configuration data (including card configuration and MBRs).	VT01	
3) In WORK mode, provide a state machine with three distinct states of operation: A, B and T (Transition).	VT13	ET02
4) In WORK mode, provide a different MBR for each security state during boot.	VT14	ET03
5) In WORK mode, control access to disk partitions based on the current security state and the access security policy.	VT05 VT06	ET04
6) In WORK mode, control access to networks based on the current security state and the access security policy.	VT02 VT04	
7) In WORK mode, control the flow of state changes.	VT11	ET02
8) Clear the PC's RAM during the Transition state.	VT15	See Note
9) In WORK mode, monitor access to the floppy disk during the Transition state and prevent state switching upon detection thereof.	VT07	ET05
10) In WORK mode, control access to external devices such as floppy drives and SCSI disks	VT10	ET06

Table 9.2.10.2.1-1 Correspondence of Developer and Independent Tests to Functional Specifications

Functional Specification	Developer Tests	Independent Tests
11) Detect the presence of a physical set-up plug in order to switch into Set-up mode and allow configuration.	VT03	ET01
Note: This function is not within the TSC.		

Table 9.2.10.2.1-1 Correspondence of Developer and Independent Tests to Functional Specifications (Cont.)

Developer Test ID	Element	Test to Confirm
VT01	EEPROM	The configuration data stored on the EEPROM is storable, editable and retrievable.
VT02	Electro-mechanical Relays	The 2in1 PC™ card supports the connection of two physically separated networks.
VT03	Set-up Plug	The EEPROM becomes writeable with the set-up plug placed on the 2in1 PC™ card. The card will allow full disk access with the set-up plug placed on it.
VT04	Network Connectors	For each user state, the network functions normally, as it would without the 2in1 PC™ card being installed.
VT05	Direct Disk Access (Via Interrupt 13)	Low-level disk editing utilities (e.g., Norton Disk Editor) that are based on BIOS Interrupt 13 are denied the ability to read/alter unauthorised disk partitions when the 2in1 PC™ is running in Work Mode.
VT06	Direct Disk Access (I/O Ports)	The 2in1 PC™ card will block the reading of unauthorised disk partitions when using low-level I/O port access.
VT07	Floppy Based Automatic Copying	The 2in1 PC™ card prevents the switch from Transition state upon detection of DMA2 activity.
VT08	IDE Connectors	The TOE does not introduce errors into the normal use of IDE drives.
VT09	Network Connectors	The 2in1 PC™ card does not introduce errors into the normal use of networks.
VT10	Floppy Disconnection Jumpers	External devices controlled by the 2in1 PC™ card will be inaccessible in the relevant states, and accessible in the other states.
VT11	Reset Cable	The 2in1 PC™ card (with the reset cable) provides a physical reset signal that is indicated on the ISA/IDE buses. The TOE does not switch if such a reset is not identified.
VT12	Software Diskettes	The installation diskettes allow the complete installation of the 2in1 PC™ card.
VT13	Altera Chip, Prom Chip	The 2in1 PC™ card provides a state machine with three distinct states and operates accordingly.
VT14	EEPROM Chip, Altera Chip, PROM Chip	The 2in1 PC™ card can provide a different MBRs for the relevant state.
VT15	PC RAM	During the Transition state, the PC's RAM is cleared.

Table 9.2.10.2.1-2 Identification of Developer Tests

Independent Test ID	Element	Test to Confirm
ET01	Set-up Plug	TOE can only be configured with the Set-up Plug installed.
ET02	2in1 PC™ Card Control Signals	The three states (A, B, and Transition) are reflected by hardware control signals.
ET03	Disk Partitions	The Master Boot Record (MBR) is different when booting into each of the three states.
ET04	Disk Partitions	Access to different partitions is limited
ET05	2in1 PC™ Card	The TOE will not switch the computer from the Transition state to an active state (A or B) if DMA2 activity is detected.
ET06	Floppy Diskette Disable Cable Control Connector	When using the Floppy Diskette Disable Cable, the floppy drive cannot be accessed without the Control Connector installed.

Table 9.2.10.2.1-3 Identification of Independent Tests

9.2.10.2.2 Test Coverage Evidence

The following documentation was reviewed in mapping between the test documentation and the functional specification. The test coverage check was primarily based on the *2in1 PC™ Functional Testing* and the *Evaluation Test Plan for the 2in1 PC™, Version 1.21* documents.

- CA1298006, *Evaluation Test Plan for the 2in1 PC™ , Version 1.21*
- E21298054(4), *2in1 PC™ Functional Specifications*
- E21198042(3), *2in1 PC™ Functional Testing*
- E20598019(2), *2in1 PC™ Install White Box Tests Sheet*
- E20598018(2), *2in1 Platform Tests Description*
- E21198038, *2in1 PC™ Operating System QA Test*
- E21198043(2), *2in1 PC™ Test Coverage*
- E20698036(3), *2in1 PC™ Hacking Tests*
- E21198040(2), *2in1 PC™ Vulnerability Analysis*

9.2.11 ATE_FUN.1 Functional Testing

9.2.11.1 Evidence Elements

This section presents the results of the evaluation of the developer's test documentation. The results of the evaluation of each document are summarised in table format in Section 9.2.11.2.3.

9.2.11.2 Evaluator Action Elements and Findings

9.2.11.2.1 Content of Test Documentation

Table 9.2.11.2.1-1 identifies the test documentation presented by the developer.

Document #	Title	Description
E20698036(3)	*2in1 PC™ Hacking Tests*	Describes tests performed to attempt to exploit 2in1 PC™ security.
E21198042(3)	*2in1 PC™ Functional Testing*	Describes the functional tests performed on the 2in1 PC™.
E21198043(2)	*2in1 PC™ Test Coverage*	Identifies tests performed to verify functional specifications.

Table 9.2.11.2.1-1 Vendor Test Documentation

9.2.11.2.2 Developer Test Documentation Examination

The developer's test documentation was checked and examined in accordance with the ATE_FUN.1C requirements identified in Section 9.2.11.1. Table 9.2.11.2.2-1, presents the results of the examination.

The ATE_FUN.1 evaluation elements presented in Table 9.2.11.2.2-1 are:

Identify Test Procedures:	ATE_FUN.1.1C
Expected Results:	ATE_FUN.1.1C
Actual Results:	ATE_FUN.1.1C
ID Security Functions to be Tested:	ATE_FUN.1.2C
Reproducible Initial Test Conditions:	ATE_FUN.1.2C
Reproducible Means to Stimulate Security Functions:	ATE_FUN.1.2C
ID Tests to be Performed:	ATE_FUN.1.3C
Successful Execution of the Test:	ATE_FUN.1.4C
Results are Consistent:	ATE_FUN.1.5C

Developer Test Document	Identify Test Procedures	Expected Results	Actual Results	ID Security Functions to be Tested	Reproducible Initial Test Conditions	Reproducible Means to Stimulate Sec Func	ID Tests to be Performed	Successful Execution of the Test	Results are Consistent
Hacking Tests	X	1	2	X	2	X	X	2	3
Functional Testing	X	X	X	X	X	X	X	X	X
Test Coverage	1	1	1	X	1	1	1	1	3
Legend: X = Adequate information provided. 2 = Insufficient detail provided. 1 = Information not provided. 3 = Unable to make determination.									

Table 9.2.11.2.2-1 ATE_FUN.1.1C Test Documentation Examination

9.2.11.2.3 Test Documentation Examination Results

The developer test documentation included a test plan in the *2in1 PC Functional Testing* document that provided sufficient information to fully satisfy the ATE_FUN.1 element. This document tested all of the security functions identified in the *2in1 PC Functional Testing*. Other vendor supplied test documentation (identified in Table 9.2.11.2.2-1) was

not used to satisfy the ATE_FUN.1 element since these documents did not provide the required content to test the TSF, however they were reviewed by the evaluators.

The *2in1 PC Functional Testing* document clearly identifies the test approach and goals in the introductory section and provides a detailed analysis near the end of the document. The content of this document was reviewed by the evaluators and a selection of tests was made to be verified in section 9.2.12 ATE_IND.2 Independent Testing – Sample. Furthermore, the *Evaluation Test Plan for the 2in1 PC™* was created to satisfy the ATE_IND.2 requirement. This document identifies the vendor tests that were selected and independent tests developed by the evaluators to confirm the TSF enforcement. These two test suites were identified by the evaluators to verify the validity of the developer's functional testing and provide correspondence to the functional specifications. Voltaire provided detailed test procedures for functional tests that could be replicated and verified by the evaluators, see Table 9.2.11.2.2-2. The second suite of tests was independently developed and performed by CAFÉ Lab evaluators, see Table 9.2.11.2.2-3. All of the test descriptions and results are contained in the *Evaluation Test Plan for the 2in1 PC™, Version 1.21*.

Developer Test ID	Element	Test to Confirm
VT01	EEPROM	The configuration data stored on the EEPROM is storable, editable and retrievable.
VT02	Electro-mechanical Relays	The 2in1 PC™ card supports the connection of two physically separated networks.
VT03	Set-up Plug	The EEPROM becomes writeable with the set-up plug placed on 2in1 PC™ card after the machine has been hard booted. The card will allow full disk access with the set-up plug placed on it.
VT04	Network Connectors	The network connection for each user state (A,B,& T) functions normally, as it would without the 2in1 PC™ card being installed.
VT05	Direct Disk Access (Via Interrupt 13)	Low-level disk editing utilities such as Norton Disk Editor that are based on BIOS Interrupt 13 are denied the ability to read / alter unauthorised disk partitions when the TOE is running in Work Mode.
VT06	Direct Disk Access (I/O Ports)	The 2in1 PC™ card will block the reading of unauthorised disk partitions when using low-level I/O port access when the TOE is running in Work Mode.
VT07	Floppy Based Automatic Copying	The 2in1 PC™ card prevents the switch from Transition state upon detection of DMA2 activity.
VT08	IDE Connectors	The TOE does not introduce errors into the normal use of IDE drives.

Table 9.2.11.2.2-2 Developer Tests

Developer Test ID	Element	Test to Confirm
VT09	Network Connectors	The 2in1 PC™ card does not introduce errors into the normal use of networks.
VT10	Floppy Disconnection Jumpers	External devices controlled by the 2in1 PC™ card will be inaccessible in the relevant states, and accessible in the other states.
VT11	Reset Cable	The 2in1 PC™ card (with the reset cable) provides a physical reset signal that is indicated on the ISA/IDE buses. The TOE does not switch if such a reset is not identified.
VT12	Software Diskettes	The installation diskettes allow the complete installation of the 2in1 PC™ card.
VT13	Altera Chip, Prom Chip	The 2in1 PC™ card provides a state machine with three distinct states and operates accordingly.
VT14	EEPROM Chip, Altera Chip, PROM Chip	The 2in1 PC™ card can provide a different MBRs for the relevant state.
VT15	PC RAM	During the Transition state, the PC's RAM is cleared.

Table 9.2.11.2.2-2 Developer Tests (Cont.)

Independent Test ID	Element	Test to Confirm
ET01	Set-up Plug	The TOE can only be configured with the Set-up Plug installed.
ET02	2in1 PC™ Card Control Signals	The three machine states (A, B, and Transition) are reflected by hardware control signals.
ET03	Disk Partitions	The Master Boot Record (MBR) is different when booting into each of the three machine states.
ET04	Disk Partitions	Access to disk partitions is limited.
ET05	2in1 PC™ Card	The TOE will not switch the computer from the Transition state to an active state (A or B) when DMA2 activity is detected.
ET06	Floppy Diskette Disable Cable Control Connector	The floppy drive can only be accessed with the Control Connector installed and the 2in1 PC™ card in the configured state.

Table 9.2.11.2.2-3 Independent Tests

9.2.12 ATE_IND.2 Independent Testing – Sample

9.2.12.1 Evidence Elements

This section addresses the independent testing performed by the evaluators. The testing has been broken down into two test suites that are defined in the *Evaluation Test Plan for 2in1 PC™, Version 1.2*. The first test suite defines the replicated vendor tests that verify the enforcement of the TSF, while the second test suite defines the independent tests performed by the evaluators to verify the enforcement of the TSF.

9.2.12.2 Evaluator Action Elements and Findings

9.2.12.2.1 TOE Suitable for Testing

The TOE evaluated in this element was configured in accordance with the stated security functions listed in the *2in1 PC™ Security Target.* The details of this configuration are given in Section 2.2 of the *Evaluation Test Plan for 2in1 PC™, Version 1.21.* Verification of the TOE's suitability for testing was performed in the following manner:

1. After receiving the TOE from the vendor (ref. 9.2.2 ADO_DEL.1 Delivery Procedures), verification of the configuration items was made. The details of this verification are located in Section 9.2.1 ACM_CAP.2 Configuration Items.

2. The TOE was installed using only the vendor supplied product documentation. The details of this installation process are located in Section 9.2.3 ADO_IGS.1 Installation, Generation, and Start-Up Procedures.

3. Resources used in the test were calibrated to ensure their proper operation. A listing of the test resources used for the TOE evaluation is located in Section 9.2.12.2.2 Equivalent Set of Resources, and also in Section 2 of the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

After the steps listed above were completed, the enforcement of the settings configured during the installation procedure was verified. Verification was made by testing the disk access privileges and network connectivity for the Secure (A) and Public (B) machine operating states. This was performed by creating a small text file, reading/writing the file to other disk partitions and sending it to other PCs connected to the Secure (A) and Public (B) network connections. Once this process was completed and the enforcement of the TOE configuration settings was verified, the TOE was found to be suitable to commence the vendor and evaluator tests defined in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

9.2.12.2.2 Equivalent Set of Resources

The set of resources used during the execution of the vendor tests performed included the following:

1. Twinbrook Systems, Intel 200Mhz Pentium-MMX – provided by the testing lab. Specific platform information is located in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

2. Fluke 75 Multi-meter – provided by the testing lab to evaluate the network connectors for test VT03 in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

3. llr.exe – source code was provided by the vendor and then compiled by the evaluation lab to test the low-level read access to the hard disk based on Cylinder,

Head, Sector (CHS) and Logic Block Addressing (LBA) schemes. This application was used in test VT06 located in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

4. rwe2.exe – source code was provided by the vendor and then compiled by the evaluation lab to test the read, write and execute permissions to the EEPROM on the 2in1 PC™ card. This application was used in tests VT01 and VT03 located in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

5. diskedit.exe (Norton) – provided by the vendor to read/write to specific addresses on the hard disk. This application was used in test VT05 (first and second sub-tests) located in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

The evaluators used the list of items above to verify the documented vendor test results. Most of the vendor performed tests were done so in a manner in which the scope was larger (i.e. factors outside of the TSC were relied upon for the test results). The scope of the independent tests on the other hand, relied strictly upon the 2in1 PC™ card itself and its' interfaces. Due to the differences in the scope, a subset of the vendor tests was replicated by the lab and the independent tests were used to verify the TOE security functions defined in the *2in1 PC™ Security Target.* The resources used in the independent tests included the following:

1. Twinbrook Systems, Intel 200Mhz Pentium-MMX – provided by the testing lab. Specific platform information is located in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

2. Innotec ID520 IDE Analyzer – provided by Voltaire. This device was used to in tests ET03 and ET04 located in the *Evaluation Test Plan for 2in1 PC™, Version 1.21* Plan.

3. Faxconn ISA Slot Extension Card – provided by Voltaire. This device was used in all of the independent tests to provide easy access to the 2in1 PC™ card components.

4. HP 545A Logic Probe – provided by Voltaire. This device was used in conjunction with the *2in1 PC™ Hardware Design* document to verify connections on the 2in1 PC™ card. This device was used in independent evaluator tests as identified in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

5. HP 1664A Logic Analyzer (50/100-MHz State/500-MHz Timing) – provided by the testing lab. This device was used in test ET02 located in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

6. diskedit.exe (Norton) – provided by the vendor to read/write to specific addresses on the hard disk. This application was used in tests ET03 and ET04 located in the *Evaluation Test Plan for 2in1 PC™, Version 1.21.*

The evaluators used the list of items above to execute the independent tests in order to evaluate the TOE at the interface level. The specific test details for the entire vendor and independent tests performed are presented in Appendix A, B and C of the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

Other applications installed on the system as part of the installation process (ref. 9.2.3 ADO_IGS.1 Installation, Generation, and Start-Up Procedures) were also used during the vendor and independent testing. These applications were:

1. sense.exe – provided by installed files that were loaded onto the PC from installation disk 1. This application enables the Administrator to verify that the configuration settings stored on the EEPROM have not been modified. A value is displayed in hexadecimal and reflects the current configuration settings, therefore any changes to the EEPROM's configuration will result in a different value being displayed. This application also displays the cards current working state (i.e. Secure (A), Public (B), or Transition).

2. report.exe – provided by installed files that were loaded onto the PC from installation disk 1. This application generates a report of the hard disk configuration (i.e. defining borders for each disk partition). This application works in conjunction with report.bat.

3. report.bat – provided by installed files that were loaded onto the PC from installation disk 1. This application executes report.exe and redirects the output to the display screen. This batch file was edited during the evaluation and renamed report2.bat so that the output could be redirected to a file for printing. The output of this file was used as a reference for other tests that were executed and is located after test VT02 in the *Evaluation Test Plan for 2in1 PC™, Version 1.21.*

9.2.12.2.3 Test a Subset of the TSF

The developer test documentation evidence was evaluated as to the relevance of the identified security functions to be tested (ref. 9.2.11 ATE_FUN.1 Functional Testing). The selection of the developer tests was based upon a requirement to verify developer functional testing (see Section 9.2.11.2.3 Describe Scenarios) and correspondence to the tests mapped to the *2in1 PC™ Functional Specification.* Once the test sample was selected, independent tests were developed to further evaluate the security functions that were addressed by the developer test documentation (ref. 9.2.11 ATE_FUN.1 Functional Testing). With the confirmation of developer tests and the independent tests performed by the evaluators, every security function within the TSC has been tested. For the details of the testing coverage, refer to Table 9.2.10.2.1-1 Correspondence of Developer and Independent Tests to Functional Specifications.

A selection of independent tests was also based on the identification of residual TOE vulnerabilities. After reviewing these vulnerabilities, the selection was made to be included as part of the independent tests. The specific details of these vulnerabilities are defined in Section 9.2.14 AVA_VLA.1, Developer Vulnerability Analysis.

The independent tests were performed at the IDE interface level using an IDE analyzer. This test method was selected to capture all of the IDE bus traffic on both the controller and hard disk side of the bus, thus allowing the ability to verify the card operated according to its' configured security state.

The identification and details for each of the evaluation tests performed is contained in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*.

The expected results for all of the tests performed in the *Evaluation Test Plan for 2in1 PC™, Version 1.21* were verified by the actual results. There were no inconsistencies between the expected result and the actual results.

9.2.12.2.4 Verify Test Results for a Sample of Tests

This element addresses the scope of the documented vendor tests and provides a rationale for the selection of specific vendor tests that were included in the *Evaluation Test Plan for 2in1 PC™, Version 1.21*. The details of these procedures were documented by the evaluators and are located in Appendix A of the *Evaluation Test Plan for 2in1 PC™, Version 1.21*. The following vendor tests were selected to confirm their actual results:

1. VT01 – States that the configuration data on the EEPROM is storable, editable and retrievable. This test was selected to verify that the configuration data stored on the EEPROM could only be modified while the card is in set-up mode.
   Actual Result: The expected result was verified.

2. VT02 – States that the 2in1 PC™ card supports the connection of two physically separated networks. This test was selected to verify:

   a. When the PC is running in the Transition machine state, all network connections are severed.
   b. When the PC is running in the Secure (A) machine state, connection is made to only the Secure (A) network.
   c. When the PC is running in the Public (B) machine state, connection is made to only the Public (B) network.
   Actual Result: The expected result was verified.

3. VT03 – States that the EEPROM becomes writeable and full access to the hard disk is allowed when the PC is fully powered down, the set-up plug is installed on the 2in1 PC™ card, and then the machine is powered back on. This test was selected to verify that the detection of the installed set-up plug occurs after the PC

has been hard booted. Once this detection is made, the Administrator has the ability to re-configure the EEPROM and also have full access to the hard disk.
Actual Result: The expected result was verified.

4. VT04 – States that the connectivity to each of the two networks will function normally as it would without the 2in1 PC™ card being installed on the PC. This test was selected to verify that the 2in1 PC™ card supports the connection of two networks and that these networks are physically separated from one other. This test was also selected to verify that connectivity to each network is not affected as a result of having the 2in1 PC™ card installed on the machine (i.e. the card is transparent to the connected network).
   Actual Result: The expected result was verified.

5. VT05 – States that low-level disk editing utilities based on BIOS interrupt 13 are denied the ability to read/alter unauthorised disk partitions when the TOE is running in work mode. This test was selected to verify that when the PC is running in any given machine state (Secure (A), Public (B), or Transition), access to unauthorised disk partitions is blocked.
   Actual Result: The expected result was verified.

6. VT06 – States that the 2in1 PC™ card will block the reading of unauthorised disk partitions when using low-level I/O port access methods while the TOE is running in work mode. This test was selected to verify that when the PC is running in any given machine state (Secure (A), Public (B), or Transition), access to unauthorised disk partitions using LBA or CHS disk addressing methods will be blocked.
   Actual Result: The expected result was verified.

7. VT07 – States that the 2in1 PC™ card will prevent the switch from the Transition machine state upon detection of a floppy disk being accessed. This test was selected to verify that the TOE monitors the ISA bus for any DMA2 traffic while the machine is running in the Transition machine state. If traffic is traveling across the DMA2 channel, then the PC will not reboot into the Secure (A) or Public (B) machine states; rather the PC will continue to reboot into the Transition state until no traffic is detected on the DMA2 channel.
   Actual Result: The expected results were verified.

The vendor tests defined above were selected to verify that the key security functions offered by the TOE operated in accordance with the *2in1 PC™ Functional Specification* and the functional requirements listed in the *2in1 PC™ Security Target.* Specifically, the key security functions are three machine operating states (Secure (A), Public (B), and Transition), network access separation, hard disk access separation, and protection of configuration information. Some of these key security functions, and also other security functions offered by the TOE, have been further evaluated and defined in detail in the independent tests described in Appendix B of the *Evaluation Test Plan for 2in1 PC™, Version 1.21*. The results of all of the independent tests performed were verified as

expected. Table 9.2.10.2.1-1 Correspondence of Developer and Independent Tests to Functional Specification provides a mapping from the vendor and independent tests performed to the *2in1 PC™ Functional Specification.*

9.2.13 AVA_SOF.1 Strength of TOE Security Function Evaluation

9.2.13.1 Evidence Elements

This section addresses the strength of TOE security function, defining any mechanisms relied upon by the TOE to enforce the TSF.

9.2.13.2 Evaluator Action Elements and Findings

9.2.13.2.1 Minimum Strength Level

This element is met because the TOE makes no strength of function claims.

9.2.13.2.2 Meets or Exceeds Claimed Strength of Function Metric

This element is met because the TOE makes no strength of function claims.

9.2.13.2.3 Confirm Correctness of Claimed Strength of Function

This element is met because the TOE makes no strength of function claims.

9.2.14 AVA_VLA.1 Developer Vulnerability Analysis

9.2.14.1 Evidence Elements

This section presents the results of the evaluation of the developer's vulnerability analysis and penetration testing performed by the CAFÉ Lab. The attack potential for the TOE is low or higher based on the *Voltaire 2in1 PC™ Security Target Report* Secure Usage Assumptions and Organisational Security Policies (see Table 9.2.14.2-1 and Table 9.2.14.2-2) and the identification and mitigation of obvious vulnerabilities in accordance with AVA_VLA.1, Developer Vulnerability Analysis.

9.2.14.2 Evaluator Action Elements and Findings

9.2.14.2.1 Content of Developer's Vulnerability Analysis

The *2in1 PC™ Vulnerability Analysis*, E21198040(2), satisfies this element by providing a unique identification and description of each vulnerability along with a description of how each vulnerability is addressed by the TOE.

9.2.14.2.2 Security Threats Addressed by the TOE

The security threats addressed by the TOE are identified in section 3.5 of the *Voltaire 2in1 PC™ Security Target Report.*

9.2.14.2.3 Security Threats Addressed by the Operating Environment

The security threats addressed by the TOE operating environment are identified in section 3.6 of the *Voltaire 2in1 PC™ Security Target Report.*

9.2.14.2.4 Obvious and Residual Vulnerabilities

Table 9.2.14.2.4-1 lists the TOE vulnerabilities identified in the *2in1 PC™ Vulnerability Analysis*, E21198040(2). These vulnerabilities are identified as "obvious vulnerabilities" in accordance with the guidance provided in the *(Draft) Common Methodology for Information Technology Security Evaluation* (see Section 9.2.14.2).

Obvious Vulnerability	Explanation
Relay failure	An electromechanical relay might malfunction.
Card removal	The TOE could be removed from the system and the disk accessed directly.
Improper installation	The TOE might be installed or configured incorrectly in a way that could undermine security.
Tampering en route	The TOE could be replaced or tampered with during shipment to the customer.

Table 9.2.14.2.4-1 Obvious Vulnerabilities

Table 9.2.14.2.4-2 lists the TOE vulnerabilities identified in the *2in1 PC™ Vulnerability Analysis*, E21198040(2). These vulnerabilities are identified as "residual vulnerabilities" in accordance with the guidance provided in the *(Draft) Common Methodology for Information Technology Security Evaluation* (see Section 9.2.14.2).

Vulnerability	Explanation
Floppy based copying	A floppy diskette could be used as a buffer between the two partitions, using an automatic script that switches from one state to the other.
Crash/forced shutdown	An attacker might shut down the system to force a state change. The same effect would occur should the system crash.
Transition altering	An attacker might change the automatic routines run in the Transition state, overcoming the memory clearing and any other access control routines implemented.
EEPROM altering	An attacker might remotely change the configuration data on the EEPROM, thereby gaining full access to the entire disk, or having the ability to change certain attributes which would compromise the disk's security
CHS remapping	An attacker might change the CHS addressing of the hard disk, thereby gaining access to unauthorised areas.
Using RAM as a buffer	An attacker might store data from one partition in the RAM, switch to the other partition and retrieve the data from the RAM.

Table 9.2.14.2.4-2 Residual Vulnerabilities

9.2.14.2.5 Exploitability of Obvious Vulnerabilities

A determination was made in accordance with the guidance provided in the *(Draft) Common Methodology for Information Technology Security Evaluation* (see Section 9.2.14.2) that the obvious vulnerabilities contained in developer's vulnerability analysis were not exploitable in the identified areas of malicious intent, hardware failure, and tampering during the delivery process. The results of additional CAFÉ Lab vulnerability testing are presented in Section 9.2.14.2.7.

An example of this determination is the TOE's dependence on the IT and non-IT environment for protection against malicious users. Physical tampering with the TOE, e.g., removing the 2in1 PC™ card, is one of the easiest and least sophisticated ways to circumvent the TOE's security functions. Mitigation of this vulnerability is dependent on both the physical security of the operating environment and restricting access to only authorised users. The *(Draft) Common Methodology for Information Technology Security Evaluation* states that "An obvious vulnerability is not exploitable in the intended environment if one or more of the following conditions exist: security functions or measures in the (IT or non-IT) environment prevent exploitation of the vulnerability in the intended environment. For instance, restricting physical access to the TOE to authorised users only may effectively render a TOE's vulnerability to tampering unexploitable; …". Since it is assumed that the TOE will be operated by authorised users in a secure environment (see Table 9.2.14.2-1, *Security Target Report* Secure Usage Assumptions, and Table 9.2.14.2-2, *Security Target Report* Organisational Security Policies), this vulnerability was determined to be unexploitable**.**

9.2.14.2.6 Consistency of Documentation

A determination was made that the *2in1 PC™ Vulnerability Analysis*, E21198040(2), satisfies this element based on the mapping presented in Table 9.2.14.2.6-1 and a review of the following documentation:

- *Voltaire 2in1 PC™ Security Target Report*
- E21198046, *2in1 PC™ User Guide*
- E21298063, *2in1 PC™ Installation Guide*
- E20598004, *2in1 PC™ Physical Data Security*
- E20698036, *2in1 PC™ Hacking Tests*

Table 9.2.14.2.6-1 provides a mapping between vulnerabilities, the security threats addressed by the TOE and the operating environment, and their mitigation by the TOE or applicable assumption.

Vulnerability	Threat	Mitigation/Assumption
Floppy Based Copying	T.T.COPY	Disabling switching during TRANSITION when DMA2 activity is detected.
Crash/Forced Shutdown	T.T.CRASH T.T.ENTRY T.T.ATTACK	Forcing each power-up of the system into the controlled Transition state.
Transition Altering	T.T.TRANSFER T.T.CONFIGURATION	Making the Transition partition read-only, and disallowing the bypassing of the automatic routines.
EEPROM Altering	T.T.ATTACK T.T.CONFIGURATION	Allowing the EEPROM to be written to only when a physical set-up plug is inserted.
CHS Remapping	T.T.DATA	Tracking the remap command and disabling disk activity when it is detected.
Using RAM as a Buffer	T.T.TRANSFER	Rebooting the PC between states and automatically forcing a memory clearing routine during TRANSITION. Note: This memory clearing routine was not evaluated in the configuration and cannot be trusted to work.
Peripheral Devices	T.T.DISK	Only allowing peripheral devices to be connected to the TOE using special cables, and controlling their operation.
Relay Failure	T.T.DEVICE.FAIL	Using a second set of redundant relays, each having a 10^-8 likelihood of failure. The relay's failure position is off.
Card Removal	T.E.PHYSICAL	A.E.ACCESS
Improper Installation	T.E.INSTALL T.E.ADMIN-ERROR	A.E.ADMIN
Tampering En Route	T.E.INSTALL T.E.PHYSICAL	Voltaire's handling and shipping procedures to include tamper resistant packaging.
T = Threat, .T = Threat, .E = Environment		

Table 9.2.14.2.6-1 Vulnerability Mapping

9.2.14.2.7 CAFÉ Lab Vulnerability Testing

The TOE can easily be exploited if proper physical and personnel security is not enforced, e.g., switching network connections and card removal. Based on a review of the TOE vulnerabilities, a determination was made to focus on testing the TOE's susceptibility to attack through unauthorised access to the disk partitions and copying information via the floppy disk. These vulnerabilities represent residual vulnerabilities not requiring physical access to be exploited although they would require the attacker to have more than minimal skills, technical sophistication, resources, and understanding of the TOE. The results of the testing showed that the TSF successfully countered these attacks. Sections 9.2.14.2.7.1 and 9.2.14.2.7.2 identify additional obvious and residual vulnerabilities that were considered during the TOE evaluation.

Table 9.2.14.2.7-1 identifies the testing performed by the CAFÉ Lab to replicate developer tests and validate the results. Specific scenarios, procedures, and test results are presented in the *Evaluation Test Plan for 2in1 PC™, Version 1.21,* Appendix A.

Element	Test to Confirm	Vulnerability
Direct Disk Access (Via Interrupt 13) VT05	Low-level disk editing utilities such as Norton Disk Editor that are based on BIOS Interrupt 13 are denied the ability to read / alter unauthorised disk partitions when the TOE is running in Work Mode.	An attacker might gain access to unauthorised disk partitions.
Direct Disk Access (I/O Ports) VT06	The 2in1 PC™ card will block the reading of unauthorised disk partitions when using low-level I/O port access.	An attacker might gain access to unauthorised disk partitions.
Floppy Based Automatic Copying VT07	The 2in1 PC™ card prevents the switch from the Transition machine state upon detection of any DMA2 activity.	A floppy diskette could be used as a buffer between the two partitions, using an automatic script that switches from one state to the other.
VT [Number] = Vendor Test [Test Reference Number]		

Table 9.2.14.2.7-1 Sample Tests to Confirm Developer Vulnerability Test Results

Table 9.2.14.2.7-2 identifies the testing performed by the CAFÉ Lab to independently verify the mitigation of the unauthorised disk partition access and floppy disk copying vulnerabilities. Specific scenarios, procedures, and test results are presented in the *Evaluation Test Plan for 2in1 PC™, Version 1,* Appendix B.

Element	Tests to Perform	Vulnerability
ET04	Access to the four disk partitions (Secure (A), Public (B), Transition, and Functional) is controlled by the TSF.	An attacker might gain access to unauthorised disk partitions.
ET05	The TOE will not switch the computer from the Transition machine state to an active state (Secure (A) or Public (B)) when DMA2 activity has been detected.	A floppy diskette could be used as a buffer between the two partitions, using an automatic script that switches from one state to the other.
ET [Number] = Evaluator Test [Test Reference Number]		

Table 9.2.14.2.7-2 TSF Tests to Confirm Mitigation of TOE Vulnerabilities

9.2.14.2.7.1 Obvious Vulnerabilities

Table 9.2.14.2.7.1-1 identifies obvious vulnerabilities considered as part of the TOE evaluation. It also identifies the mitigation for each vulnerability.

Obvious Vulnerability	Mitigation
1. Card removal.	A.E.ACCESS P.E.KNOWN
2. Switch network connections.	A.E.ACCESS P.E.KNOWN
3. Unauthorised use of the external set-up plug in conjunction with internal enabler plug.	A.E.ACCESS P.E.KNOWN
4. Unauthorised use of set-up plug	A.E.ACCESS P.E.KNOWN

Table 9.2.14.2.7.1-1 Obvious Vulnerabilities

Obvious Vulnerability	Mitigation
5. Unauthorised modification of device control connection jumpers.	A.E.ACCESS P.E.KNOWN
6. Unauthorised configuration of PC with more than 2 storage devices to be controlled by the TOE (jumper connections).	A.E.ACCESS P.E.KNOWN
A = Assumption, P = Physical, .E = Environment	

Table 9.2.14.2.7.1-1 Obvious Vulnerabilities (Cont.)

9.2.14.2.7.2 Residual Vulnerabilities

Table 9.2.14.2.7.2-2 identifies vulnerabilities requiring the attacker to have more than minimal skills, technical sophistication, resources, and understanding of the TOE. It also identifies the mitigation for each vulnerability.

Residual Vulnerability	Mitigation
1. Directly addressing the Altera chip and modifying the configuration settings derived from the EEPROM during the boot/reboot process.	Making the Altera chip non-addressable mitigates this vulnerability. The EEPROM chip on the other hand does have a machine address and the Altera chip controls the write access to it. Write access is only granted when the machine is running in set-up mode by the set-up plug jumpering the write enable pins on the 2in1 PC™ card.
2. Deleting 2in1 PC™ drivers/files stored in the A&B machine via networks to prevent state switching.	This vulnerability is not within the scope of the TSF, however it can lead to a denial of service attack preventing a user from switching to another machine state (i.e. Secure (A) or Public (B)). This vulnerability does not undermine the security provided by the TOE and can be resolved by the administrator reinstalling the drivers/files that were removed.
3. Introduction of malicious code, e.g. B>F>A.	This vulnerability is not within the scope of the TSF, however it can lead to corruption of data controlled by the TOE. The operating environment must address this vulnerability by having software, such as anti-virus programs, installed into the Transition disk partition. By storing such software in this disk partition, whenever the machine boots into the Transition machine state, the anti-virus software is executed to scan the Functional disk partition to prevent the spread of malicious code to the other machine state (i.e. Secure (A) or Public (B)).

Table 9.2.14.2.7.2-2 Residual Vulnerabilities

SECTION 10

EVALUATOR COMMENTS/RECOMMENDATIONS

10 EVALUATOR COMMENTS/RECOMMENDATIONS

This section contains some brief comments on the evaluated product and the evaluation process.

10.1 PRODUCT ENVIRONMENT

The TOE is an effective product for its' intended use. However, the requirement for a secure environment with non-malicious users can not be over stressed. The single largest vulnerability of the system is to a physical attack, where the network connections are switched.

10.2 INDIVIDUAL IDENTIFICATION & AUTHENTICATION

In most environments it would seem prudent to provide one, or more, effective I&A mechanisms to use with the TOE. This could be done by a single product running in the Transition partition and state, identifying and authenticating each individual user before allowing them to do anything on the system. Another way would be to use an I&A mechanism with the operating system in each of the user states (i.e., A and B). A third method would be to use I&A mechanisms in both the Transition and user states.

10.3 USE OF THE CEM

The TOE evaluation process incorporated the guidance provided in the *(Draft) Common Methodology for Information Technology Security Evaluation*, CEM-98-030, Version 0.5, November 1998. The guidance in Part 2: Evaluation Methodology was especially useful in defining the evaluation effort for achieving an EAL2 evaluation and in explaining the required actions for each element. The document is still in draft status and was only used as a guide. The evaluation was performed in accordance with the requirements in the *Common Criteria for Information technology Security Evaluation*, CCIB-98-028, Version 2.0, May 1998.

APPENDIX A

ACRONYMS

A

ACC – Access control [family of requirements from the CC]
ACF – Access control functions [family of requirements from the CC]
ACM – Configuration management [class of assurance requirements from the CC]
ADM – Administrator guidance [family of requirements from the CC]
ADO – Delivery and operation [class of assurance requirements from the CC]
ADV – Development [class of assurance requirements from the CC]
AGD – Guidance [class of assurance requirements from the CC]
AMO – A MBR Open [When this option is on (default), read MBR requests for state A return the MBR from address 0,0,1 of the hard disk]
ATE – Testing [class of assurance requirements from the CC]
AVA – Vulnerability assessment [class of assurance requirements from the CC]

B

BIOS – Basic Input/Output System

C

CAP – Configuration management [family of requirements from the CC]
CC – *Common Criteria for Information Technology Security Evaluation* (Version 2.0)
CEM – *Common Methodology for Information Technology Security Evaluation* (Version 0.5)
CHS – Cylinder, Head, Sector [method to access the PC's hard disk]
CM – Configuration Management
COTS – Commercial-Off-The-Shelf
COV – Coverage [family of requirements from the CC]
CPU – Central Processor Unit
CRC – Cyclic Redundancy Check

D

DEL – Delivery [family of requirements from the CC]
DMA2 – Direct Memory Access/Addressing, Channel 2
DRQ2 – An ISA bus signal for DMA2

E

EAL – Evaluation Assurance Level
EAL2 – Evaluation Assurance Level 2 [Structurally Tested]
EEPROM – Electronically Erasable Programmable Read-Only Memory
ET – Evaluator Test

F

FDP – User data protection [class of functional requirements from the CC]
FIA – Identification and authentication [class of functional requirements from the CC]
FLS – Fail secure [family of requirements from the CC]
FMT – Security management [class of functional requirements from the CC]
FPT – Protection of the TOE security functions [class of functional requirements from the CC]
FSP – Functional specification [family of requirements from the CC]
FUN – Functional tests [family of requirements from the CC]

G

GUI – Graphical User Interface
GUID – Globally Unique Identifier

H

HD – Hard Disk
HLD – High-level design [family of requirements from the CC]

I

I&A – Identification and Authentication
I/O – Input/Output
IDE – Integrated Drive Electronics
IGS – Installation, generation and start-up [family of requirements from the CC]
IND – Independent testing [family of requirements from the CC]
ISA – Industry Standard Architecture
IT – Information Technology
ITC – Import from outside TSF control [family of requirements from the CC]

JK

L

LBA – Logical Block Addressing [method to access the PC's hard disk]
Linux – UNIX operating system named after Linus Toralds

M

MB – Megabyte(s)
MBR – Master Boot Record
MHz – Mega-Hertz
MMX – Matrix Manipulation Extensions [Intel] + Multimedia Extensions
MSA – Management of security attributes [family of requirements from the CC]
MS-DOS – Microsoft – Disk Operating System

N

NIC – Network Interface Card
NSA – National Security Agency
NT – Microsoft – New Technology [Microsoft] operating system

O

P

PC – Personal Computer
PC/AT – Personal Computer/Advanced Technology [IBM AT standard]
PCB – Printed Circuit Board
PCI – Peripheral Component Interconnect/Interface
PP – Protection Profile
PROM – Programmable Read-Only Memory

Q

QA – Quality Assurance

R

RAM – Random Access Memory
RCR – Representation Correspondence [family of requirements from the CC]
RCV – Trusted Recovery [family of requirements from the CC]
ROM – Read-Only Memory

S

SCO – Santa Cruz Operation [UNIX operating system]
SCSI – Small Computer Systems Interface
SDRAM – Synchronous Dynamic Random Access Memory
SF – Security Function
SFP – Security Function Policy
SMR – Security Management Roles [family of requirements from the CC]
SOF – Strength of Function [family of requirements from the CC]
SPM – Security Policy Model [family of requirements from the CC]
ST – Security Target
SYD – *2in1 PC™ System Design Document*

T

TCP SYN – Transmission Control Protocol Synchronization Process [denial of service attack]
TOE – Target of Evaluation
TSC – TOE Scope Of Control
TSF – TOE Security Function
TSFI – TOE Security Function Interface
TSP – TOE Security Policy

U

UID – User identification [family of requirements from the CC]
USR – User guidance [family of requirements from the CC]

V

VLA – Vulnerability analysis [family of requirements from the CC]
VT – Vendor Test

WXYZ

APPENDIX B

Evaluation Test Plan for 2in1 PC, Version 1.21

Prepared for:
Voltaire Advanced Data Security, Ltd.
103 Medinat Hayehudim
P.O.B. 12534
Herzylia 46733, Israel

By:
COACT, Inc.
Rivers Ninety Five
9140 Guilford Road, Suite L
Columbia, Maryland 21046
Phone: 301-498-0150
Fax: 301-498-0855
Email: café-lab@café.coact.com

Document No. CA1298006
07 January 1998

1 Introduction

This test plan identifies the tests performed for the 2in1 PC™ evaluation, describes specific test scenarios and procedures, and presents the test results. It includes a description of the test environment, test assumptions, and a cross-reference between specific tests and the test results.

1.1 Scope

The 2in1 PC™ product evaluation is at the Evaluation Assurance Level 2 (EAL2). EAL2 involves structural testing of the TOE but does not demand more effort on the part of the developer than is consistent with good commercial practice and does not require a substantially increased investment in cost or time. It is applicable where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record.

This test plan addresses the ATE_IND.2, Independent testing - sample, assurance component of EAL2. The objective of this component is to demonstrate that the security functions perform as specified. It requires the evaluator to repeat a sample of the developer's tests to gain confidence in the results obtained and to build on the developer's testing by conducting additional tests that exercise the TOE in a different manner.

The specific requirements of ATE_IND.2 are:

Dependencies:

ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrative guidance
AGD_USR.1 User Guidance
ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.
ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

1.2 Functional Testing

Developer-provided information required by the ATE_FUN.1, Functional testing, assurance component has been evaluated separately and is not part of this test plan. The evaluation methodology and results are detailed in the FER, Section 9.2.11.

1.3 Document Organization

The *Evaluation Test Plan for the 2in1 PC, Version 1.21* is comprised of 5 Sections and 4 Appendices.

Section 1, Introduction, provides the scope of the 2in1 PC™ product testing and the documents organization.

Section 2, Test Environment, describes the TOE configuration, the hardware and software, and assumptions used during testing.

Section 3, Repeated Developer Tests to Confirm Developer Test Results, defines the sample of tests used to confirm the vendor test results and provides a mapping to the *2in1 PC Functional Specification.*

Section 4, Tests to Confirm the TOE Operates as Specified, defines the sample of independent tests used to confirm the 2in1 PC™ operates as specified and provides a mapping to the *2in1 PC Functional Specification.*

Section 5, Cross-Reference between Specific Tests and Test Results, defines the mapping between the tests listed in Sections 3 and 4 to their corresponding locations in Appendixes A and B and also defines the test document numbering scheme.

Appendix A, Test Results to Confirm Developer Test Results, this Section defines the following for each test performed:

1) Naming the evaluators that performed the test.
2) Identifying the date and time the test was performed.
3) Provides a brief test description.
4) Lists vendor documentation used as a reference.
5) Defines any changes to the TOE configuration identified in Section.
6) Identification of the expected test results.
7) Identification of the actual test results.
8) Identification of the repeatable test procedures.
9) Evaluator details/observations noted during the test.

Appendix B, Test Results to Confirm the TOE Operates as Specified, this section defines the following for each independent test performed:

1) Naming the evaluators that performed the test.
2) Identifying the date and time the test was performed.
3) Provides a brief test description.
4) Lists vendor documentation used as a reference.
5) Defines any changes to the TOE configuration identified in Section.
6) Identification of the expected test results.
7) Identification of the actual test results.
8) Identification of the repeatable test procedures.
9) Evaluator details/observations noted during the test.

Appendix C, Independent Evaluation Test Output, defines the complete output files generated to confirm the TOE operates as specified in the Test Results confirmed in Appendix B.

Appendix D, References, defines the vendor documentation that was used during testing.

2 Test Environment

2.1 TOE

Voltaire 2in1 PC™, Version 1.21 (For content version numbers, please refer to the Voltaire document titled "Configuration Items"). The 2in1 PC™ evaluation covers the 2in1 PC™ ISA Slot PC card, network connections and peripheral device connections controlled by the 2in1 PC™ card. These following items were tested:

1) The 2in1 PC™ ISA slot card was tested with an IDE analyzer to verify that it monitors all IDE signals defined in the evaluation test documents in Appendix B.
2) The network connections were tested to verify that the two connections were separated and operated in accordance with the *2in1 PC Informal Security Policy Model*.
3) The jumpers on the 2in1 PC™ card were tested to verify the enabling/disabling of access to peripheral devices such as a floppy drive, SCSI connection, or parallel port connection for each machine state of operation, A and B.
4) The machine states were tested with a Logic Analyzer to verify that the bootable partitions and network connections were enforced for the three operating states, Transition, Secure (A) and Public (B).

2.2 TOE Configuration

The 2in1 PC™ card was properly installed and configured in accordance with the steps provided in the *2in1 PC Installation Guide*. The configuration settings made during these steps are defined in the following tables. Any changes to the specified settings are noted in the test results in Appendix A and B.

Partition	Drive %	Total MB	Primary MB	Extended MB	File System	Access to Functional
Functional	3	49	----	----	FAT	----
Secure (A)	60	950	950	0	FAT	Read Only
Public (B)	37	592	592	0	FAT	Read/Write
Transition	----	9	----	----	FAT	No Access
Total: 100% 1600 MB						

Table 2-1 Partition Configuration

Transition Settings	Advanced Settings	
Power-Up Mode: Menu	Reset Signal	Advanced
	Network Mode	2in1 PC
	2nd HD (if exists)	A only
	Force Shutdown	No

Table 2-2 Settings Configuration

2.3 System Hardware

Computer: Twinbrook Systems, Intel 200Mhz Pentium-MMX
Motherboard: TX Chipset

Hard Disk: Seagate hard disk; model ST31720A, 1,705MB
BIOS Information: Award Modular BIOS Version 5.41PGM / Award Plug and Play BIOS Extension V1.0A
ISA Slot Cards: Voltaire 2in1 PC™, Version 1.21
Generic PIC Combo Network Interface Card (NIC)
Generic 16Bit SoundBlaster Compatible Sound Card
Diamond Stealth 4MB PCI Video Card / 3D 2000 Pro
Generic 33.6K Compatible Modem
Other: 32 MB SDRAM
24X LG CD-ROM Model CRD-8240B
Generic 3.5" 1.44MB NEC Floppy Diskette Drive
512K L2 Pipeline Burst Cache

2.4 Installed System Software

Operating System Used for Evaluation: DOS 7, Windows 95
2in1 PC Drivers: Operating System Dependent
Other Software: 2in1 PC Configuration Information from the 2in1 PC Installation Diskettes, Version 1.21 (2 Disks)

2.5 Test Equipment

Other Software: diskedit.exe (Norton)
llr.exe (Voltaire)
rwe2.exe (Voltaire)
Other Test Equipment: HP 1660A Logic Analyzer (50/100-MHz State/500-MHz Timing)
Innotec ID520 IDE Analyzer
Fluke 75 Multi-meter
HP 545A Logic Probe
Faxconn ISA Slot Extension Card

2.6 Test Assumptions

The following test assumptions, as stated in the Security Target, were used in the TOE evaluation:

1) Users of the Target of Evaluation (TOE) are trusted not to modify the hardware configuration.
2) The TOE will be located in a controlled environment (i.e. basic physical security is assumed to prevent modification of the system hardware/software).
3) The Personal Computer (PC) platform fully complies with the PC/AT standard.

3 Repeated Developer Tests to Confirm Developer Test Results

This section provides a high-level description of the sample of tests required by ATE_IND.2.3E to confirm developer test results. Specific scenarios, procedures, and test results are presented in Appendix A.

Legend VT [Number] = Vendor Test [Test Reference Number], FS = Functional Specification		
Element	**Test to Confirm**	**Mapping to FS**
EEPROM VT01	The configuration data stored on the EEPROM is storable, editable and retrievable.	Functional Specification Number 2
Electro-mechanical Relays VT02	The 2in1 PC™ card supports the connection of two physically separated networks.	Functional Specification Number 6
Set-up Plug VT03	The EEPROM becomes writeable with the set-up plug placed on the 2in1 PC™ card. The card will allow full disk access with the set-up plug placed on it.	Functional Specification Number 11
Network Connectors VT04	The network functions normally, as it would without the 2in1 PC™ card being installed.	Functional Specification Number 6

Table 3-1 Sample Developer Tests to Confirm the Functional Test Results

Legend VT [Number] = Vendor Test [Test Reference Number], FS = Functional Specification		
Element	**Test to Confirm**	**Mapping to FS**
Direct Disk Access (Via Interrupt 13) VT05	Low-level disk editing utilities such as Norton Disk Editor that are based on BIOS Interrupt 13 are denied the ability to read / alter unauthorized disk partitions when the 2in1 PC™ is running in Work Mode.	Functional Specification Number 5
Direct Disk Access (IO Ports) VT06	The 2in1 PC™ device will block the reading of unauthorized disk partitions when using low-level IO port access.	Functional Specification Number 5
Floppy Based Automatic Copying VT07	2in1 PC™ prevents the switch from the Transition machine state upon detection of a floppy disk being accessed.	Functional Specification Number 9

Table 3-2 Sample Developer Tests to Confirm the Mitigation of the Vulnerability Tests Results

4 Tests to Confirm the TOE Operates as Specified

This section provides a high-level description of the subset of TSF tests required by ATE_IND.2.2E to confirm the TOE operates as specified. Specific scenarios, procedures, and test results are presented in Appendix B.

Legend ET [Number] = Evaluator Test [Test Reference Number], FS = Functional Specification		
Element	**Tests to Perform**	**Mapping to FS**
ET01	The TOE can only be configured with the setup plug installed.	Functional Specification Number 1, 11
ET02	The three machine operating states (Secure (A), Public	Functional

	(B), and Transition) are reflected by hardware control signals.	Specification Number 3, 7
ET03	The Master Boot Record (MBR) is different when booting into each of the three machine operating states (Secure (A), Public (B), and Transition).	Functional Specification Number 4
ET06	The floppy drive cannot be accessed without the Control Connector installed.	Functional Specification Number 10

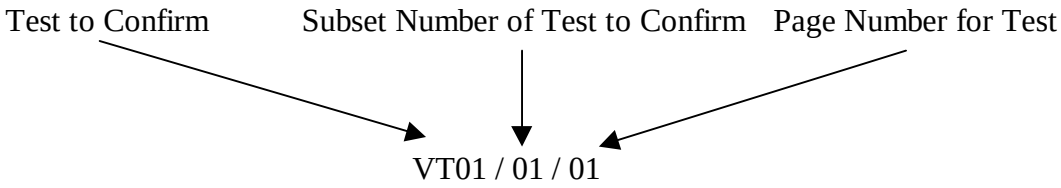
Table 4-1 TSF Tests to Confirm TOE Functionality

Legend ET [Number] = Evaluator Test [Test Reference Number], FS = Functional Specification		
Element	**Tests to Perform**	**Mapping to FS**
ET04	Access to the four disk partitions (Secure (A), Public (B), Transition, and Functional) is controlled by the TSF.	Functional Specification Number 5
ET05	The TOE will not switch the computer from the Transition machine state to an active state (Secure (A) or Public (B)) when floppy disk access has been detected.	Functional Specification Number 9

Table 4-2 TSF Tests to Confirm the Mitigation of Vulnerabilities

5 Cross-Reference between Specific Tests and Test Results

This section provides a mapping between the tests defined in the Tables from Section 3 and 4 and provides a cross-reference to the evaluator test documents located in Appendix A and B. The numbering system used for the evaluator test documents is defined as follows:



The Test to Confirm is the vendor / evaluator test that was performed from the Tables listed in Sections 3 and 4. The Subset Number of Test to Confirm is the vendor / evaluator test that was performed for each test listed in the Tables in Sections 3 and 4 (01 is the first subset test run for the indicated Test to Confirm, 02 is the second subset test run, etc.). The Page Number for Test defines the specific reference number assigned to each page in sequential order from the first to the last page of each Subset Test to Confirm.

	APPENDIX A AND APENDIX B REFERENCE
VT01	Test Plan Book One
VT02	Test Plan Book One
VT03	Test Plan Book One
VT04	Test Plan Book One
VT05	Test Plan Book One

VT06	Test Plan Book One
VT07	Test Plan Book One
ET01	Test Plan Book One (Test Plan Books One – Five contain detailed output)
ET02	Test Plan Book One (Test Plan Books One – Five contain detailed output)
ET03	Test Plan Book One (Test Plan Books One – Five contain detailed output)
ET04	Test Plan Book One (Test Plan Books One – Five contain detailed output)
ET05	Test Plan Book One (Test Plan Books One – Five contain detailed output)
ET06	Test Plan Book One (Test Plan Books One – Five contain detailed output)

APPENDIX C

BIBLIOGRAPHY

The following is a list of documents provided by the vendor in support of this evaluation (the numbering system used for each document is defined as, digits one and two represent an EAL-2 level evaluation; digits three through six define the month and date the document was delivered to the evaluation lab; digits seven through nine define the specific control number assigned to every document; and the bracketed numbers identify the document as being revision one, revision two, and so on).

E20598004 – *2in1 PC™ Physical Data Security*
E20598005 – *2in1 PC™ Security Claims*
E20698006 – *2in1 PC™ Administrative Rights*
E20698007 – *2in1 PC™ Security Policy*
E20698008 – *2in1 PC™ Flow Policy*
E20698009 – *2in1 PC™ Hardware Design*
E20698010 – *2in1 PC™ Terminal Map*
E20598011 – *2in1 PC™ Product Approval Tests*
E20598012(2) – *2in1 PC™ Software Design Document (Windows 3.11 – DOS)*
E20598013 – *2in1 PC™ Software Design Document (Windows NT)*
E20598014 – *2in1 PC™ Software Design Document (Windows 95)*
E21098015 – *2in1 PC™ Software Design Document (Windows 98)*
E21098016 – *2in1 PC™ System Development Plan*
E21098017 – *2in1 PC™ Platform Qualifications Summary*
E20598018(2) – *2in1 PC™ Platform Tests Description*
E20598019(2) – *2in1 PC™ Install White Box Tests Sheet*
E20897020 – *2in1 PC™ Code Documentation*
E20898021 – *2in1 PC™ Hardware Failure*
E20898022 – *2in1 PC™ New Version Tests*
E20398023 – *2in1 PC™ White Paper*
E20598024 – *2in1 PC™ System Design Document*
E20498025 – *2in1 PC™ SPOCK Presentation*
E20198034 – *2in1 PC™ IDE Tests – Source Code*
E21198035(4) – *2in1 PC™ Informal Security Policy Model*
E20698036(3) – *2in1 PC™ Hacking Tests*
E21198037 – *Preliminary Evaluation of 2in1 PC™*
E21198038 – *2in1 PC™ Operating System QA Test*
E21198039(2) – *Evaluation of 2in1 PC™ Installation Guide, Version 1.21*
E21198040(2) – *2in1 PC™ Vulnerability Analysis*
E21198041(3) – *2in1 PC™ Configuration Items*
E21198042(3) – *2in1 PC™ Functional Testing*
E21198043(2) – *2in1 PC™ Tests Coverage*
E21197044 – *2in1 PC™ Product Requirements Document*
E21198045(3) – *2in1 PC™ Delivery Procedure*

E21198046 – *2in1 PC™ User Guide*
E21198047(2) – *2in1 PC™ Mapping of Assurance Elements*
E21198048 – *2in1 PC™ Claims*
E21198049 – *2in1 PC™ Relay Information*
E21298050 – *2in1 PC™ Software Components*
E21298053 – *2in1 PC™ Transition partition*
E21298054(4) – *2in1 PC™ Functional Specifications*
E21298056 – *2in1 PC™ Addendum to the 2in1 PC™ – Installation Software*
E21298057 – *2in1 PC™ IDE Tests – Output*
E21298058 – *2in1 PC™ Addendum to the 2in1 PC™ – The Transition partition*
E21298061 – *2in1 PC™ Updates to the SYD EEPROM Mapping Section*
E21298062 – *2in1 PC™ Application Notes*
E21298063 – *2in1 PC™ Installation Guide*
E21298064 – *2in1 PC™ Quick Installation Guide*
E21197065 – *2in1 PC™ IO Protocol Tests*
E20199066 – *2in1 PC™ Addendum to the 2in1 PC™ – System Design Document*

The following is a list of other documentation referenced in support of this evaluation:

CCIB-98-026 – *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model,* May 1998, Version 2.0.
CCIB-98-027 – *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements*, May 1998, Version 2.0.
CCIB-98-027A – *Common Criteria for Information Technology Security Evaluation, Part 2: Annexes*, May 1998, Version 2.0.
CCIB-98-028 – *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements*, May 1998, Version 2.0.
CEM-98/030 – *Common Criteria for Information Technology Security Evaluation, Part 2: Evaluation Methodology*, November 1998, Version 0.5.
Proposed TTAP Process for Common Criteria EAL1 & 2 Evaluations.