SECURITY TARGET FOR CONSEAL PRIVATE DESKTOP VERSION 1.4

Document No. 1351-013-D001
Version 1.01, 31 March 1999

Public Works and Government Services Canada
Contract No: W2213-7-3927/04-QE
Requisition No: W2213-9-9804

Prepared for:

Certification Body
Communications Security Establishment
P.O. Box 9703
Terminal
Ottawa, Ontario
K1G 3Z4

Prepared by:

Electronic Warfare Associates-Canada, Ltd.
275 Slater St., Suite 1600
Ottawa, Ontario
K1P 5H9

Security Target for ConSeal Private Desktop Version 1.4

Document No. 1351-013-D001
Version 1.01, 31 March 1999

<Original> Approved by:

Project Engineer: R. Walters ______________

Project Manager: P. Zatychec ______________

Program Director: J. Robbins ______________

(Signature) (Date)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 IDENTIFICATION

This document details the Security Target (ST) for a networked personal computer (PC) running the Microsoft Windows 98 operating system, a representative suite of office and network applications, and the Signal 9 Solutions, *ConSeal Private Desktop* (*CPD)*, version 1.4. This ST has been prepared in accordance with the Common Criteria for Information Technology Security Evaluation (CC), Version 2.0, May 1998.

1.2 OVERVIEW

The *CPD* is designed to protect a Windows/Intel (Wintel) PC from network attacks, and to limit the system's use of network NDIS interfaces to what the user wants. *CPD* is a hybrid product that provides some of the functionality typically associated with traffic-filter and application-level firewalls, but in a host-based solution. It requires Windows 95 (with Winsock 2 update), or Windows 98 as the underlying PC operating system.

CPD mediates access between the host PC and its network NDIS interfaces based on rules defined by the user. At an individual application level, *CPD* monitors Winsock (Windows Sockets) applications for network access requests. When trusted applications need to access a network, *CPD* manages network access to transparently permit that application's traffic. When non-trusted applications try to access a network, *CPD* blocks all traffic to and from that application. The user selects whether *CPD* trusts an application or not.

In addition to application network access, *CPD* also intercepts all inbound network packets as they are passed from the network device driver, and allows or blocks them in accordance with a set of user-defined rules. Mediation of all protocols (e.g., TCP/IP, UDP/IP, ICMP/IP, ARP, Net BT, IPX, NetBEUI, etc.) is supported at this level.

The *CPD* human machine interface (HMI) enables the user to specify how network access it mediated, the level of network activity displayed and what network activity is logged. The HMI also provides the user with current and historical views of Winsock application network access, and their associated level of activity. In addition to other security relevant events, application network activity and mediated incoming network traffic can also be logged to a separate ASCII text file. This file can be reviewed using standard text editors.

While the *CPD* product is designed for a non-technical user (someone without a detailed knowledge of network protocols and services), it is assumed that it is operated in a benign environment – one in which the user does not have malicious intent and configures the product appropriately. The product will not prevent a user from carelessly configuring *CPD* such that network protection is compromised.

The evaluated configuration consists of a networked PC running the Microsoft Windows 98 operating system, a representative suite of office and network applications, and *CPD* version 1.4. As installed in this configuration, *CPD* is considered to be an intrinsic component of the operating system.

1.3 CC CONFORMANCE

The Target of Evaluation (TOE) for this ST is conformant with the functional requirements specified in Part 2, and the assurance requirements for Evaluation Assurance Level (EAL) 1, as specified in Part 3, of the CC.

2 TARGET OF EVALUATION DESCRIPTION

The TOE consists of a PC running the Microsoft Windows 98 operating system, a representative suite of office and network applications, and the *CPD*, version 1.4. The TOE is connected to a network, or networks, by one or more PC network interfaces, and is used by a single user/administrator. For CC evaluation purposes, the external TOE interfaces include the network interfaces, and the HMI. The HMI includes the display and input devices through which the user interacts with the *CPD* program, plus the ASCII log files created by *CPD*.

The TOE software environment consists of the software listed in Table 1.

Name	Version	Purpose	Comment
MS Windows	98	Operating System	Default installation with MS Network client, and TCP/IP, NetBIOS over TCP/IP (NBT) and NetBEUI network protocols.
MS Telnet	98	Telnet client included with Windows 98	Included with Windows 98. Representative network application.
MS FTP	98	FTP client included with Windows 98	Included with Windows 98. Representative network application.
MS Internet Explorer	4.0	Web browser	Included with Windows 98. Representative network application.
MS Outlook Express	4.0	E-mail, newsreader client	Representative network application.
MS Office	97 Pro SR 2a	Word processor, spreadsheet, presentation, database application	Default installation less Outlook. Representative office application.
Netscape Communicator	4.5	Web browser, E-mail, newsreader, FTP client	Representative network application.
Eudora Light	3.06	E-mail client	Representative network application.
Free Agent	1.11	Newsreader	Representative network application.
WS FTP Pro	5.00	FTP client	Representative network application.
mIRC	5.51	IRC client	Representative network application.
ICQ	99a	ICQ client	Representative network application.
Real Player	G2	Streaming audio/video client	Representative network application.
Terra Term	1.4	Telnet client	Representative network application.
ConSeal Private Desktop	1.4	Desktop Security	TOE security application

Table 1 TOE Software Environment

The TOE hardware environment consists of an Intel-based PC that meets the minimum systems requirements for the Microsoft Windows 98 operating system, and includes floppy and CD-ROM drives. It also includes an Ethernet network interface card (NIC), and an external modem for PPP dial-up network access. Figure 1 shows a typical TOE installation consisting of a PC with both a modem and NIC network interfaces, connected to local and remote networks.

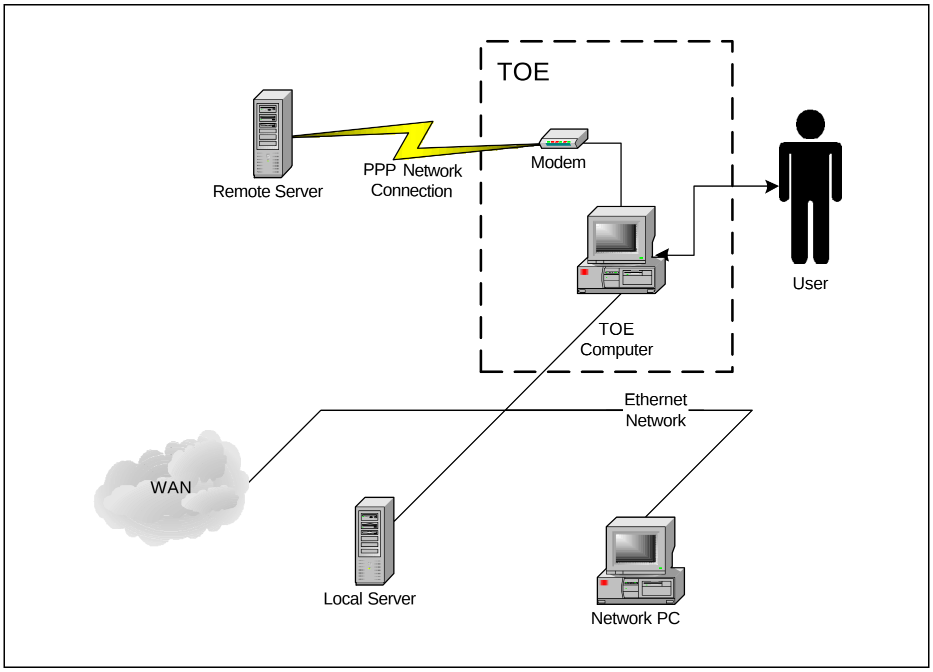

Figure 1 Typical TOE Installation

CPD is a hybrid product that provides much of the functionality typically associated with traffic- and application-filtering firewalls, but in a host-based solution. It is designed to protect a Wintel PC from network attacks, and to limit the system's use of network interfaces to what the user wants. *CPD* requires Windows 95 (with Winsock 2 update), or Windows 98 as the underlying PC operating system.

The user of the TOE also administers the TOE security functions, with network access control grouped into two main areas: Winsock application network access control; and, system network access control.

At the individual application level, when a Winsock (Windows Sockets) application requests network access, *CPD* mediates this request and allows or blocks network access based on whether the user has specified that the application is permitted or denied network access. This decision is based on the file name of the application executable.

System and external entity network access is based on the network interface involved, and the specific system services and protocol settings the user has specified for that device. The system services and protocols that can be controlled for each NDIS interface include:

a. NetBIOS shares of TOE resources;
b. NetBIOS access of remote, shared network resources;
c. TCP Identification requests;
d. ICMP traffic;
e. ARP traffic;
f. UDP DHCP traffic;
g. TCP RIP traffic;
h. TCP PPTP traffic;
i. IP protocols, other than TPC, UDP or ICMP; and
j. non-IP protocols, other than ARP.

In addition to the above network access control, *CPD* blocks fragmented IP packets, and IP packets with the same destination and source address. The user can also override all network access control rules to either permit, or deny, all network access requests from TOE or external sources.

The *CPD* HMI enables the user to specify how network access is mediated, the level of network activity displayed and what network activity is logged. The HMI also provides the user with current and historical views of Winsock application network access, and their associated level of activity.

CPD generates a time-stamped event audit log of security relevant events, as well as application network activity and mediated incoming network traffic. The *CPD* HMI has no intrinsic capability to view, modify, delete, search or sort audit log data, but the audit log is a formatted ASCII file that can be viewed and edited with any text editor. The audit log is rolled over each month and is limited to a maximum size of 5 MB, at which time auditing is reduced, but *CPD* continues functioning.

While the *CPD* product is designed for a non-technical user (someone without a detailed knowledge of network protocols and services), it is assumed that it is operated in a benign environment – one in which the user does not have malicious intent and configures the product and its host platform appropriately. The product will not prevent a user from carelessly configuring *CPD*, or the underlying PC, such that network protection is compromised.

3 TOE SECURITY ENVIRONMENT

3.1 ASSUMPTIONS

The following conditions are assumed to exist in the operational environment:

A.PHYSEC The TOE is physically secure.

A.NETWS The TOE is functioning as a single-user, networked workstation. The sharing of TOE resources with external network IT entities is limited to the peer-to-peer file and print sharing capabilities provided by the underlying TOE operating system.

A.USRADM The user of the TOE is also the administrator who manages TOE security functions locally (no remote administration).

A.NOIA The TOE does not provide any user identification or authentication functionality.

A.NOEVIL Users are non-hostile and follow all administrator guidance; however, they are capable of error.

A.LOCADM Administration of TOE security functions is only conducted locally from the TOE HMI.

A.CMPTIF Only network devices compatible with *CPD* are installed and functioning within the TOE. This includes Ethernet-like network devices, but excludes Token Ring, FDDI, Frame Relay and X.25 network devices.

A.USRKNW The user is knowledgeable of TOE applications that require network access.

A.NOROUTE The TOE does not route traffic between network interfaces.

A.BADAPP Users do not execute applications on the TOE that communicate over network interfaces, but bypass TOE security functionality. This includes applications and protocols that interface directly with the network device drivers, bypassing the Winsock protocol stack and NDIS interface.

A.APPFLAW The TOE cannot protect against an external network user or IT entity that exploits flaws in authorized application or service implementations, to read, modify or destroy TOE internal data.

3.2 THREATS

The following threats are addressed either by the TOE or the environment.

3.2.1 Threats Addressed By The TOE

The threats discussed below are addressed by a compliant TOE. The threat agents are either human users or external IT entities not authorized to use the TOE. The assets that are subject to attack are the IT resources residing on the TOE.

T.TOEDOS An external network user or IT entity user may compromise TOE integrity and/or availability by conducting Denial of Service attacks against TOE resources.

Application Note. Threats that conduct denial of service attacks against the network pipeline itself (e.g., bandwidth saturation attacks), or against servers and services to which the TOE connects via the network, are not included since these are not direct threats to the assets defined above.

T.TOEPRO An external network user or IT entity user may bypass, deactivate, or tamper with TOE security functions.

T.ATKVIS An external network user or IT entity may conduct undetected attack attempts against the TOE.

T.TOEDATA An external network user or IT entity may read, modify or destroy TOE internal data.

T.TOEFCN An external network user or IT entity may access and use security and/or non-security functions of the TOE.

T.NONAPP A local user may be unaware that an unauthorized Winsock application, executing on the TOE, is accessing the network via TOE network interfaces.

3.2.2 Threats To Be Addressed By Operating Environment

The threat possibilities discussed below must be countered by procedural measures and/or administrative methods:

T.USAGE The TOE may be configured, used and administered in an insecure manner.

T.TROJAN Compromise of the integrity and/or availability of the TOE may occur as a result of a TOE user unwittingly introducing a virus or trojan into the system.

4 SECURITY OBJECTIVES

4.1 TOE SECURITY OBJECTIVES

The following are the IT security objectives for the TOE:

O.MEDAPP The TOE must mediate the capability of Winsock applications executing on the TOE to communicate over TOE network interfaces.

O.MEDEXT The TOE must mediate network access to and from the TOE itself at the NDIS layer of each network interface.

O.DSPAPP The TOE must display to the user the current and recent history of network activity associated with Winsock applications executing on the TOE.

O.DSPSYS The TOE must display to the user the current network activity associated with the TOE operating system accessing, or attempting to access, networks, and external network entities accessing, or attempting to access, the TOE.

O.AUDIT The TOE must record a readable audit trail of TOE network activity and security relevant events, and permit their review by the user.

O.SELFPRO The TOE must protect itself against attempts by an external network user or IT entity to bypass, deactivate, or tamper with TOE security functions.

O.NETATK The TOE must protect itself from Denial of Service attacks against the TOE via TOE network interfaces.

O.ADMIN The TOE must provide functionality that enables an administrator to effectively manage the TOE and its security functions from its local HMI.

4.2 ENVIRONMENT SECURITY OBJECTIVES

The following are non-IT security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

O.GUIDAN The user responsible for the TOE must ensure that the TOE is delivered, installed, configured, administered, and operated in a manner that maintains its security.

O.AUTHUSR Only authorized users are permitted physical access to the TOE.

5 IT SECURITY REQUIREMENTS

5.1 TOE SECURITY REQUIREMENTS

This section provides functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC.

5.1.1 TOE Security Functional Requirements

The functional security requirements for this ST consist of the following components from Part 2 of the CC, summarized in Table 2. The TOE controls information flow for Winsock applications executing on the TOE quite differently from system services and external entities. Therefore, the FDP_IFC.1 and FDP_IFF.1 requirements have been iterated to define two TOE information flow Security Function Policies (SFPs).

Functional Components	
Identifier	**Name**
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SEL.1	Selective audit
FAU_STG.4	Prevention of audit data loss
FDP_IFC.1	Subset information flow control (1)
FDP_IFC.1	Subset information flow control (2)
FDP_IFF.1	Simple security attributes (1)
FDP_IFF.1	Simple security attributes (2)
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.3	Static attribute initialization
FPT_STM.1	Reliable time stamps

Table 2 Summary of Security Functional Requirements

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 – The TSF shall be able to generate an audit record of the following auditable events:

a. Start-up and shutdown of the audit functions;
b. All auditable events for the [basic] level of audit identified in Table 3; and
c. [none].

FAU_GEN.1.2 – The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity, and the outcome (success of failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the ST, [information specified in column four of Table 3].

Functional Component	Level	Auditable Event	Additional Audit Record Contents
FAU_SEL.1	Minimum	All modifications to the audit configuration that occur while the audit collection functions are operating.	
FAU_STG.4	Basic	Actions taken due to the audit storage failure.	
FDP_IFF.1	Minimum	Decisions to permit requested information flows.	The presumed addresses of the source and destination subject, or the Winsock application name and presumed remote address., local and remote port, and number of bytes sent and received.
	Basic	All decisions on requests for information flows.	The presumed addresses of the source and destination subject, or the Winsock application name and presumed remote address.
FMT_MOF.1	Basic	All modifications in the behaviour of the functions in the TSF.	
FMT_MSA.3	Basic	Modifications of the default setting of permissive or restrictive rules.	

Table 3 Auditable Events

FAU_SAR.1 Audit review

FAU_SAR.1.1 – The TSF shall provide [an authorized user] with the capability to read [all audit data] from the audit records.

FAU_SAR.1.2 –The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SEL.1 Selective Audit

FAU_SEL.1.1 – The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes: [event type].

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 – The TSF shall [ignore auditable events] and [create an audit entry indicating that event auditing has been stopped, and continue logging system errors and changes in TOE security functionality] if the audit trail is full.

FDP_IFC.1 Subset information flow control (1)

FDP_IFC.1.1 – The TSF shall enforce the [APPLICATION SFP] on:

a. [subjects: TOE Winsock applications that send and receive information over TOE network interfaces;
b. information: network traffic sent to or from the TOE;
c. operations: pass information].

FDP_IFC.1 Subset information flow control (2)

FDP_IFC.1.1 – The TSF shall enforce the [SYSTEM SFP] on:

a. [subjects: TOE system services and external IT entities that send and receive information to and from the TOE over network NDIS interfaces;
b. information: network traffic sent to or from the TOE;
c. operations: pass information].

FDP_IFF.1 Simple security attributes (1)

FDP_IFF.1.1 – The TSF shall enforce the [APPLICATION SFP] based on the following types of subject and information security attributes:

a. [subject security attributes:

(1) reported subject executable name;
(2) trust status;

b. information security attributes:

(1) Ethernet packet type;
(2) Ethernet packet fragmentation status;
(3) presumed destination address;
(4) presumed source address].

FDP_IFF.1.2 – The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rule holds: [The TOE shall permit a subject to have network access when the reported subject executable name has been assigned “trusted” status by the user].

FDP_IFF.1.3 – The TSF shall enforce the [none].

FDP_IFF.1.4 – The TSF shall provide the following [none].

FDP_IFF.1.5 – The TSF shall explicitly authorize an information flow based on the following rules: [The user has overridden the information flow security policy rules to permit all TOE network access requests].

FDP_IFF.1.6 – The TSF shall explicitly deny an information flow based on the following rule: [The TOE shall reject a subject request for network access, and block network access, when:

a. the reported subject executable name has been assigned “blocked” (untrusted) status by the user;
b. the user has overridden the information flow security policy rules to deny all TOE network access requests;
c. (Packet Type = IP) AND (Packet is fragmented);
d. (Packet Type = IP) AND (Source Address = Destination Address); or
e. the request matches the predetermined combination of security attributes specified in FDP_IFF.1.2 (2), but the user has explicitly denied the particular security attribute combination].

FDP_IFF.1 Simple security attributes (2)

FDP_IFF.1.1 – The TSF shall enforce the [SYSTEM SFP] based on the following types of subject and information security attributes:

a. [subject security attributes: none;

b. information security attributes:

(1) TOE NDIS interface on which traffic arrives and departs;
(2) Ethernet packet type;
(3) Ethernet packet fragmentation status;
(4) transport layer protocol;
(5) presumed destination address;
(6) presumed source address;
(7) service (i.e., source or destination port)].

FDP_IFF.1.2 – The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rule holds:

[The following predetermined combinations of information security attributes are met, and the rule has been explicitly set to permit information flow over the requested network NDIS interface, in accordance with the information flow security policy set by the authorized user:

a. Local NetBIOS Share – (Packet Type = IP) AND (Destination Address = Local) AND (Local Port = (UDP 137/138) OR (TCP 139))

b. Remote NetBIOS Share – (Packet Type = IP) AND (Source Address = Local) AND (Remote Ports = (UDP 137/138) OR (TCP 139))

c. Identification – (Packet Type = IP) AND ((Destination OR Source Address) = Local) AND (Local Port = TCP 113)

d. ICMP – (Packet Type = IP) AND (Protocol = ICMP) AND ((Destination OR Source Address) = Local) AND (Packet Rate ≤ Max Packet Rate)

e. ARP – (Packet Type = ARP)

f. DHCP – (Packet Type = IP) AND ((Local OR Remote Port) = UDP 67/68)

g. RIP – (Packet Type = IP) AND ((Local OR Remote Port) = UDP 520)

h. PPTP – (Packet Type = IP) AND (Remote Port = TCP 1723)

i. Other IP – (Packet Type = IP) AND (Protocol ≠ (ICMP OR UDP OR TCP))

j. Non IP - (Packet Type ≠ (IP OR ARP))

FDP_IFF.1.3 – The TSF shall enforce the [none].

FDP_IFF.1.4 – The TSF shall provide the following [none].

FDP_IFF.1.5 – The TSF shall explicitly authorize an information flow based on the following rules: [The user has overridden the information flow security policy rules to permit all TOE network access requests].

FDP_IFF.1.6 – The TSF shall explicitly deny an information flow based on the following rule: [The TOE shall reject subject requests for access or services via a TOE network NDIS interface, when:

a. the requested access or services are not explicitly permitted in accordance with FDP_IFF.1.2;
b. the user has overridden the information flow security policy rules to deny all TOE network access requests;
c. (Packet Type = IP) AND (Packet is fragmented); or
d. (Packet Type = IP) AND (Source Address = Destination Address)].

Application Note: The TOE can make no claim as to the real address of any source or destination for external IT subjects, therefore the TOE can only suppose that these addresses are accurate. A "service", mentioned in FDP_IFF.1.1(b), could be identified, for example by a source port number and/or destination port number.

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 – The TSF shall provide and restrict the ability to perform the functions:

a. [start-up and shutdown of TSF security functions;
b. create, delete, modify and view information flow security policy rules that permit or deny information flows;
c. to override the information flow security policy rules to permit all, or deny all, TOE network access;
d. modify and set TOE time and date;
e. select the level of network activity detail that is displayed on the HMI;
f. view the executable path of TOE Winsock applications currently communicating via the network;
g. view on-line user and administrator guidance;
h. view and modify the settings that enable or disable the logging of selected network traffic;
i. archive, modify, create and delete the audit trail.

to an authorized user].

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 – The TSF shall enforce the [information flow controls APPLICATION SFP and SYSTEM SFP,] to provide restrictive default values for information flow security attributes that are used to enforce the SPF.

Application Note: The default values for the information flow control security attributes appearing in FDP_IFF.1 (1) and FDP_IFF.1 (2) are intended to be restrictive in the sense that both inbound and outbound information is denied by the TOE until the default values are modified by an authorized user.

FMT_MSA.3.2 – The TSF shall allow the authorized user to specify alternative initial values to override the default values when an object or information is created.

Application Note: FMT_MSA.3.2 has been included as the complete set of functional elements of a component must be selected for inclusion in an ST, but it is not applicable to the TOE. See Section 8.2.1 for the rationale explaining this.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 – The TSF shall be able to provide reliable time stamps for its own use.

Application Note: The word “reliable” in the above requirement means that the order of occurrence of auditable events is preserved.

5.1.2 TOE Security Assurance Requirements

The assurance security requirements for this ST, taken from Part 3 of the CC, compose EAL1. The assurance components are summarized in the following table:

Assurance Class	Assurance Components	
	Identifier	**Name**
Configuration Management	ACM_CAP.1	Version numbers
Delivery and Operation	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_IND.1	Independent testing – conformance

Table 4 Assurance Requirements EAL1

Evaluation Note: All of the above assurance requirements, except for ATE_IND.1, only apply to the *CPD* product itself, and not to the underlying operating system. ATE_IND.1 applies to the complete TOE.

ACM_CAP.1 Version numbers

Developer action elements:

ACM_CAP.1.1D – The developer shall provide a reference for the TOE.

Content and presentation of evidence elements:

ACM_CAP.1.1C – The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.1.2C – The TOE shall be labelled with its reference.

Evaluator action elements:

ACM_CAP.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D – The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C – The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E – The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_FSP.1.1D – The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C – The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C – The functional specification shall be internally consistent.

ADV_FSP.1.3C – The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C – The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E – The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_RCR.1.1D – The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representation that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C – For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_ADM.1 Administrator guidance

Developer action elements:

AGD_ADM.1.1D – The developer shall provide administrator guidance addressed to system administration personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C – The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C – The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C – The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C – The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C – The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C – The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C – The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C – The administrator guidance shall describe all se3curity requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Evaluation Note: The user of the TOE is also the administrator. There is one set of user/administrator documentation, and it is contained in the *CPD* on-line help file.

AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D – The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C – The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C – The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C – The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C – The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C – The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C – The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Evaluation Note: The user of the TOE is also the administrator. There is one set of user/administrator documentation, and it is contained in the *CPD* on-line help file.

ATE_IND.1 Independent testing – conformance

Developer action elements:

ATE_IND.1.1D – The developer shall provide the TOE for testing.

Evaluation Note: The developer is limited to providing the *CPD* product in this case.

Content and presentation of evidence elements:

ATE_IND.1.1C – The TOE shall be suitable for testing.

Evaluator action elements:

ATE_IND.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2E – The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

6 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

6.1 TOE SECURITY FUNCTIONS

A description of each of the TOE security functions follows.

F.APPCTL The TOE shall allow or block network access by Winsock applications, executing on the TOE, based on the file name of the application executable. Network access allowed by this function does not override the limiting or blocking of network access by F.SYSCTL and F.NETATK.

F.SYSCTL The TOE shall allow, limit or block the ability of TOE services and external IT entities to send and receive information, via each TOE network NDIS interface, as follows:

a. allow or block NetBIOS shares of TOE resources (TCP/139);
b. allow or block NetBIOS access of remote, shared network resources (TCP/139);
c. allow or block incoming Identification requests (TCP/113);
d. allow, limit or block incoming and outgoing ICMP traffic;
e. allow or block incoming and outgoing ARP packets;
f. allow or block incoming and outgoing DHCP traffic (UDP 67/68);
g. allow or block incoming and outgoing RIP traffic (TCP/520);
h. allow or block incoming and outgoing PPTP (TCP/1723);
i. allow or block incoming and outgoing IP protocols, other than TPC, UDP or ICMP; and
j. allow or block incoming and outgoing non-IP protocols, other than ARP.

Network access allowed by this function does not override the blocking of network access by F.NETATK.

F.NETATK The TOE shall block:

a. fragmented IP packets; and
b. IP packets with the same destination and source address.

F.BLKOTH All other network traffic not specifically permitted in accordance with the above, shall be blocked.

F.OVRIDE The TOE shall permit the user to override TOE network access control functions F.APPCTL, F.SYSCTL, F.NETATK and F.BLKOTH to either:

a. permit all TOE network access requests; or
b. deny all TOE network access requests.

F.GUI The TOE shall provide the user with the capability to perform the following functions:

a. start-up and shutdown the TOE security functions;
b. permit or deny Winsock applications, executing on the TOE, the ability to communicate via the network;
c. view the executable path of TOE Winsock applications currently communicating via the network;
d. selectively permit or deny system functions from communicating via the network, by interface;
e. override all access rules to permit, or deny, all TOE network access;
f. select the level of network activity detail that is displayed to the user;
g. view and modify the settings that enable or disable the logging of selected network traffic;
j. view on-line user and administrator guidance;
h. modify and set the system time and date; and
i. archive, modify, create and delete the audit logs.

F.INIT When TOE security functions are started, the TOE shall initialize with the security settings in effect when it was last shutdown. If this saved configuration cannot be loaded or does not exist, the TOE shall warn the user that a new, default configuration is being created. The default configuration shall restrict TOE network access to the minimum required to establish network connectivity.

F.AUDEVT The TOE shall generate an audit log of the following events:

a. start-up and shutdown;
b. start-up security configuration;
c. changes in TOE security function configuration;
d. traffic generated by trusted applications;
e. when log file reaches maximum size;
f. when log entries have been skipped; and
g. permitted, denied and unknown network traffic, as selected by the user.

F.AUDINF For each audit event entry, the TOE shall record the data and time, type of event, event details, and success or failure of the event.

F.AUDRVW The TOE shall provide the user with the capability to view, modify or delete audit record logs.

F.AUDLOG On TOE security function start-up, the TOE shall create a new log file if it is the first time it has been started that month. For a given monthly log, after the log file reaches 5 MB in size, the TOE shall no longer create log entries for information flow control related events and shall create a log entry indicating that event auditing has been stopped. The TOE shall continue to create log entries for error messages and TOE security functionality changes.

F.TIME The TOE shall provide a reliable time and date for the time stamping audit log entries.

6.2 ASSURANCE MEASURES

A description of each of the TOE assurance measures follows.

M.ID The TOE shall incorporate a unique version identifier that can be displayed to the user.

M.SETUP The TOE shall include an automated installation and setup program compatible with the TOE operating system. The installation process shall be self-explanatory, or provide additional instructions to clearly document the installation process. The default installation shall result in the secure installation and start-up of the TOE.

M.SPEC A top-level, TOE functional specification shall be provided that describes TOE security functionality and its external interfaces.

M.TRACE The security functionality detailed in the TOE functional specification shall be upwards traceable to this ST, and downwards traceable to the TOE design.

M.DOCS Sufficient user and administrator guidance documentation shall be provided in the form of an on-line, help file, accessible from the TOE HMI.

M.TEST A suitably configured TOE shall be evaluated in a controlled networked environment to confirm that TOE functionality operates as specified, and that the TOE is protected from a representative set of well-known network attacks. TOE functionality shall also be evaluated in a real-world environment, using a representative set of network applications to communicate with remote networked systems.

7 PROTECTION PROFILE CLAIMS

This ST does not make compliance claims with respect to any Protection Profiles.

8 RATIONALE

8.1 SECURITY OBJECTIVES RATIONALE

8.1.1 TOE Security Objectives Rationale

Table 5 provides a bi-directional mapping of TOE Security Objectives to Threats, and is followed by a discussion of how each Threat is addressed by the corresponding TOE Security Objectives.

	T.TOEDOS	T.TOEPRO	T.ATKVIS	T.TOEDATA	T.TOEFCN	T.NONAPP
O.MEDAPP						X
O.MEDEXT				X	X	
O.DSPAPP						X
O.DSPSYS			X			
O.AUDIT			X			
O.SELFPRO		X				
O.NETATK	X					
O.ADMIN				X	X	X

Table 5 Mapping of TOE Security Objective to Threats

T.TOEDOS *An external network user or IT entity user may compromise TOE integrity and/or availability by conducting Denial of Service attacks against TOE resources.*

O.NETATK protects the TOE from Denial of Service attacks via TOE network interfaces.

T.TOEPRO *An external network user or IT entity user may bypass, deactivate, or tamper with TOE security functions.*

O.SELFPRO protects the TOE from attempts by an external network user or IT entity to bypass, deactivate, or tamper with TOE security functions.

T.ATKVIS *An external network user or IT entity may conduct undetected attack attempts against the TOE.*

O.DSPSYS displays to the user the current network activity associated with external network entities accessing, or attempting to access, the TOE. O.AUDIT records a readable audit trail of allowed and denied external network access attempts, and permits the user to review the audit log entries.

T.TOEDATA *An external network user or IT entity may read, modify or destroy TOE internal data.*

O.MEDEXT mediates network access to and from the TOE itself via each network NDIS interface. O.ADMIN permits the user to manage network access of internal TOE data by an external network user or IT entity.

T.TOEFCN *An external network user or IT entity may access and use security and/or non-security functions of the TOE.*

O.MEDEXT mediates network access to and from the TOE itself via each network NDIS interface. O.ADMIN permits the user to manage network access by an external network user or IT entity.

T.NONAPP *A local user may be unaware that an unauthorized Winsock application, executing on the TOE, is accessing the network via TOE network interfaces.*

O.MEDAPP mediates the capability of Winsock applications executing on the TOE to communicate over TOE network NDIS interfaces. O.DSPAPP displays to the user the current and recent history of network activity associated with Winsock applications executing on the TOE. O.ADMIN permits the user to manage network access by Winsock applications.

8.1.2 Environment Security Objectives Rationale

Table 6 provides a bi-directional mapping of Environment Security Objectives to Assumptions and Threats, and is followed by a discussion of how each Assumption or Threat is addressed by the corresponding Environment Security Objectives.

	A.PHYSEC	A.NETWS	A.USRADM	A.NOIA	A.NOEVIL	A.LOCADM	A.CMPTIF	A.USRKNW	A.NOROUTE	A.BADAPP	A.APPFLAW	T.USAGE	T.TROJAN
O.GUIDAN		X	X		X	X	X	X	X	X	X	X	X
O.AUTHUSR	X			X		X							

Table 6 Mapping of Environment Security Objectives to Threats and Assumptions

A.PHYSEC *The TOE is physically secure.*

O.AUTHUSR ensures that only authorized users be permitted physical access to the TOE.

A.NETWS *The TOE is functioning as a single-user, networked workstation. The sharing of TOE resources with external network IT entities is limited to the peer-to-peer file and print sharing capabilities provided by the underlying TOE operating system.*

O.GUIDAN ensures that the user administers and operates the TOE in a manner that maintains its security.

A.USRADM *The user of the TOE is also the administrator who manages TOE security functions.*

O.GUIDAN ensures that the user is responsible for administering the security of the TOE.

A.NOIA *The TOE does not provide any user identification or authentication functionality.*

O.AUTHUSR ensures that only authorized users be permitted physical access to the TOE.

A.NOEVIL *Users are non-hostile and follow all administrator guidance; however, they are capable of error.*

O.GUIDAN ensures that the user administers and operates the TOE in a manner that maintains its security.

A.LOCADM *Administration of TOE security functions is only conducted locally from the TOE HMI.*

O.GUIDAN ensures that the user administers and operates the TOE in a manner that maintains its security. O.AUTHUSR ensures that only authorized users be permitted physical access to the TOE.

A.CMPTIF *Only network devices compatible with CPD are installed and functioning within the TOE. This includes Ethernet-like network devices, but excludes Token Ring, FDDI, Frame Relay and X.25 network devices.*

O.GUIDAN ensures that the user installs and configures the TOE in a manner that maintains its security.

A.USRKNW *The user is knowledgeable of TOE applications that require network access.*

O.GUIDAN ensures that the user administers and operates the TOE in a manner that maintains its security.

A.NOROUTE *The TOE does not route traffic between network interfaces.*

O.GUIDAN ensures that the user installs and configures the TOE in a manner that maintains its security.

A.BADAPP *Users do not execute applications on the TOE that communicate over network interfaces, but bypass TOE security functionality. This includes applications and protocols that interface directly with the network device drivers, bypassing the Winsock protocol stack and NDIS interface.*

O.GUIDAN ensures that the user installs and configures the TOE in a manner that maintains its security.

A.APPFLAW *The TOE cannot protect against an external network user or IT entity that exploits flaws in authorized application or service implementations, to read, modify or destroy TOE internal data.*

O.GUIDAN ensures that the user configures, administers and operates the TOE in a manner that maintains its security.

T.USAGE *The TOE may be configured, used and administered in an insecure manner.*

O.GUIDAN ensures that the user configures, administers and operates the TOE in a manner that maintains its security.

T.TROJAN *Compromise of the integrity and/or availability of the TOE may occur as a result of a TOE user unwittingly introducing a virus or trojan into the system.*

O.GUIDAN ensures that the user administers and operates the TOE in a manner that maintains its security.

8.2 SECURITY REQUIREMENTS RATIONALE

8.2.1 Security Functional Requirements Rationale

Table 7 provides a bi-directional mapping of Security Functional Requirements to Security Objectives, and is followed by a discussion of how each Security Objective is addressed by the corresponding Security Functional Requirements.

	O. MEDAPP	O. MEDEXT	O. DSPAPP	O. DSPSYS	O. AUDIT	O. SELFPRO	O. NETATK	O. ADMIN	O. GUIDAN	O. AUTHUSR
FAU_ GEN.1					X					
FAU_ SAR.1					X					
FAU_ SEL.1					X					
FAU_ STG.4							X			
FDP_ IFC.1(1)	X									
FDP_ IFC.1(2)		X				X				
FDP_ IFF.1(1)	X						X			
FDP_ IFF.1(2)		X					X			
FMT_ MOF.1			X	X	X			X		
FMT_ MSA.3						X				
FPT_ STM.1					X					

Table 7 Mapping of Security Functional Requirements to Security Objectives

O.MEDAPP *The TOE must mediate the capability of Winsock applications executing on the TOE to communicate over TOE network interfaces.*

FDP_IFC.1 (1) together with FDP_IFF.1 (1) requires that the TOE mediate the capability of Winsock applications executing on the TOE to communicate over TOE network interfaces, permitting communication when the application is trusted by the user, and denying communication when the application is not trusted by the user.

O.MEDEXT *The TOE must mediate network access to and from the TOE itself at the NDIS layer of each network interface.*

FDP_IFC.1 (2) together with FDP_IFF.1 (2) requires that the TOE mediate the network access via each network NDIS interface by TOE system services and external IT entities, in accordance with the system access settings selected by the user.

O.DSPAPP *The TOE must display to the user the current and recent history of network activity associated with Winsock applications executing on the TOE.*

FMT_MOF.1 provides the user with the capability to select the level of network activity that is displayed on the HMI.

O.DSPSYS *The TOE must display to the user the current network activity associated with the TOE operating system accessing, or attempting to access, networks, and external network entities accessing, or attempting to access, the TOE.*

FMT_MOF.1 provides the user with the capability to select the level of network activity that is displayed on the HMI.

O.AUDIT *The TOE must record a readable audit trail of TOE network activity and security relevant events, and permit their review by a user.*

FAU_GEN.1 and FAU_STM.1 combine to require that a readable audit trail of network activity and security related events is recorded with reliable time stamps. FAU_SAR.1 provides the user with the capability to review the audit trail. FAU_SEL.1 and FMT_MOF.1 combine to provide the user with the capability to select what level of network activity is recorded in the audit trail.

The following events that would normally be subject to audit at the Basic audit level are not audited for the reasons indicated:

Functional Component	Auditable Event	Rationale for Exclusion
FAU_SAR.1	Reading of information from the audit records.	This audit requirement is based on the TOE requirement to limit access to audit records to authorized users. In this case, user authorization is a requirement met by the non-IT environment in that physical access to the TOE determines whether a user is authorized or not. As a result, since the TOE itself cannot determine if a user is authorized, this auditing requirement is not applicable.
FMT_MSA.3	All modifications of the initial value of security attributes.	This audit record is related to the TOE mediating object and information security attributes. The TOE presented in this ST does not mediate objects and information, hence this audit requirement is not applicable.
FPT_STM.1	Changes to the time.	This audit requirement has not been included because: • The only security functionality that relies on TOE system time is the time stamping of audit log entries. Since the TOE maintains the sequence of audit entries in the log, regardless of changes in system time, any relevant changes in system time would be apparent. • Authorized users, or applications executing on the TOE must initiate system time changes.

Functional Component	Auditable Event	Rationale for Exclusion
		Users are assumed to be knowledgeable of the applications they are running, and hence are aware of changes in system time they initiate. If the operating system itself changes system time (e.g., daylight saving time changes), the user is notified. • System time is maintained by the operating system. In this case, the TOE operating system, Windows 98, does not support a capability to audit system time changes.

O.SELFPRO *The TOE must protect itself against attempts by an external network user or IT entity to bypass, deactivate, or tamper with TOE security functions.*

FMT_MSA.3 requires that the default TOE configuration deny information flow, via network interfaces, to and from the TOE. FDP_IFF.1 (2) requires that all external network access be denied unless specifically permitted by the security policy specified by the administrator.

Element FMT_MSA.3.2 has been included as the complete set of functional elements of a component must be selected for inclusion in an ST. The TOE presented in this ST does create, modify or delete objects and information. Therefore the concept of specifying alternative initial values when an object or information is created does not apply, and FMT_MSA.3.2 is not applicable.

O.NETATK *The TOE must protect itself from Denial of Service attacks against the TOE via TOE network interfaces.*

FAU_IFF.1 (1) and FAU_IFF.1 (2) combine to provide the TOE with the capability to protect itself from network Denial of Service attacks against the TOE IP stack, and from ICMP flooding. FAU_STG.4 requires that the TOE ignore auditable events when the audit trail is full, preventing storage resource exhaustion as a Denial of Service attack against the TOE.

O.ADMIN *The TOE must provide functionality that enables an administrator to effectively manage the TOE and its security functions from its local HMI.*

FMT_MOF.1 provides the administrator with the capability to manage the TOE and its security functions from its local HMI.

O.GUIDAN *The user responsible for the TOE must ensure that the TOE is delivered, installed, configured, administered, and operated in a manner that maintains its security.*

This objective is satisfied by non-IT environment security requirements that do not relate directly to the implementation of the TOE and are not included in the ST.

O.AUTHUSR *Only authorized users are permitted physical access to the TOE.*

This objective is satisfied by non-IT environment security requirements that do not relate directly to the implementation of the TOE and are not included in the ST.

8.2.2 Assurance Requirements Rationale

The *CPD* product is designed to protect the TOE PC and data from network attacks, to limit the system's use of network interfaces to what the user wants, and to be simple enough for an average PC user to use. An assurance level of EAL 1, Functionally Tested, was selected as the threat to security is considered to be unsophisticated network attackers, and the data to be protected consists primarily of user-private data and system resources. It is felt that an evaluation at this level provides evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.

8.2.3 Rationale for Not Satisfying All Dependencies

Table 8 identifies the ST Security Functional Requirements and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency. For those cases where dependencies have not specifically been addressed, explanations of the rationale for excluding them are provided.

ST Requirement	Dependencies	Dependency Satisfied?
FAU_ GEN.1	FPT_STM.1	Y
FAU_ SAR.1	FAU_GEN.1	Y
FAU_ SEL.1	FAU_GEN.1	Y
	FMT_MTD.1	N
FAU_ STG.4	F MT_STG.1	N
FDP_ IFC.1(1)	FDP_IFF.1 (1)	Y
FDP_ IFC.1(2)	FDP_IFF.1 (2)	Y
FDP_ IFF.1(1)	FDP_IFC.1 (1)	Y
	FMT_MSA.3	Y
FDP_ IFF.1(2)	FDP_IFC.1 (2)	Y
	FMT_MSA.3	Y
FMT_ MOF.1	FMT_SMR.1	N
FMT_ MSA.3	FMT_MSA.1	N
	FMT_SMR.1	N
FPT_ STM.1	-	-

Table 8 Security Functional Requirement Dependencies

Functional components FMT_MOF.1 and FMT_MSA.3 depend on functional component FMT_SMR.1, Security Roles.

The concept of ‘security roles’ does not apply to the TOE. By assumption, the TOE is considered to be a single-user workstation, where the user is also considered to be the TOE administrator. Therefore, there is no need to distinguish and control the assignment of different roles to users, and a requirement satisfying this dependency has not been included.

Functional component FAU_SEL.1 depends on functional component FMT_MTD.1, Management of TSF Data.

FAU_SEL.1, Selective Audit, depends on functional component FMT_MTD.1, which requires only authorised roles manage TSF data. As detailed above, the concept of ‘security roles’ does not apply to this TOE, and any user with access to the TOE may manage TSF data. Therefore, a requirement satisfying this dependency has not been included.

Functional component FAU_STG.4 depends on functional component FAU_STG.1, Protected Audit Trail Storage.

FAU_STG.4 specifies TOE requirements if the audit trail is full. This requirement has been incorporated in order to prevent the exhaustion of TOE storage resources as a means of conducting a denial of service attack on the TOE. FAU_STG.4 depends on FAU_STG.1, which requires the TOE protect the stored audit records from unauthorized deletion. By assumption, any TOE user is authorized, and has full access to TOE resources including the TOE audit logs. Therefore, the concept of unauthorized deletion does not apply and a requirement satisfying this dependency has not been included.

Functional component FMT_MSA.3 depends on functional component FMT_MSA.1, Management of Security Attributes

In an effort to consolidate all management requirements in a central place, FMT_MOF.1 more than adequately satisfies the concerns of not including a requirement satisfying this dependency. In addition, FMT_MSA.1 depends on the concept of ‘security roles’, which is not applicable to this TOE.

8.3 TOE SUMMARY SPECIFICATION RATIONALE

8.3.1 TOE Security Functions Rationale

Table 9 provides a bi-directional mapping of Security Functions to Security Functional Requirements, and is followed by a discussion of how each Security Functional Requirement is addressed by the corresponding Security Function.

	FAU_ GEN.1	FAU_ SAR.1	FAU_ SEL.1	FAU_ STG.4	FDP_ IFC.1(1)	FDP_ IFC.1(2)	FDP_ IFF.1(1)	FDP_ IFF.1(2)	FMT_ MOF.1	FMT_ MSA.3	FPT_ STM.1
F.APPCTL					X		X				
F.SYSCTL						X		X			
F.NETATK							X	X			
F.BLKOTH							X	X			
F.OVRIDE							X	X			
F.GUI									X		
F.INIT										X	
F.AUDEVT	X		X								
F.AUDINF	X										
F.AUDRVW		X									
F.TIME											X
F.AUDLOG				X							

Table 9 Mapping of Security Functions to Security Functional Requirements

FAU_GEN.1 *Audit data generation*

F.AUDEVT and F.AUDINF combine to satisfy the requirement for the generation of audit data for the specified set of TOE events.

FAU_SAR.1 *Audit review*

F.AUDRVW satisfies the requirement for the TOE to provide the user with the capability to view, modify or delete audit record logs.

FAU_SEL.1 *Selective Audit*

F.AUDEVT satisfies the requirement for the user to be able to select the events to be audited, based on event type.

FAU_STG.4 *Prevention of audit data loss*

F.AUDLOG satisfies the requirement for the TOE to ignore auditable events and create a log entry indicating that event auditing has been stopped when the audit log is full. It also specifies the system errors and changes in TOE security functionality shall continue to be logged.

FDP_IFC.1 *Subset information flow control (1)*

F.APPCTL satisfies the requirement to enforce information control on TOE Winsock applications that send and receive information over TOE network interfaces.

FDP_IFC.1 *Subset information flow control (2)*

F.SYSCTL satisfies the requirement to enforce information control on TOE system services and external IT entities that send and receive information to and from the TOE over network interfaces.

FDP_IFF.1 *Simple security attributes (1)*

F.APPCTL, F.NETATK, F.BLKOTH and F.OVRIDE combine to satisfy the requirement to mediate network access by Winsock applications, executing on the TOE.

FDP_IFF.1 *Simple security attributes (2)*

F.SYSCTL, F.NETATK, F.BLKOTH and F.OVRIDE combine to satisfy the requirement to mediate network access by TOE services and external IT entities.

FMT_MOF.1 *Management of security functions behaviour*

F.GUI satisfies the requirement for the TOE to provide the user with the capability to manage the security functions of the TOE.

FMT_MSA.3 *Static attribute initialization*

F.INIT satisfies the requirement for the default TOE configuration to restrict network access to the minimum required to establish network connectivity.

FPT_STM.1 *Reliable time stamps*

F.TIME satisfies the requirement for the TOE to provide a reliable time and date for the time stamping audit log entries.

8.3.2 TOE Assurance Measures Rationale

Table 10 provides a bi-directional mapping of Assurance Measures to Assurance Requirements, and is followed by a short discussion of how the Assurance Requirement are addressed by the corresponding Assurance Measures.

	ACM_CAP.1	ADO_IGS.1	ADV_FSP.1	ADV_RCR.1	AGC_ADM.1	AGD_USR.1	ATE_IND.1
M.ID	X						
M.SETUP		X					
M.SPEC			X				
M.TRACE				X			
M.DOCS					X	X	
M.TEST							X

Table 10 Mapping of Assurance Measures to Assurance Requirements

With the exception of AGC_ADM.1 and AGD_USR.1, there is a self-evident one-to-one correspondence between the Assurance Requirements and the Assurance Measures that satisfy those requirements.

AGC_ADM.1, Administrator Guidance, and AGD_USR.1, User Guidance, are satisfied by M.DOCS, which encompasses both Administrator and User guidance in a single documentation set (an on-line help file).

9 ACRONYMS AND ABBREVIATIONS

Acronym	Definition
ARP	Address Resolution Protocol
CC	Common Criteria for Information Technology Security Evaluation
CPD	ConSeal Private Desktop
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
HMI	Human Machine Interface
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IT	Information Technology
NBT	NetBIOS over TCP/IP
NDIS	Network Driver Interface Specification
NIC	Network Interface Card
PC	Personal Computer
RIP	Routing Information Protocol
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
UDP	User Datagram Protocol
Winsock	Windows sockets
Wintel	Windows/Intel