# Diamond*TEK*
# Security Target

**Revision 1.0**
June 25, 2002

**Prepared for:**
Cryptek, Inc.
1501 Moran Road
Sterling VA 20166
USA

CRYPTEK
SECURE COMMUNICATIONS

**Prepared By:**

SAIC
An Employee-Owned Company

Science Applications International Corporation

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

**Restricted Rights Legend**

USE, DUPLICATION, OR DISCLOSURE IS SUBJECT TO THE RESTRICTIONS AS SET FORTH IN SUBPARAGRAPH [C][1][II] OF THE RIGHTS IN TECHNICAL DATA AND COMPUTER SOFTWARE CLAUSE OF DFARS 252.227-7013 (OR AT FAR 52.227 [C][1]).

## LIST OF TABLES

# 1. Security Target Introduction

This section identifies the Security Target and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization.

## 1.1 Security Target, TOE and CC Identification

**ST Title –** Diamond*TEK* Security Target

**ST Version** – Revision 1.0

**ST Date** – June 25, 2002

**TOE Identification** – The Diamond*TEK* TOE consists of the following components:

- Diamond*Central* (part number: DC1, DC2, or DC3[1])
    - NSC Application S/W version 2.0.1
    - NSD-Prime F/W version 2.1.4
- Diamond*Link* (part number: DL100, DL100F[2])
    - F/W version 2.1.4
- Diamond*Pak* (part number: DP200, DP400, DP600[3])
    - F/W version 2.1.4
- Diamond*VPN* (part number: DV100)
    - F/W version 2.1.4
- Applicable Guidance Documents:
    - Diamond*TEK*™ 10/100 Secure Network Administration, Version 2.0.1, 19 March 2002
    - Release Notes for Diamond*TEK*™ 10/100 Secure Network Administration, Version 2.0.1, 19 March 2002
    - Diamond*TEK*™ 10/100 Secure Network Commands Manual, Version 2.0.1, 8 February 2002
    - Diamond*TEK*™ 10/100 User Pamphlet , 3/6/2002
    - Diamond*TEK* User's Guide, Revision 1.03, November 1, 2001

**CC Identification** – Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408.

## 1.2 Conformance Claims

This TOE conforms to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.1, August 1999, ISO/IEC 15408-2.

[1] DC1 supports 10 users and 250 DiamondTEK nodes. DC2 supports 10 users and 1000 DiamondTEK nodes. DC3 supports 10 users and unlimited DiamondTEK nodes.

[2] DL100 supports RJ-45 copper network interface. DL100F supports a fiberoptic network interface.

[3] DP200 supports two servers. DP400 supports four servers. DP600 supports six servers.

  - Part 2 Conformant

- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.1, August 1999, ISO/IEC 15408-3.

  - Part 3 Conformant

  - Evaluation Assurance Level 4 (EAL 4).

## 1.3 Strength of Environment

DiamondTEK provides a level of protection that is appropriate for IT environments that require that information flows be controlled and restricted among network nodes where the DiamondTEK components can be appropriately protected from physical attacks. Essentially, the DiamondTEK management console[4] must be controlled to restrict access only to authorized administrators; and while the operational DiamondTEK components[5] are protected from theft and tampering by means of encryption techniques and FIPS level 2 tamper resistance standards, it is expected that they will be protected to the extent necessary to ensure they remain connected to the hosts they protect. Essentially, this means that the DiamondTEK components need to be protected to the degree appropriate to protect the host to which they are connected. The assurance requirements, EAL 4, and the minimum strength of function, SOF-medium, were chosen to be consistent with those environments.

## 1.4 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target.

### 1.4.1 Conventions

The following conventions have been applied in this document:

- All requirements in this ST are reproduced relative to the requirements defined in CC v2.1.

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.

  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1(a) and FDP_ACC.1(b) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.

  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).

  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).

- Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").

- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

### 1.4.2 Terminology and Acronyms

The following terms and acronyms are used in this Security Target:

[4] The "DiamondTEK management console" is known as a Network Security Controller (NSC) and is described later in this document.

[5] The phrase "operational DiamondTEK components" represents Network Security Devices (NSDs), which are described later in this document.

- Association Profile - The profile associated with each user[6] that defines the Association Security Policy and Packet Filter Policy attributes.
- Association Security Policy – The policy that dictates whether information can flow based on the explicit definition of information flows based on source and destination address, as well as encryption properties.
- Clear Text Node (CTN) – A node that does not require encryption in order to send or receive information.
- Common IP Security Option (CIPSO) – FIPS 188
- Diamond*Central* – The network entity used by the NSM to manage the Diamond*TEK* system.
- Diamond*Link* – One type of NSD used to protect and control a single Host that already has an installed NIC.
- Diamond*Pak* – One type of NSD used to protect and control a set of Hosts (e.g., servers) with an Association and Mandatory Security Profile per connected Host.
- Diamond*TEK* – The TOE; a collection of network Nodes (i.e., NSDs attached to Hosts) and a Diamond*Central*.
- Diamond*VPN* – One type of NSD used to protect and control a fixed network entity or collection of such entities (e.g., sub-network).
- Host - This term is used to refer to the component (e.g., computer) or set of components (e.g., sub-network) that is protected and controlled by a NSD.
- Internet Protocol Security (IPsec) – RFC 2401 – 2406.
- Mandatory Security Policy – The policy that dictates the rules by which information can flow based on security labels.
- Network Security Controller (NSC) – See Diamond*Central*, above. Note that NSC is also sometimes expanded to "Network Security Console" or "Network Security Center", which in the context of a Diamond*TEK* system all represent the same thing (i.e., Diamond*Central*).
- Network Security Device (NSD) – This is the part of the TOE that actually enforces the information flow policies, identifies and authenticates users, and generates and sends audit records to the NSC.
- Network Security Manager (NSM) – This is the name of the authorized administrator in the Diamond*TEK* system.
- Network Interface Card (NIC) – A device that is used to connect a host to a network.
- No-Card Node – A Node that does not require a card to be inserted by a user in order to interact with the network. These Nodes are generally only used for static network Nodes (e.g., servers or VPNs).
- Node – This term is used to refer to the component (e.g., computer) or set of components (e.g., sub-network) that is protected and controlled by a NSD in combination with the NSD itself. Note that "Host" is used to refer to these components *without* including the NSD. Note also that the term "node" is used to refer to components or sets of components on the network, but are not necessarily protected and controlled by a NSD (e.g., a CTN).
- Operational Profile – The profile associated with an identified and authenticated user that contains his Association Profile and Security Profile that controls the flow of traffic on the attached network.
- Other IPsec (OIPS) – This term is used to identify a non-Diamond*TEK* entity, or a Diamond*TEK* entity controlled by another NSC, that is attached to the network and capable of successfully negotiating an IPsec exchange with a NSD.

[6] Note that statically configured devices, such as servers or VPNs, have pseudo users, and thereby Association Profiles, associated with them.

- Packet Filter Policy – The policy that, in conjunction with the Association Security Policy, dictates whether information can be sent or received based on network protocol and service.
- PIN – Personal Identification Number; used to support authentication of a user in conjunction with a personal access card.
- security label – the combination of a security level and a set of security categories to fully identify or classify a subject or object.
- security level – hierarchical part of a security label; typically used to refer to one of a set of identifying properties that share a hierarchically ordered relationship.
- security category – non-hierarchical part of a security label; typically used to refer to one of a set of identifying properties that are not comparable.
- Security Profile – The profile that is assigned with each NSD and user that defines the Mandatory Security Policy attributes.
- User – Used to refer to any individual that is or (may attempt to be) identified and authenticated in the context of a NSD and is accountable in the Diamond*TEK* system. Note that this term is also used to refer to the definition the TSF associated with the actual user.

## 1.5 Security Target Overview and Organization

The Diamond*TEK* Target of Evaluation (TOE) primarily supports the definition of and enforces information flow policies among network nodes. Part of the Diamond*TEK* TOE is installed at every protected network connection and a management center (the Network Management Console (NSC) is attached to the network to enable centralized network security management. Information flow is controlled on the basis of: security labels associated with network nodes and information packets on the network; explicit assignment of allowed information flow paths on the network; and, addresses, protocols and services associated with network traffic. In support of the information flow security functions, Diamond*TEK* requires users to be identified and authorized, ensures that security relevant activity is audited, ensures that its own functions are protected from potential attacks, and provides security tools to manage all of the security functions.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Environment (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8).

# 2. TOE Description

Diamond*TEK* is designed and manufactured by Cryptek Secure Communications, LLC, located in Sterling, Virginia, hereinafter called Cryptek. Diamond*dTEK* enforces a centrally defined security policy for the flow, encryption, and auditing of data packets transferred between nodes in a network. The Target of Evaluation (TOE), shown in Figure 1, is the portion of the network responsible for enforcing the network's security policies. It includes:

- a Network Security Controller (NSC), also referred to as Diamond*Central*, including:
  - the NSC application,
  - a special Network Security Device (NSD) known as NSD-Prime (and associated driver), and
  - a card reader/writer used to create User Authentication cards and NSD Installation cards; and,
- one or more Diamond*Link*, Diamond*Pak*, and/or Diamond*VPN* Network Security Devices (NSDs), each mediating between one or more network nodes and a network topology.

Diamond*TEK* is a trusted access control system that provides the highest level of protection available for corporate information assets. It's innovative technology removes the remaining hurdles to the secure access of corporate data by vendors, customers, suppliers, partners, and employees, enabling businesses to safely launch network-based initiatives.

Diamond*TEK* protects enterprise data, applications, and networks, by employing end-to-end security and access control at the data level to create the most trusted secure access path possible. Diamond*TEK* is a system comprised of easy-to-use, interoperable hardware appliances consisting of: Diamond*Central* – a centralized GUI security configuration and management station; Diamond*Link* – a drop-in appliance for securing individual nodes; Diamond*Pak* – a multi-channel rack appliance for protecting servers; and Diamond*VPN* – a drop-in network appliance for securing groups of nodes. Diamond*TEK* provides a seamless end-to-end information security solution that directly addresses the most critical enterprise security needs. The system has been created so that we can provide customers the best value, balancing tolerance for risk against the available budget.

Diamond*TEK* represents a next generation in network security. The first generation was comprised of devices to eliminate the problems caused by reusable passwords. The second was the firewall, invented to protect the perimeter of the business enterprise against attacks from the outside. The third and most recent is the Virtual Private Network (VPN) for securing network communications over the Internet and providing remote access to corporate resources by traveling employees and telecommuters.

We consider Diamond*TEK* a fourth generation product because it was specifically designed to provide comprehensive internal protection for sensitive information and to control information access by those authorized to use the network. Although the underlying technology makes Diamond*TEK* competitive for perimeter security and remote access, its greatest value lies in directly and proactively protecting information assets within the corporation.

Diamond*TEK* employs two innovative technologies - Dynamic Secure Virtual Networks (DSVN$_{tm}$) and Data Driven Access Control (DDAC$_{tm}$). DSVN technology enables the creation of multiple secure virtual networks (SVN) while allowing individual users to access specific SVNs as needed. This role based access control is centrally monitored and audited to provide a record of network usage. Network activity that violates security policy is prevented and alarms are triggered by attempts to breach security. By virtue of the NSC, new SVNs can be created and changed on the fly during normal operations, as the needs and policies of the business change.

Diamond*TEK* combines many of the features of point security products into a single best of breed offering. One significant benefit is that it reduces the interoperability and management issues that arise when a comparable security solution is created by combining point solutions from various suppliers. Perhaps an even more significant benefit is DDAC. This unique feature enables Diamond*TEK* to create data-aware networks and to extend the trusted path all the way into the data. This fine-grained access control, coupled with Diamond*TEK*'s high level of trust, takes the network to a level of security and flexibility never before available.

Note that in Figure 1 below, a "Node" is represented as a single computer, a collection of servers, and an entire network. The network security devices (NSDs), illustrated in Figure 1, could be any of the supported variations, listed above, and would be selected to appropriately support the attached "Node." Note also that the "Physical Network" need not be protected itself. If it were protected, there would be no need to encrypt traffic between the NSDs. However, the NSDs can be configured to encrypt their network traffic to support environments that do not include physical network protection.

Diamond*TEK* operates at the Network layer (layer 3) of the protocol stack, using Internet Protocol Version 4 (IPv4) networking. Diamond*TEK* is capable of protecting data on the open Internet, as well as on an internal Ethernet LAN. Non-IP based protocols are supported by tunneling across the IP network.

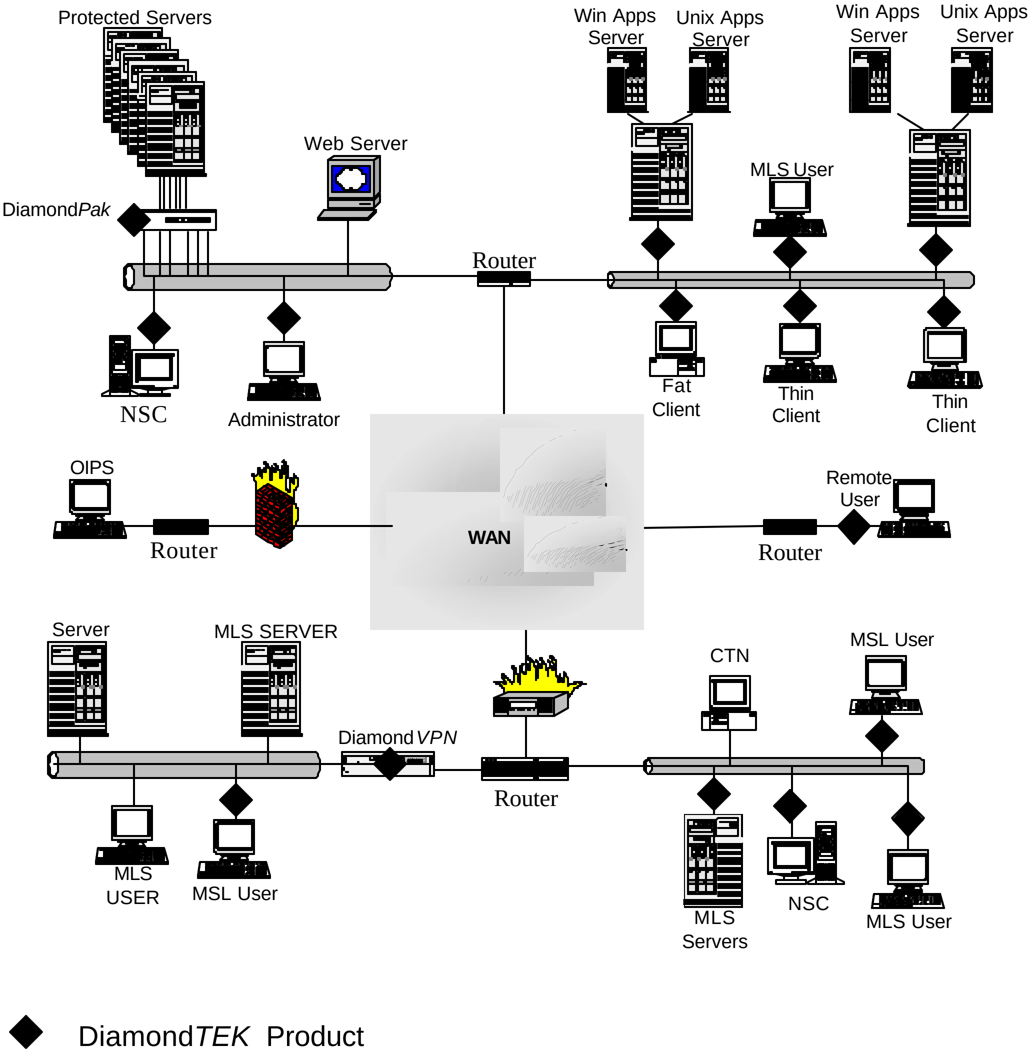

Figure 1 Logical Security Perimeters

## 2.1 Product Type

Diamond*TEK* is a secure network product designed to control the flow of information to and from nodes and access to Nodes on a network. It can be used on a closed, or otherwise protected, network using clear text interactions or alternately on an open, or unprotected, network using encryption technology, if necessary, to protect data and enforce policies.

## 2.2 Product Description

As shown in figure 1, Diamond*TEK* consists of a number of components. Each protected Node is connected to the physical network via a NSD (the combination of Host and NSD being referred to as a Node). For a single Host, the NSD is a Diamond*Link* that is installed between any NIC and a physical network. When dealing with multiple nodes (e.g., a sub-network or group of servers), the NSD may be either a Diamond*VPN* that is installed as a single point of control for all of the nodes (collectively referred to as a Host) that may be attached to it, or a Diamond*Pak* that is rack mounted and can serve to protect a set of Hosts (e.g., servers) each with its own Operational Profile. Each of the NSDs has an associated card reader that can be used to install the device and read the cards of individual users in order to identify and authenticate them. However, NSDs can be configured to not require card-based authentication (i.e., No-Card Nodes). This option is used for fixed, permanent network entities (e.g., servers, sub-network) where a user will be defined exclusively to represent the Node in the Diamond*TEK* system.

Note that while the DiamondTEK system can include a number of NSDs, it can also be configured to recognize clear text nodes (CTNs) and other IPsec (OIPS) nodes. While the Diamond*TEK* system cannot fully control information flows between CTNs and OIPSs, it does control the flow of information between them and NSDs. As such, CTNs and OIPSs can only interact with NSDs after they have been defined in the Diamond*TEK* system and are assigned appropriate information flow attributes to control information flows appropriately.

The Diamond*Central* (or NSC) is a special purpose computer designed to manage the Diamond*TEK* system. The NSC communicates with NSDs under its control via its own special NSD (sometimes referred to as NSD Prime). The NSC provides an interface and tools for the Network Security Manager (NSM). Via the NSC, the NSM configures and manages the Diamond*TEK* system, including controlling access policies, reviewing audit data, defining operational parameters, defining users, configuring NSDs, etc.

## 2.3 Product Features

A Diamond*TEK* system offers the following security functions:

- Audit: audit data regarding NSM activities, policy violations, and network traffic is sent to the NSC and can then be reviewed by the NSM.
- Mandatory Security Policy: each NSD on the network is assigned ranges of security levels and security categories that control what information can be sent and received by that NSD. Additionally, each user is assigned one or more profiles that can be selected at log in, provided the selected profile is within the range defined for the applicable NSD, and control what information can be sent and received by the user.
- Association Security Policy: each user is assigned one or more profiles that can be selected at log in and explicitly define which nodes they can send information to or receive information from. In addition to explicitly allowing information flows, the profiles indicate whether information must be encrypted or is allowed to flow in plain-text between Nodes.
- Packet Filter Policy: each user on the network can be assigned a set of rules that extend the Association Security Policy to effectively control whether network traffic can be sent or received according to protocol, and service in addition to source and destination address.
- Identification & Authentication: all users are required to be identified and authenticated before they can perform any other functions. Users are identified and authenticated by means of a card, used in the card reader associated with an NSD, and an associated PIN. NSMs are identified by means of a user ID and password at the NSC console.

- Security Management: the NSC includes a number of tools, available only to the NSM, which can be used to effectively manage the security of the Diamond*TEK* system.
- TOE protection: each NSD is a hardware device that protects itself largely by offering only a minimal logical interface to the network and attached Nodes. Cryptography is used to protect TSF data that is being passed between the NSD and the NSC (or NSD prime). Each NSD is expected to be protected as necessary to ensure it remains attached to the host it protects. The NSC is expected to be in a well-controlled environment.
- Cryptographic Support: each NSD has the ability to negotiate key exchanges and encrypt information to be protected en route to another NSD or OIPS. This support is used in conjunction with the Association Security Policy and TOE protection.

## 2.4 Security Environment TOE Boundary

The TOE includes both physical and logical boundaries.

### 2.4.1 Physical Boundaries

The physical boundary of the Diamond*TEK* system surrounds the NSD and NSC components.

The NSC attaches to the physical network and offers interactive user support primarily in the form of a graphical user interface. Note that the NSC is primarily an application running on a Windows 2000 Professional system and can offer any support that the operating platform can provide (e.g., removable media, printer). Windows 2000 Professional is shipped as part of the product but is not included in the TOE; Windows 2000 Professional is addressed by the IT Environment descriptions and requirements. The NSC application communicates with associated NSDs via its own special NSD, known as NSD-Prime. The NSC application also utilizes a card reader/writer device in order to create User Authentication cards and NSD Installation cards. However, the operating system, and associated hardware, is included largely by assumption and is not directly part of the TOE.

The NSDs come in three basic types: Diamond*Link*, Diamond*VPN*, Diamond*Pak*. In the case of Diamond*Link*, the physical interfaces are a standard network connection to a NIC installed on the associated Host and the connection to the physical network. A card reader offers an interface for users to insert their assigned cards, and optionally enter a PIN, for the purpose of identification and authentication and also to select an Operational Profile. In the case of Diamond*VPN*, the physical interfaces include two networks – one over which Diamond*TEK* controlled traffic flows and another that is treated as a single, fixed entity (referred to as a Host for convenience) with regard to Diamond*TEK* security policies. In the case of Diamond*Pak*, the physical interfaces include the physical network and a series of Hosts (e.g., servers) that will each be treated as a Host inasmuch as they each have their own security profile, though managed by a single physical device. Both the Diamond*VPN* and Diamond*Pak* have integrated card readers, but they are used solely for installation, unlike those of the other two types of NSD.

### 2.4.2 Logical Boundaries

The logical boundaries of the Diamond*TEK* system include the interfaces to communicate between the Hosts and their corresponding NSDs and the interfaces between the NSD and physical network to send and receive network traffic.

Each NSD will only forward data to their associated Host if it satisfies the information flow policies configured in the Diamond*TEK* system. If data is received by a NSD that does not conform to those policies, it will be discarded and an audit record will be sent to the NSC. A Host can freely send information to its associated NSD, but the NSD will only forward that information, in the form of network traffic, if it is properly formatted so that the NSD can interpret necessary parts (e.g., label) and if it conforms with applicable policies.

In short, Diamond*TEK* provides the following security services.

#### 2.4.2.1 Audit

When a NSD state changes (e.g., it starts) or a NSD determines that an attempt to violate a security policy has occurred, it forwards an audit record to the NSC. Additionally, NSDs can forward audit records related to general network usage (e.g., TCP connects) that will optionally be recorded by the NSC. The NSC uses the services of its host operating system to record and review audit records received from NSDs as well as audit records related to security management of the Diamond*TEK* system generated by the NSC itself.

#### 2.4.2.2 Information Flow Protection

Diamond*TEK* offers three distinct information flow security features. One is based on security labels (Mandatory Security Policy), another is based on explicitly defined information flow paths (Association Security Policy), and the last is based on source and destination addresses in combination with network protocol and service (Packet Filter Policy).

The Mandatory Security Policy is supported by requiring the labeling of each subject (NSD) and object (network packet). A NSD can only send or receive packets that have labels that fall within the range of labels assigned to the NSD. If a Host doesn't label information intended to be sent out by its NSD, the NSD will attach a default label as defined in the appropriate security profile.

The Association Security Policy is supported by allowing an administrator, the Network Security Manager (NSM), to define profiles that specify which network nodes can communicate with which other network nodes. When a user logs into a NSD, he must select a profile that has been made available to him by the NSM. Subsequently, that NSD can only send information to other NSDs, CTNs, and/or OIPSs as allowed by that profile. Additionally, the profile must indicate whether the information must be encrypted or whether it can be sent in clear-text. If it must be sent encrypted, the NSD can negotiate to exchange keys with the destination NSD or OIPS and subsequently encrypt the information flowing between them.

The Packet Filter Policy is supported simply by allowing the NSM to add rules based on network protocol and service to the set of rules related to the Association Security Policy (which deals with source and destination address) that will be used to decide whether to allow network packets to be sent and received.

#### 2.4.2.3 Identification & Authentication

Diamond*TEK* requires each user of the Diamond*TEK* system to be identified and authenticated prior to allowing the user to perform any other security functions. There are two roles supported by the DiamondTEK system and each is identified and authenticated differently.

> Network Security Manager (NSM) – the NSM must log into the host operating system for the NSC using a user account name and password. Subsequently, the NSM must log into the NSC application using another user name and password.
>
> User – a user of a NSD generally must insert their personal card into a card reader, attached to the NSD, and enter the associated PIN. The exception to this rule is that the NSM can configure static Nodes that can operate without a card inserted (i.e., No-Card Nodes). The NSM must configure the associated NSD to operate in No-Card mode and must associate a user with the Node and select the appropriate Operational Profile.

#### 2.4.2.4 Security Management

Diamond*TEK* offers security management functions via the NSC. Only administrators, specifically the NSM, can log into the NSC. This effectively restricts all management functions to the NSM. Using the NSC, the NSM can add, remove, and configure security properties of NSDs; add, remove, and configure security properties of users; manage the information flow security policies; and manage the audit filters and audit log.

#### 2.4.2.5 TOE Self Protection

Some of the TOE self-protection (e.g., against physical tampering) is ensured by its environment. In particular, it is assumed that NSDs will remain attached to their Hosts so that they cannot be bypassed. However, cryptographic techniques and FIPS 140-1 level 2 tamper techniques are used to protect against or serve to identify tampering and theft of a NSD. The TOE protects its management functions by isolating them within a single component that allows only administrators (i.e., NSMs) to log in and perform management functions. It is assumed that the management console will be appropriately protected from unauthorized physical access.

Logically, each NSD is protected largely by virtue of the fact that its interface is limited to primarily only support network traffic. The identification and authentication interface of the NSD is provided by a physical card reader device that limits any potential for logical attacks. The security policy management interface of the NSD is limited to the NSD initiating connections to the NSC when it starts-up or when a user logs on. The network identity of the NSC is set in the NSD when the NSD is added to the network configuration. The information flow policies, including encryption capabilities, contribute to protection of the TOE since they serve to ensure that TSF data is only accepted when it originates from an allowed source and that it is protected when outside control of the TOE. All communication between an NSD and the NSC is protected by always requiring that it be encrypted using IPsec.

# 3. Security Environment

The TOE security environment consists of the threats to security, organizational security policies, and usage assumptions as they relate to Diamond*TEK.*

Diamond*TEK* provides for a level of protection that is appropriate for IT environments that require strict control over the information flow across a network. Diamond*TEK* is not designed to withstand physical attacks directed at disabling or bypassing its security features, however it is designed to withstand logical attacks originating from its attached network. Diamond*TEK* is suitable for use in both commercial and government environments.

## 3.1 Threats to Security

T.Noauth An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

T.Repeat An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.

T.Aspoof An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.

T.Mediat An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.

T.Oldinf Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.

T.Procom An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between separate parts of the TSF.

T.Audacc Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.

T.Selpro An unauthorized person may read, modify, or destroy security critical TOE configuration data.

T.Audful An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.

T.Tusage The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.

## 3.2 Organization Security Policies

P.Clsify The TOE must limit access to information based on sensitivity of information and the clearance of subjects. The access rules must prevent a subject from accessing information which is of a higher or non-comparable sensitivity than it is cleared to process. The method for classification of information and clearance of subjects is set forth by the organization. The determination of classification and clearance is outside the scope of the TOE; the TOE is expected only to enforce the access rules.

P.Asciat The TOE will ensure that information can only flow between nodes as explicitly allowed by an Administrator. Unlike the Classification policy, the association policy is based on a simple matching criteria. Each allowable communication path must be explicitly defined by an authorized administrator. Furthermore, the authorized administrator must be able to specify whether the information is further protected (e.g., using encryption) while it is in transit across the TSF boundary. The determination of which communication paths should be allowed is outside the scope of the TOE; the TOE is expected only to enforce the associations it is configured with.

P.Athrzd A user must be identified and authenticated at each node before it can send or receive traffic on the physical network. The determination of whether a user should be allowed to access the TOE is outside the scope of the TOE; the TOE is expected only to ensure that the identification and authentication information provided by the user is consistent information that has been configured in the TOE by an authorized administrator.

## 3.3 Secure Usage Assumptions

### 3.3.1 Personnel Assumptions

A.Usract Users will follow provided guidance and will not attempt to violate the information flow policies by entering data at the user interface that is not appropriate for the associated network node.

A.Noevil Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

### 3.3.2 Physical Assumptions

A.Physec The TOE is physically secure; specifically, to ensure that NSDs remain attached to their associated Hosts and to ensure that only authorized administrators can access the management console.

A.Singen Information cannot flow among the internal and external networks (or hosts) unless it passes through the TOE.[7]

### 3.3.3 Logical Assumptions

A.Pltfrm The IT environment will be suitable to support the correct operation of the TOE that will not negatively affect the security functions of the TOE.

A.Exttim The IT environment will provide a time resource that can be used by the TOE to reliably represent the date and time of day.

[7] Since DiamondTEK is a highly distributed product, the notion of an internal network represents a Host protected by a NSD and the notion of an external network represents the network to which a given NSD is attached.

# 4. Security Objectives

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

## 4.1 IT Security Objectives

O.MAC1 The TSF shall allow an authorized administrator to assign security labels to network nodes and users.

O.MAC2 The TSF shall restrict the flow of information between network nodes based on security labels of associated users and information that is being communicated.

O.MAC3 The TSF shall restrict a user to using only network nodes that allow a range of security labels that include those of the user.

O.AAC1 The TSF shall allow an authorized administrator to explicitly define allowed information flows between specific network nodes.

O.AAC2 The TSF shall restrict all information flows except those explicitly allowed by an authorized administrator.

O.AAC3 The TSF shall be able to protect information, using encryption, while it is in transit between parts of the TOE. All TSF data must be protected while outside the control of the TOE.

O.Thresh The TSF shall allow audit thresholds to be defined that will trigger alarms when attempted policy violations exceed the defined thresholds.

O.Idauth The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.

O.Repeat The TSF shall ensure that if a user repeatedly fails to be authenticated, the user account will be disabled automatically.

O.Mediat The TOE must mediate the flow of all information from users on a connected network to users on another connected network, and must ensure that residual information from a previous information flow is not transmitted in any way.

O.Secsta Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.

O.Selpro The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

O.Audrec The TOE must provide a means to record an audit trail of security-related events, with accurate dates and times.

O.Accoun The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.

O.Secfun The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

O.Limext The TOE must provide the means to control and limit access to TOE security functions by an authorized external IT entity.

O.Audsaf The TSF shall protect the audit trail so that only an authorized administrator can read or modify the audit trail.

O.Audlos The TSF shall be configurable to limit the potential loss of audit information.

## 4.2 Non-IT Security Objectives

OE.Usract Individuals intended to use the TOE will follow procedures applicable to the TOE's operation.

OE.Admins Individuals responsible for installing and managing the TOE will be competent and non-malicious.

OE.Guidan The TOE must be delivered, installed, administered, and operated in a manner that maintains security.

OE.Protct The TOE shall be appropriately physically protected; specifically, to ensure only authorized administrators can access the management console and to ensure the NSDs remain attached to their associated Hosts.

## 4.3 IT Security Objectives for the Environment

Some of the IT Security Objectives for the TOE are actually addressed by corresponding IT Security Objectives for the environment. Those aspects are identified below.

OIE.Time The environment shall provide a means to obtain reliable time information.

OIE.Audsup The environment shall provide features necessary to effectively review the audit trail.

# 5. IT Security Requirements

## 5.1 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. All SFRs were drawn from Part 2 of the Common Criteria.

| Security Functional Class | Security Functional Components |
|---|---|
| Security Audit (FAU) | Security alarms (FAU_ARP.1) |
| | Audit data generation (FAU_GEN.1) |
| | User identity association (FAU_GEN.2) |
| | Potential violation analysis (FAU_SAA.1) |
| | Restricted audit review (FAU_SAR.2) |
| | Selectable audit review (FAU_SAR.3) |
| | Selective audit (FAU_SEL.1) |
| | Protected audit trail storage (FAU_STG.1) |
| | Prevention of audit data loss (FAU_STG.4) |
| Cryptographic support (FCS) | Cryptographic key generation (FCS_CKM.1) |
| | Cryptographic key destruction (FCS_CKM.4) |
| | Cryptographic operation (FCS_COP.1(a)) |
| | Cryptographic operation (FCS_COP.1(b)) |
| | Cryptographic operation (FCS_COP.1(c)) |
| User Data Protection (FDP) | Subset information flow control (FDP_IFC.1(a)) |
| | Subset information flow control (FDP_IFC.1(b)) |
| | Subset information flow control (FDP_IFC.1(c)) |
| | Simple security attributes (FDP_IFF.1(a)) |
| | Simple security attributes (FDP_IFF.1(b)) |
| | Hierarchical security attributes (FDP_IFF.2) |
| Identification and authentication (FIA) | Authentication failure handling (FIA_AFL.1) |
| | User attribute definition (FIA_ATD.1) |
| | User authentication before any action (FIA_UAU.2) |
| | User identification before any action (FIA_UID.2) |
| | User-subject binding (FIA_USB.1) |
| Security management (FMT) | Management of security functions behaviour (FMT_MOF.1) |
| | Secure security attributes (FMT_MSA.2) |

| Security Functional Class | Security Functional Components |
|---|---|
| | Management of security attributes (FMT_MSA.1(a)) |
| | Management of security attributes (FMT_MSA.1(b)) |
| | Management of security attributes (FMT_MSA.1(c)) |
| | Static attribute initialization (FMT_MSA.3(a)) |
| | Static attribute initialization (FMT_MSA.3(b)) |
| | Static attribute initialization (FMT_MSA.3(c)) |
| | Management of TSF data (FMT_MTD.1) |
| | Security roles (FMT_SMR.1) |
| Protection of the TSF (FPT) | Non-bypassability of the TSP (FPT_RVM.1) |
| | TSF domain separation (FPT_SEP.1) |

Table 1 Security Functional Components

## 5.1.1 Security Audit (FAU)

### 5.1.1.1 Security alarms (FAU_ARP.1)

#### 5.1.1.1.1 FAU_ARP.1.1

The TSF shall take [**action to issue an alarm**] upon detection of a potential security violation.

### 5.1.1.2 Audit data generation (FAU_GEN.1)

#### 5.1.1.2.1 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 [***not specified***[8]] level of audit; and
c) [**Starting and Stopping a NSD,**
**d) NSM commands (excluding find and print),**
**e) User I&A failures,**
**f) Attempted Mandatory Security Policy violations,**
**g) Attempted Association Security Policy violations,**
**h) Attempted Packet Filter Policy violations, and**
**i) the events described in the following table:**

| Auditable Event | Additional Audit Record Contents |
|---|---|
| **Modifications to the group of users that are part of the Network Security Manager role** | **The identity of the Network Security Manager performing the modification and the user identity being associated with the Network Security Manager role** |
| **All use of the user identification mechanism** | **The user identities provided to the TOE** |
| **All use of the authentication mechanism** | **The user identities provided to the TOE** |
| **The reaching of the threshold for** | **The identity of the offending user and the** |

[8] Note that the CC requires this operation to be completed to indicate a selected level of audit. In this case, none was selected, since all auditable events are explicitly listed subsequently, and therefore "not specified" is the appropriate refinement.

| | |
|---|---|
| **unsuccessful authentication attempts and the subsequent restoration by the Network Security Manager of the users capability to authenticate** | **Network Security Manager** |
| **All decisions on requests for information flow** | **The presumed address of the source and destination subject; except when the decision involves a failure for a Clear Text Node related to Mandatory Security Policy or Packet Integrity** |
| **Changes of time** | **The identity of the Network Security Manager performing the operation** |
| **Use of the Network Security Manager functions pertaining to audit** | **The identity of the Network Security Manager performing the operation** |

]

#### 5.1.1.2.2 FAU_GEN.1.2

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**no additional information**]**.**

### 5.1.1.3 User identity association (FAU_GEN.2)

#### 5.1.1.3.1 FAU_GEN.2.1

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

### 5.1.1.4 Potential violation analysis (FAU_SAA.1)

#### 5.1.1.4.1 FAU_SAA.1.1

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

#### 5.1.1.4.2 FAU_SAA.1.2

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [**access or authentication related events**] known to indicate a potential security violation;

b) [**When accumulated potential security violation indications exceed administrator defined thresholds a potential security violation is detected**].

### 5.1.1.5 Restricted audit review (FAU_SAR.2)

#### 5.1.1.5.1 FAU_SAR.2.1

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

#### 5.1.1.6 Selective audit (FAU_SEL.1)

##### 5.1.1.6.1 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:

a) [***host identity***]
b) [**Selectable Audit Type (Statistical, Broadcast, and TCP open/close)**].

#### 5.1.1.7 Protected audit trail storage (FAU_STG.1)

##### 5.1.1.7.1 FAU_STG.1.1

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

##### 5.1.1.7.2 FAU_STG.1.2

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

#### 5.1.1.8 Prevention of audit data loss (FAU_STG.4)

##### 5.1.1.8.1 FAU_STG.4.1

The TSF shall [***ignore auditable events* or *overwrite the oldest stored audit records***] and [**take no other actions**] if the audit trail is full.

### 5.1.2 Cryptographic support (FCS)

#### 5.1.2.1 Cryptographic key generation (FCS_CKM.1)

##### 5.1.2.1.1 FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**pseudo-random number generation**] and specified cryptographic key sizes [**56-168 bits**] that meet the following: [**FIPS 140-1**].

#### 5.1.2.2 Cryptographic key destruction (FCS_CKM.4)

##### 5.1.2.2.1 FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zeroization of all plaintext cryptographic keys and other critical security parameters within the device**] that meets the following: [**FIPS 140-1**].

#### 5.1.2.3 Cryptographic operation (FCS_COP.1(a))

##### 5.1.2.3.1 FCS_COP.1.1(a)

The TSF shall perform [**data encryption services**] in accordance with a specified cryptographic algorithm [**DES and 3DES** ] and cryptographic key sizes [**56 bits for DES and 168 bits for 3DES** ] that meet the following: [**FIPS 46-3 for DES and 3DES, and RFC 2406, “Encapsulating Security Payload (ESP)”** ].

### 5.1.2.4 Cryptographic operation (FCS_COP.1(b))

#### 5.1.2.4.1 FCS_COP.1.1(b)

The TSF shall perform [**hashing**] in accordance with a specified cryptographic algorithm [**SHA-1**] and cryptographic key sizes [**56 bits for broadcast group related hashes, otherwise 160 bits**] that meet the following: [**FIPS 180-1**].

### 5.1.2.5 Cryptographic operation (FCS_COP.1(c))

#### 5.1.2.5.1 FCS_COP.1.1(c)

The TSF shall perform [**key exchange**] in accordance with a specified cryptographic algorithm [**Diffie-Hellman**] and cryptographic key sizes [**768 And 1024 bits**] that meet the following: [**RFC 2409, "Internet Key Exchange (IKE)"**].

## 5.1.3 User Data Protection (FDP)

### 5.1.3.1 Subset information flow control (FDP_IFC.1(a))

#### 5.1.3.1.1 FDP_IFC.1.1(a)

The TSF shall enforce the [**Mandatory Security Policy**] on**:**

**a)** [**subjects: all IT entities that send and receive information through the TOE to one another;**
**b)** **information: unicast Internet Protocol (IP) traffic sent through the TOE from one subject to another;**
**c)** **operation: pass information**].

### 5.1.3.2 Subset information flow control (FDP_IFC.1(b))

#### 5.1.3.2.1 FDP_IFC.1.1(b)

The TSF shall enforce the [**Association Security Policy**] on**:**

**a)** [**subjects: all IT entities that send and receive information through the TOE to one another;**
**b)** **information: traffic sent through the TOE from one subject to another;**
**c)** **operation: pass information**].

### 5.1.3.3 Subset information flow control (FDP_IFC.1(c))

#### 5.1.3.3.1 FDP_IFC.1.1(c)

The TSF shall enforce the [**Packet Filter Policy**] on**:**

**a)** [**subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;**
**b)** **information: traffic sent through the TOE from one subject to another;**
**c)** **operation: pass information**].

### 5.1.3.4 Simple security attributes (FDP_IFF.1(a))

#### 5.1.3.4.1 FDP_IFF.1.1(a)

The TSF shall enforce the [**Association Security Policy**] based on the following types of subject and information security attributes:

[**a) subject Association Profile settings for source and destination addresses, and**
**b) information source and destination addresses**].

#### 5.1.3.4.2 FDP_IFF.1.2(a)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[**a) a subject can only receive information if, based on the subject Association Profile settings for information source address:**

**1) the information source address is explicitly allowed to send information, and**
**2) if the information source address is not explicitly allowed to send information in clear text, a valid key exchange must succeed and the information must be encrypted; and**

**b) a subject can only send information if, based on the subject Association Profile settings for information destination address:**

**1) the information destination address is explicitly allowed to receive information, and**
**2) if the information destination subject is not explicitly allowed to receive information in clear text, a valid key exchange must succeed and the information must be encrypted**].

#### 5.1.3.4.3 FDP_IFF.1.3(a)

The TSF shall enforce the [**none**].

#### 5.1.3.4.4 FDP_IFF.1.4(a)

The TSF shall provide the following [**none**].

#### 5.1.3.4.5 FDP_IFF.1.5(a)

The TSF shall explicitly authorise an information flow based on the following rules:

[**a) The TOE shall permit non-IP-based traffic to flow without further restriction when specifically allowed by a Network Security Manager;**

**b) The TOE shall permit DHCP requests from an internal network to flow to the external network and responses from the external network to flow to the internal network when explicitly allowed by a Network Security Manager; and**

**c) The TOE shall permit broadcast IP traffic to flow to other IT entities when specifically allowed by a Network Security Manager**].

#### 5.1.3.4.6 FDP_IFF.1.6(a)

The TSF shall explicitly deny an information flow based on the following rules:

[**none**].

### 5.1.3.5 Simple security attributes (FDP_IFF.1(b))

#### 5.1.3.5.1 FDP_IFF.1.1(b)

The TSF shall enforce the [**Packet Filter Policy**] based on **at least** the following types of subject and information security attributes:

**a)** [**subject security attributes:**
- **presumed address**

**b) information security attributes:**
- **presumed address of source subject;**
- **presumed address of destination subject;**
- **transport layer protocol;**
- **TOE interface on which traffic arrives and departs;**
- **service**].

#### 5.1.3.5.2 FDP_IFF.1.2(b)

The TSF shall permit an information flow between a controlled subject and **another** controlled ~~information~~ **subject** via a controlled operation if the following rules hold:

**a)** [**Subjects on an internal network can cause information to flow through the TOE to another connected network if:**

- **all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information security attributes, created by the Network Security Manager;**
- **the presumed address of the source subject, in the information, translates to an internal network address;**
- **and the presumed address of the destination subject, in the information, translates to an address on the other connected network.**

**b)** **Subjects on the external network can cause information to flow through the TOE to another connected network if:**

- **all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information security attributes, created by the Network Security Manager;**
- **the presumed address of the source subject, in the information, translates to an external network address;**
- **and the presumed address of the destination subject, in the information, translates to an address on the other connected network.]**

#### 5.1.3.5.3 FDP_IFF.1.3(b)

The TSF shall enforce the [**none**].

#### 5.1.3.5.4 FDP_IFF.1.4(b)

The TSF shall provide the following [**none**].

#### 5.1.3.5.5 FDP_IFF.1.5(b)

The TSF shall explicitly authorise an information flow based on the following rules: [**none**].

#### 5.1.3.5.6 FDP_IFF.1.6(b)

The TSF shall explicitly deny an information flow based on the following rules:

**a)** [**The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;**

**b)** **The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;**

**c)** **The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;**

d) **The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network.**]

### 5.1.3.6 Hierarchical security attributes (FDP_IFF.2)

#### 5.1.3.6.1 FDP_IFF.2.1

**THE TSF SHALL ENFORCE THE [**MANDATORY SECURITY POLICY**] BASED ON THE FOLLOWING TYPES OF SUBJECT AND INFORMATION SECURITY ATTRIBUTES: [**

**a) source subject sensitivity labels,**
**b) destination subject sensitivity labels, and**
**c) information sensitivity labels**].

#### 5.1.3.6.2 FDP_IFF.2.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules, based on the ordering relationships between security attributes hold: [

**a) a source subject can only send information if:**

**1) the sensitivity label of the information is dominated**[9] **by the maximum sensitivity label of the source subject and**

**2) the sensitivity label of the information dominates the minimum sensitivity label of the source subject**

**b) a destination subject can only receive information if:**

**1) the sensitivity label of the information is dominated**[9] **by the maximum sensitivity label of the destination subject and**

**2) the sensitivity label of the information dominates the minimum sensitivity label of the destination subject**].

#### 5.1.3.6.3 FDP_IFF.2.3

The TSF shall enforce the [**none**].

#### 5.1.3.6.4 FDP_IFF.2.4

The TSF shall provide the following [**none**]

#### 5.1.3.6.5 FDP_IFF.2.5

The TSF shall explicitly authorise an information flow based on the following rules:

[**a)** **The TOE shall permit traffic to flow when the Mandatory Security Policies rules are satisfied with the exception of checks related to the non-hierarchical part of the sensitivity label when specifically allowed by a Network Security Manager and the non-hierarchical part of the sensitivity label of the traffic is empty**].

#### 5.1.3.6.6 FDP_IFF.2.6

The TSF shall explicitly deny an information flow based on the following rules:

[**none**].

#### 5.1.3.6.7 FDP_IFF.2.7

The TSF shall enforce the following relationships for any two valid information flow control security attributes:

[9] In order for a label to dominate another, any hierarchically related component of the label must be greater than or equal *and* any non-hierarchically related component of the label must be a superset. If each label includes non-hierarchically related components not included in the other, the labels are not comparable and neither dominates the other. Similarly, it is possible that the hierarchical component of a label can be greater than or equal to another label while the non-hierarchical component can be a non-equal subset of the other label. In this case neither label dominates the other.

a) There exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable; and
b) There exists a "least upper bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and
c) There exists a "greatest lower bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is not greater than the two valid security attributes.

## 5.1.4 Identification and authentication (FIA)

### 5.1.4.1 Authentication failure handling (FIA_AFL.1)

#### 5.1.4.1.1 FIA_AFL.1.1

The TSF shall detect when [**a Network Security Manager defined number of**] unsuccessful authentication attempts occur related to [**a user logging onto a NSD**].

#### 5.1.4.1.2 FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**disable the user and generate an alarm**].

### 5.1.4.2 User attribute definition (FIA_ATD.1)

#### 5.1.4.2.1 FIA_ATD.1.1

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

**For Users,**
**User role,**
**Identity,**
**Authentication data,**
**Association Security Profiles,**
**Mandatory Security Profiles, and**
**Audit Thresholds; and**
**For Network Security Managers,**
**Network Security Manager role,**
**Identity, and**
**Authentication data**].

### 5.1.4.3 User authentication before any action (FIA_UAU.2)

#### 5.1.4.3.1 FIA_UAU.2.1

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

### 5.1.4.4 User identification before any action (FIA_UID.2)

#### 5.1.4.4.1 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.

### 5.1.4.5 User-subject binding (FIA_USB.1)

#### 5.1.4.5.1 FIA_USB.1.1

The TSF shall associate the ~~appropriate~~ **following** user security attributes with subjects acting on behalf of that user: **[user identity]**.[10]

## 5.1.5 Security management (FMT)

### 5.1.5.1 Management of security functions behaviour (FMT_MOF.1)

#### 5.1.5.1.1 FMT_MOF.1.1

The TSF shall restrict the ability to [***determine the behaviour of, modify the behaviour of***] **or otherwise manage** the functions [**start-up and shutdown, change of time and date, Security Audit, Mandatory Security Policy, Association Security Policy, Packet Filter Policy, and Identification and Authentication**] to [**the Network Security Manager**].

### 5.1.5.2 Management of security attributes (FMT_MSA.1(a))

#### 5.1.5.2.1 FMT_MSA.1.1(a)

The TSF shall enforce the [**Mandatory Security Policy**] to restrict the ability to [***query, modify, delete,*** **create, and assign**] the security attributes [**sensitivity labels and Mandatory Security Profiles**] to [**the Network Security Manager**].

### 5.1.5.3 Management of security attributes (FMT_MSA.1(b))

#### 5.1.5.3.1 FMT_MSA.1.1(b)

The TSF shall enforce the [**Association Security Policy**] to restrict the ability to [***query, modify, delete,*** **create, and assign**] the security attributes [**Association Security Profiles**] to [**the Network Security Manager**].

### 5.1.5.4 Management of security attributes (FMT_MSA.1(c))

#### 5.1.5.4.1 FMT_MSA.1.1(c)

The TSF shall enforce the [**Packet Filter Policy**] to restrict the ability to [***query, modify, delete,*** **and create**] the security attributes [**packet filter policy rules**] to [**the Network Security Manager**].

### 5.1.5.5 Secure security attributes (FMT_MSA.2)

#### 5.1.5.5.1 FMT_MSA.2.1

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

### 5.1.5.6 Static attribute initialization (FMT_MSA.3(a))

#### 5.1.5.6.1 FMT_MSA.3.1(a)

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

[10] This requirement has been modified (i.e., refined) from the original CC v2.1 version based on U.S. National Interpretation I-0351: "User Attributes To Be Bound Should Be Specified".

##### 5.1.5.6.2 FMT_MSA.3.2(a)

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

#### 5.1.5.7 Static attribute initialization (FMT_MSA.3(b))

##### 5.1.5.7.1 FMT_MSA.3.1(b)

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

##### 5.1.5.7.2 FMT_MSA.3.2(b)

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

#### 5.1.5.8 Static attribute initialization (FMT_MSA.3(c))

##### 5.1.5.8.1 FMT_MSA.3.1(c)

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

##### 5.1.5.8.2 FMT_MSA.3.2(c)

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

#### 5.1.5.9 Management of TSF data (FMT_MTD.1)

##### 5.1.5.9.1 FMT_MTD.1.1

The TSF shall restrict the ability to [***query, [*****define, configure, and assign*****]***] the [**Mandatory Security Profiles, Association Security Profiles, Audit Thresholds, Audit Event filters**] to [**the Network Security Manager**].

#### 5.1.5.10 Security roles (FMT_SMR.1)

##### 5.1.5.10.1 FMT_SMR.1.1

The TSF shall maintain the roles [**user and Network Security Manager**[11]].

##### 5.1.5.10.2 FMT_SMR.1.2

The TSF shall be able to associate users with roles.

### 5.1.6 Protection of the TSF (FPT)

#### 5.1.6.1 Non-bypassability of the TSP (FPT_RVM.1)

##### 5.1.6.1.1 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.

[11] Note that this Security Target defines only a single administrator role, Network Security Manager (NSM), for simplicity. There are actually other roles, such as operator and crypto operator, but for the purpose of this Security Target, it is assumed that those roles are a subset of the NSM role.

#### 5.1.6.2 TSF domain separation (FPT_SEP.1)

##### 5.1.6.2.1 FPT_SEP.1.1

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

##### 5.1.6.2.2 FPT_SEP.1.2

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

## 5.2 Security Functional Requirements for the IT Environment

The following security functional requirements (SFRs) are intended to be satisfied by the IT environment rather than the TOE itself. All SFRs were drawn from Part 2 of the Common Criteria.

| Security Functional Class | Security Functional Components |
|---|---|
| Security Audit (FAU) | Audit review (FAU_SAR.1) |
| Protection of the TSF (FPT) | Reliable time stamps (FPT_STM.1) |

Table 2 Security Functional Components for the IT Environment

### 5.2.1 Security Audit (FAU)

#### 5.2.1.1 Audit review (FAU_SAR.1)

##### 5.2.1.1.1 FAU_SAR.1.1

The TSF shall provide [**Network Security Manager**] with the capability to read [**all information**] from the audit records.

##### 5.2.1.1.2 FAU_SAR.1.2

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

### 5.2.2 Protection of the TSF (FPT)

#### 5.2.2.1 Reliable time stamps (FPT_STM.1)

##### 5.2.2.1.1 FPT_STM.1.1

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

## 5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level (EAL) 4 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

| Assurance Class | Assurance Components |
|---|---|

| | |
|---|---|
| Configuration Management (ACM) | ACM_AUT.1 Partial CM automation |
| | ACM_CAP.4 Generation support and acceptance procedures |
| | ACM_SCP.2 Problem tracking CM coverage |
| Delivery and Operation (ADO) | ADO_DEL.2 Detection of modification |
| | ADO_IGS.1 Installation, generation, and start-up procedures |
| Development (ADV) | ADV_FSP.2 Fully defined external interfaces |
| | ADV_HLD.2 Security enforcing high-level design |
| | ADV_IMP.1 Subset of the implementation of the TSF |
| | ADV_LLD.1 Descriptive low-level design |
| | ADV_RCR.1 Informal correspondence demonstration |
| | ADV_SPM.1 Informal TOE security policy model |
| Guidance Documents (AGD) | AGD_ADM.1 Administrator guidance |
| | AGD_USR.1 User guidance |
| Life cycle support (ALC) | ALC_DVS.1 Identification of security measures |
| | ALC_LCD.1 Developer defined life-cycle model |
| | ALC_TAT.1 Well-defined development tools |
| Tests (ATE) | ATE_COV.2 Analysis of Coverage |
| | ATE_DPT.1 Testing: high-level design |
| | ATE_FUN.1 Functional testing |
| | ATE_IND.2 Independent testing - sample |
| Vulnerability assessment (AVA) | AVA_MSU.2 Validation of analysis |
| | AVA_SOF.1 Strength of TOE security function evaluation |
| | AVA_VLA.2 Independent vulnerability analysis |

Table 3 EAL 4 Assurance Components

## 5.3.1 Configuration Management (ACM)

### 5.3.1.1 Partial CM automation (ACM_AUT.1)

#### 5.3.1.1.1 ACM_AUT.1.1D

The developer shall use a CM system.

#### 5.3.1.1.2 ACM_AUT.1.2D

The developer shall provide a CM plan.

#### 5.3.1.1.3 ACM_AUT.1.1C

The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation.

#### 5.3.1.1.4 ACM_AUT.1.2C

The CM system shall provide an automated means to support the generation of the TOE.

#### 5.3.1.1.5 ACM_AUT.1.3C

The CM plan shall describe the automated tools used in the CM system.

#### 5.3.1.1.6 ACM_AUT.1.4C

The CM plan shall describe how the automated tools are used in the CM system.

#### 5.3.1.1.7 ACM_AUT.1.1E

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

### 5.3.1.2 Generation Support and Acceptance Procedures (ACM_CAP.4)

#### 5.3.1.2.1 ACM_CAP.4.1D

The developer shall provide a reference for the TOE.

#### 5.3.1.2.2 ACM_CAP.4.2D

The developer shall use a CM system.

#### 5.3.1.2.3 ACM_CAP.4.3D

The developer shall provide CM documentation.

#### 5.3.1.2.4 ACM_CAP.4.1C

The reference for the TOE shall be unique to each version of the TOE.

#### 5.3.1.2.5 ACM_CAP.4.2C

The TOE shall be labeled with its reference.

#### 5.3.1.2.6 ACM_CAP.4.3C

The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

#### 5.3.1.2.7 ACM_CAP.4.4C

The configuration list shall describe the configuration items that comprise the TOE.

#### 5.3.1.2.8 ACM_CAP.4.5C

The CM documentation shall describe the method used to uniquely identify the configuration items.

##### 5.3.1.2.9 ACM_CAP.4.6C

The CM system shall uniquely identify all configuration items.

##### 5.3.1.2.10 ACM_CAP.4.7C

The CM plan shall describe how the CM system is used.

##### 5.3.1.2.11 ACM_CAP.4.8C

The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

##### 5.3.1.2.12 ACM_CAP.4.9C

The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

##### 5.3.1.2.13 ACM_CAP.4.10C

The CM system shall provide measures such that only authorised changes are made to the configuration items.

##### 5.3.1.2.14 ACM_CAP.4.11C

The CM system shall support the generation of the TOE.

##### 5.3.1.2.15 ACM_CAP.4.12C

The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

##### 5.3.1.2.16 ACM_CAP.4.1E

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

#### 5.3.1.3 Problem tracking CM coverage (ACM_SCP.2)

##### 5.3.1.3.1 ACM_SCP.2.1D

The developer shall provide CM documentation.

##### 5.3.1.3.2 ACM_SCP.2.1C

The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

##### 5.3.1.3.3 ACM_SCP.2.2C

The CM documentation shall describe how configuration items are tracked by the CM system.

##### 5.3.1.3.4 ACM_SCP.2.1E

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

## 5.3.2 Delivery and Operation (ADO)

### 5.3.2.1 Detection of modification (ADO_DEL.2)

#### 5.3.2.1.1 ADO_DEL.2.1D

The developer shall document procedures for delivery of the TOE or parts of it to the user.

#### 5.3.2.1.2 ADO_DEL.2.2D

The developer shall use the delivery procedures.

#### 5.3.2.1.3 ADO_DEL.2.1C

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

#### 5.3.2.1.4 ADO_DEL.2.2C

The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

#### 5.3.2.1.5 ADO_DEL.2.3C

The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

#### 5.3.2.1.6 ADO_DEL.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence

### 5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

#### 5.3.2.2.1 ADO_IGS.1.1D

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

#### 5.3.2.2.2 ADO_IGS.1.1C

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

#### 5.3.2.2.3 ADO_IGS.1.1E

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

#### 5.3.2.2.4 ADO_IGS.1.2E

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

## 5.3.3 Development (ADV)

### 5.3.3.1 Fully defined external interfaces (ADV_FSP.2)

#### 5.3.3.1.1 ADV_FSP.2.1D

The developer shall provide a functional specification.

#### 5.3.3.1.2 ADV_FSP.2.1C

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

#### 5.3.3.1.3 ADV_FSP.2.2C

The functional specification shall be internally consistent.

#### 5.3.3.1.4 ADV_FSP.2.3C

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

#### 5.3.3.1.5 ADV_FSP.2.4C

The functional specification shall completely represent the TSF.

#### 5.3.3.1.6 ADV_FSP.2.5C

The functional specification shall include rationale that the TSF is completely represented.

#### 5.3.3.1.7 ADV_FSP.1.1E

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

#### 5.3.3.1.8 ADV_FSP.1.2E

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

### 5.3.3.2 Security enforcing high-level design (ADV_HLD.2)

#### 5.3.3.2.1 ADV_HLD.2.1D

The developer shall provide the high-level design of the TSF.

#### 5.3.3.2.2 ADV_HLD.2.1C

The presentation of the high-level design shall be informal.

#### 5.3.3.2.3 ADV_HLD.2.2C

The high-level design shall be internally consistent.

#### 5.3.3.2.4 ADV_HLD.2.3C

The high-level design shall describe the structure of the TSF in terms of subsystems.

#### 5.3.3.2.5 ADV_HLD.2.4C

The high-level design shall describe the security functionality provided by each subsystem of the TSF.

#### 5.3.3.2.6 ADV_HLD.2.5C

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

#### 5.3.3.2.7 ADV_HLD.2.6C

The high-level design shall identify all interfaces to the subsystems of the TSF.

#### 5.3.3.2.8 ADV_HLD.2.7C

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

#### 5.3.3.2.9 ADV_HLD.2.8C

The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

#### 5.3.3.2.10 ADV_HLD.2.9C

The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

#### 5.3.3.2.11 ADV_HLD.1.1E

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

#### 5.3.3.2.12 ADV_HLD.1.2E

The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

### 5.3.3.3 Subset of the implementation of the TSF (ADV_IMP.1)

#### 5.3.3.3.1 ADV_IMP.1.1D

The developer shall provide the implementation representation for a selected subset of the TSF.

#### 5.3.3.3.2 ADV_IMP.1.1C

The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

#### 5.3.3.3.3 ADV_IMP.1.2C

The implementation representation shall be internally consistent.

#### 5.3.3.3.4 ADV_IMP.1.1E

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

#### 5.3.3.3.5 ADV_IMP.1.2E

The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

### 5.3.3.4 Descriptive low-level design (ADV_LLD.1)

#### 5.3.3.4.1 ADV_LLD.1.1D

The developer shall provide the low-level design of the TSF.

#### 5.3.3.4.2 ADV_LLD.1.1C

The presentation of the low-level design shall be informal.

#### 5.3.3.4.3 ADV_LLD.1.2C

The low-level design shall be internally consistent.

#### 5.3.3.4.4 ADV_LLD.1.3C

The low-level design shall describe the TSF in terms of modules.

#### 5.3.3.4.5 ADV_LLD.1.4C

The low-level design shall describe the purpose of each module.

#### 5.3.3.4.6 ADV_LLD.1.5C

The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

#### 5.3.3.4.7 ADV_LLD.1.6C

The low-level design shall describe how each TSP-enforcing function is provided.

#### 5.3.3.4.8 ADV_LLD.1.7C

The low-level design shall identify all interfaces to the modules of the TSF.

#### 5.3.3.4.9 ADV_LLD.1.8C

The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

#### 5.3.3.4.10 ADV_LLD.1.9C

The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

#### 5.3.3.4.11 ADV_LLD.1.10C

The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

#### 5.3.3.4.12 ADV_LLD.1.1E

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

#### 5.3.3.4.13 ADV_LLD.1.2E

The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

### 5.3.3.5 Informal correspondence demonstration (ADV_RCR.1)

#### 5.3.3.5.1 ADV_RCR.1.1D

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

#### 5.3.3.5.2 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.

#### 5.3.3.5.3 ADV_RCR.1.1E

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

### 5.3.3.6 Informal TOE security policy model (ADV_SPM.1)

#### 5.3.3.6.1 ADV_SPM.1.1D

The developer shall provide a TSP model.

#### 5.3.3.6.2 ADV_SPM.1.2D

The developer shall demonstrate correspondence between the functional specification and the TSP model.

#### 5.3.3.6.3 ADV_SPM.1.1C

The TSP model shall be informal.

#### 5.3.3.6.4 ADV_SPM.1.2C

The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

#### 5.3.3.6.5 ADV_SPM.1.3C

The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

##### 5.3.3.6.6 ADV_SPM.1.4C

The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

##### 5.3.3.6.7 ADV_SPM.1.1E

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

### 5.3.4 Guidance Documents (AGD)

#### 5.3.4.1 Administrator Guidance (AGD_ADM.1)

##### 5.3.4.1.1 AGD_ADM.1.1D

The developer shall provide administrator guidance addressed to system administrative personnel.

##### 5.3.4.1.2 AGD_ADM.1.1C

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

##### 5.3.4.1.3 AGD_ADM.1.2C

The administrator guidance shall describe how to administer the TOE in a secure manner.

##### 5.3.4.1.4 AGD_ADM.1.3C

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

##### 5.3.4.1.5 AGD_ADM.1.4C

The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

##### 5.3.4.1.6 AGD_ADM.1.5C

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

##### 5.3.4.1.7 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.

##### 5.3.4.1.8 AGD_ADM.1.7C

The administrator guidance shall be consistent with all other documents supplied for evaluation.

#### 5.3.4.1.9 AGD_ADM.1.8C

The administrator guidance shall describe all security requirements on the IT environment that are relevant to the administrator.

#### 5.3.4.1.10 AGD_ADM.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence

### 5.3.4.2 User Guidance (AGD_USR.1)

#### 5.3.4.2.1 AGD_USR.1.1D

The developer shall provide user guidance.

#### 5.3.4.2.2 AGD_USR.1.1C

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

#### 5.3.4.2.3 AGD_USR.1.2C

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

#### 5.3.4.2.4 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.

#### 5.3.4.2.5 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 behavior found in the statement of TOE security environment.

#### 5.3.4.2.6 AGD_USR.1.5C

The user guidance shall be consistent with all other documentation supplied for evaluation.

#### 5.3.4.2.7 AGD_USR.1.6C

The user guidance shall describe all security requirements on the IT environment that are relevant to the user.

#### 5.3.4.2.8 AGD_USR.1.1E

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

## 5.3.5 Life Cycle Support (ALC)

### 5.3.5.1 Identification of security measures (ALC_DVS.1)

#### 5.3.5.1.1 ALC_DVS.1.1D

The developer shall produce development security documentation.

#### 5.3.5.1.2 ALC_DVS.1.1C

The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

#### 5.3.5.1.3 ALC_DVS.1.2C

The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

#### 5.3.5.1.4 ALC_DVS.1.1E

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

#### 5.3.5.1.5 ALC_DVS.1.2E

The evaluator shall confirm that the security measures are being applied.

### 5.3.5.2 Developer defined life-cycle model (ALC_LCD.1)

#### 5.3.5.2.1 ALC_LCD.1.1D

The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

#### 5.3.5.2.2 ALC_LCD.1.2D

The developer shall provide life-cycle definition documentation.

#### 5.3.5.2.3 ALC_LCD.1.1C

The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

#### 5.3.5.2.4 ALC_LCD.1.2C

The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

#### 5.3.5.2.5 ALC_LCD.1.1E

The evaluator shall confirm that the information meets all requirements for content and presentation of evidence.

### 5.3.5.3 Well-defined development tools (ALC_TAT.1)

#### 5.3.5.3.1 ALC_TAT.1.1D

The developer shall identify the development tools being used for the TOE.

#### 5.3.5.3.2 ALC_TAT.1.2D

The developer shall document the selected implementation-dependent options of the development tools.

#### 5.3.5.3.3 ALC_TAT.1.1C

All development tools used for implementation shall be well defined.

#### 5.3.5.3.4 ALC_TAT.1.2C

The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

#### 5.3.5.3.5 ALC_TAT.1.3C

The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

#### 5.3.5.3.6 ALC_TAT.1.1E

The evaluator shall confirm that the information meets all requirements for content and presentation of evidence.

## 5.3.6 Security Testing (ATE)

### 5.3.6.1 Analysis of coverage (ATE_COV.2)

#### 5.3.6.1.1 ATE_COV.2.1D

The developer shall provide an analysis of the test coverage.

#### 5.3.6.1.2 ATE_COV.2.1C

The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

#### 5.3.6.1.3 ATE_COV.2.2C

The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

#### 5.3.6.1.4 ATE_COV.2.1E

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

### 5.3.6.2 Testing: high-level design (ATE_DPT.1)

#### 5.3.6.2.1 ATE_DPT.1.1D

The developer shall provide the analysis of the depth of testing.

#### 5.3.6.2.2 ATE_DPT.1.1C

The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

#### 5.3.6.2.3 ATE_DPT.1.1E

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

### 5.3.6.3 Functional testing (ATE_FUN.1)

#### 5.3.6.3.1 ATE_FUN.1.1D

The developer shall test the TSF and document the results.

#### 5.3.6.3.2 ATE_FUN.1.2D

The developer shall provide test documentation.

#### 5.3.6.3.3 ATE_FUN.1.1C

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

#### 5.3.6.3.4 ATE_FUN.1.2C

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

#### 5.3.6.3.5 ATE_FUN.1.3C

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

#### 5.3.6.3.6 ATE_FUN.1.4C

The expected test results shall show the anticipated outputs from a successful execution of the tests.

#### 5.3.6.3.7 ATE_FUN.1.5C

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

#### 5.3.6.3.8 ATE_FUN.1.1E

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

### 5.3.6.4 Independent testing – sample (ATE_IND.2)

#### 5.3.6.4.1 ATE_IND.2.1D

The developer shall provide the TOE for testing.

#### 5.3.6.4.2 ATE_IND.2.1C

The TOE shall be suitable for testing.

#### 5.3.6.4.3 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.

#### 5.3.6.4.4 ATE_IND.2.1E

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

#### 5.3.6.4.5 ATE_IND.2.2E

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

#### 5.3.6.4.6 ATE_IND.2.3E

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

## 5.3.7 Vulnerability Assessment (VLA)

### 5.3.7.1 Validation of analysis (AVA_MSU.2)

#### 5.3.7.1.1 AVA_MSU.2.1D

The developer shall provide guidance documentation.

#### 5.3.7.1.2 AVA_MSU.2.2D

The developer shall document an analysis of the guidance documentation.

#### 5.3.7.1.3 AVA_MSU.2.1C

The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

#### 5.3.7.1.4 AVA_MSU.2.2C

The guidance documentation shall be complete, clear, consistent and reasonable.

#### 5.3.7.1.5 AVA_MSU.2.3C

The guidance documentation shall list all assumptions about the intended environment.

#### 5.3.7.1.6 AVA_MSU.2.4C

The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

#### 5.3.7.1.7 AVA_MSU.2.5C

The analysis documentation shall demonstrate that the guidance documentation is complete.

#### 5.3.7.1.8 AVA_MSU.2.1E

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

#### 5.3.7.1.9 AVA_MSU.2.2E

The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

##### 5.3.7.1.10 AVA_MSU.2.3E

6.7.1.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

##### 5.3.7.1.11 AVA_MSU.2.4E

The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

#### 5.3.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

##### 5.3.7.2.1 AVA_SOF.1.1D

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

##### 5.3.7.2.2 AVA_SOF.1.1C

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

##### 5.3.7.2.3 AVA_SOF.1.2C

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

##### 5.3.7.2.4 AVA_SOF.1.1E

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

##### 5.3.7.2.5 AVA_SOF.1.2E

The evaluator shall confirm that the strength claims are correct.

#### 5.3.7.3 Independent vulnerability analysis (AVA_VLA.2)

##### 5.3.7.3.1 AVA_VLA.2.1D

The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

##### 5.3.7.3.2 AVA_VLA.2.2D

The developer shall document the disposition of identified vulnerabilities.

##### 5.3.7.3.3 AVA_VLA.2.1C

The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

##### 5.3.7.3.4 AVA_VLA.2.2C

The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

#### 5.3.7.3.5 AVA_VLA.2.1E

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

#### 5.3.7.3.6 AVA_VLA.2.2E

The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

#### 5.3.7.3.7 AVA_VLA.2.3E

The evaluator shall perform an independent vulnerability analysis.

#### 5.3.7.3.8 AVA_VLA.2.4E

The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

#### 5.3.7.3.9 AVA_VLA.2.5E

The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

# 6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

## 6.1 TOE Security Functions

### 6.1.1 Security Audit

The Network Security Console (NSC) records audit information that originates with the NSC itself (e.g., from Network Security Manager actions) and events forwarded from Network Security Devices (NSDs). The content of each audit record depends primarily on its source.

Each NSC audit record includes:

- Audit type
    - Note: the type will indicate if the command was cancelled or aborted.
- Time
- Date
- Current Network Security Manager (NSM; see Section 6.1.4), when applicable
- Audit data specific to the audit type:
    - NSD state changes:
        - Responsible user and node identification
    - User logon failures:
        - The responsible user and node identification
        - Note: certain logon failures are subject to thresholds after which the user account will be disabled. This causes the NSC to issue a shutdown command to the applicable NSD, which is audited as indicated below.
    - NSM logon and logoff:
        - NSM identification
    - NSM logon failure:
        - NSM identification

Each NSD audit record includes:

- Audit type
- Time
- Date
- User (note that this identifies the user at the NSD where the exception occurred, not necessarily the user that actually caused the exception, e.g., a remote user sending offending traffic)
- Other user (in cases where another user might be involved)
- Source network address (except when the decision involves a failure for a Clear Text Node related to Mandatory Security Policy or Packet Integrity)

- Destination network address (except when the decision involves a failure for a Clear Text Node related to Mandatory Security Policy or Packet Integrity)
- Protocol source port number (when appropriate)
- Protocol destination port number (when appropriate)

Each NSD will send an audit record to the NSC when:

- It processes a command to change state (e.g., start or stop);
- When IP packet integrity errors are detected;
- When there is an attempt to violate either the Mandatory Security Policy, Association Security Policy, or Packet Filter Policy; and,
- Optionally, for packets sent and received (i.e., statistical auditing), broadcast (ARP) traffic, and TCP connections.

When the NSC generates an audit record or receives an audit record from a NSD, it will incorporate the current time and date and insert the event into its audit trail. This is actually accomplished by invoking a Windows 2000 audit logging function. The NSC restricts unauthorized access to the audit trail. The NSC has only two types of interfaces that might be used to access the audit trail: access through the IT environment and access through the TOE. Due to assumptions on the IT environment, only the NSM has physical access to the NSC and its IT environment and all network connections must pass through the TOE, so only the NSM can access the audit trail using the NSC commands (or other access that might be provided by the IT environment). Access through the TOE is protected by two mechanisms: 1) the NSC application requires users to logon before offering the capability to access the audit trail; and, 2) the NSC prevents network access to itself and its IT environment by restricting network traffic to a well defined set of messages (which do not include any audit access services) that must originate from known NSDs. The NSM can manage the audit function (e.g., set up audit filters, clear the audit trail) as well as review audit records. Windows 2000 provides the ability to store and review audit logs. Diamond*TEK* collects, including filtering, all audit records and provides an interface to invoke the Windows 2000 functions.

In addition to receiving audit records, the NSC allows the NSM to configure per-user security violation thresholds, to set audit filters, to manage the storage of audit records, and to review and print the audit records.

- Security violation thresholds can be established per-violation-type (e.g., access and authentication violations) for each user and the NSC will keep track of (i.e., count, in addition to simply record) violations as they occur. When enough security violations occur that exceed a threshold, the NSC issues an alarm to help ensure that the NSM is aware of the violations.
- The audit filters can be configured to limit pre-selectable audit events (statistical, broadcast, and TCP open/close) based on specific NSDs[12] and users.
- The NSC can be configured to ignore auditable events or overwrite the audit oldest audit records when the audit trail becomes full.
- The NSC provides an audit review capability that can be used to review the audit trail.
- Note that auditing is being performed whenever the NSC is operational. There is no explicit function available to stop or restart the audit function, however starting and stopping the network or an individual NSD is audited.

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1
- FAU_GEN.2

[12] Note that each NSD is always uniquely associated with a single logical host (e.g., workstation, server, subnetwork).

- FAU_ARP.1
- FAU_SAA.1
- FAU_SAR.2
- FAU_SEL.1
- FAU_STG.1
- FAU_STG.4

The following security functional requirements are additionally satisfied by the IT environment:

- FAU_SAR.1

### 6.1.2 User Data Protection

DiamondTEK provides three distinct user data security functions. One implements the Association Security Policy, another implements the Mandatory Security Policy, and the last implements the Packet Filter Policy. In addition, there is a fourth user data security function in the form of cryptographic support. This fourth function is used in conjunction with the Association Security Policy.

The Association Security Policy allows each node to communicate only with (i.e., send or receive data) other *authorized* nodes based on an Association Profile. The NSM can explicitly define three types of associations in an Association Profile: NSD-to-NSD, NSD-to-OIPS (Other IPsec), and NSD-to-CTN (Clear Text Node). Both the NSD-to-NSD and NSD-to-OIPS associations generally require that encryption is used when transferring information.

The Mandatory Security Policy allows a node to communicate with another node only when it has an appropriately matching security label. There are 256 security levels and 65,535 security categories that can be used to construct a security label. Each node labels each packet (either explicitly or implicitly) that is placed on the network, and when a NSD receives a packet it checks the label to ensure it is allowed to receive the packet. Similarly, when a NSD sends a packet it checks the label to ensure it is allowed to transmit the packet. If there is an attempt to send or receive unauthorized packets, they are discarded and corresponding audit records are generated.

The Packet Filter Policy allows a node to be configured to accept traffic only if it satisfies a set of rules based on network protocol and service as well as by source and destination address (per the Association Security Policy). Any traffic that fails to satisfy the acceptance rules will be discarded and corresponding audit records will be generated.

Regardless of information flow policy, each NSD is designed to only send information that is received (in either direction). For example, when a network packet is constructed and placed on the network, the NSD will ensure that only information intended to be sent by the Host is included in the packet.

#### 6.1.2.1 Association Security Policy

Operational Profiles, including Association Profiles, can only be created and changed by a NSM. Up to 5,000 Operational Profiles can be defined in the NSC. When a user logs[13] onto a NSD, the NSD downloads associations based on the Association Profile associated with the Operational Profile selected by the user. New associations may be subsequently downloaded or deleted if they are changed while a user is using the NSD. These associations control the ability to send to and receive from other nodes on the network.

Access control is enforced on each NSD by performing an association lookup using its local association table. The NSD always makes decisions based on the contents of its local association table. The association lookup can use either destination IP addresses or Ethernet addresses (on the local subnet). Each association lookup results in either: unavailable association (Association Security Policy failure), encrypted association (only encrypted packets are

[13] Note that in the case of a “No Card” node, a User is always exclusively assigned to the associated NSD and that User is logged on automatically, with a default Operational Profile, whenever the NSD is reset.

permitted), or clear text association. If the association is not permitted, the NSD sends an audit record to the NSC and discards the packet.

When encryption is required for a given information flow, the NSDs will negotiate traffic keys constrained by encryption configuration options (e.g., allowable algorithms) set by the NSM. Subsequently, the NSDs will encrypt the traffic in order to successfully transmit and receive the information within the established Association Security Policy rules.

If the traffic that is sent or received is broadcast IP traffic, the NSD must be configured to allow broadcast messages. If traffic that is sent or received is non-IP, the NSD must be configured to allow non-IP type traffic. If non-IP traffic is allowed, the NSD will either encapsulate it in IP or will forwarded it unmodified, depending on other configuration parameters.

Note that when an NSD is offline it can be configured to allow DHCP requests to originate from its attached host and responses to originate from the network. This is the only traffic that is allowed when an NSD is offline, and when the NSD goes online DHCP traffic is constrained by all of the information policy rules just like other traffic.

In addition to these special traffic handling considerations, a Network Security Manager can configure settings that apply to otherwise unidentified IT entities. If an IT entity cannot be specifically identified these settings will be used. Hence, an administrator can configure the policy strictly and allow communication only with known IT entities, or the administrator can choose to allow all IT entities to communicate in a common manner that can be as restrictive or permissive as necessary based on the configuration settings for all of the information flow policies. Note that this applies to all of the information flow policies.

#### 6.1.2.2 Mandatory Security Policy

Operational Profiles also include Security Profiles that are used to enforce the Mandatory Security Policy. Security Profiles can only be defined by a NSM and serve to define security windows, in terms of security levels and categories, for all nodes on the network. Each security window consists of maximum and minimum security levels, as well as allowable, disallowed, and mandatory security categories. Separate security windows are defined for transmitting and receiving; hence, a given Security Profile includes: Maximum Transmit Level, Minimum Transmit Level, Allowable Transmit Categories, Disallowed Transmit Categories, Mandatory Transmit Categories, Maximum Receive Level, Minimum Receive Level, Allowable Receive Categories, Disallowed Receive Categories, and Mandatory Receive Categories.

The NSM assigns Security Profiles to NSDs and Operational Profiles, and assigns Operational Profiles to users from the NSC. Each Security Profile can be assigned to one or more NSDs and one or more users (via Operational Profiles). On a NSD, the Security Profile defines the absolute limits for processing packets in the context of the Mandatory Security Policy. Each user must select an Operational Profile when logging onto an NSD. However, the Security Profile associated with the user's Operational Profile must represent a security window that is a subset of that defined in the Security Profile assigned to the NSD.

Each NSD is configured (via its Security Profile) with separate transmit and receive security windows that define the range of packets it will process. The NSD security windows are downloaded from the NSC to the NSD when the node is installed in order to restrict users from using inappropriate Security Profiles (contained in Operational Profiles). Based upon the identity of the user authenticated at the NSD and the Operational Profile selected by the user, the appropriate security window is automatically downloaded from the NSC to the NSD before any node data is transmitted or received. However, as described above, the Operational Profile selected by the user must satisfy the security constraints associated with the NSD. Note that the NSD Security Profile is not used while a user is logged in.

Before a NSD will transmit a packet the following conditions must be satisfied:

- Either the packet is appropriately labeled using a CIPSO format by the Host *or* the NSD will assign the node's default label as indicated in the corresponding Security Profile.
- The security level of the packet must be less than or equal to the Maximum Transmit Level and greater than or equal to the Minimum Transmit Level.

- The categories of the packet must be contained in the categories in the Allowable Transmit Categories set, must not contain any categories in the Disallowed Transmit Categories set, and must contain the categories in the Mandatory Transmit Categories set. As an exception, the security window can be configured to allow traffic without categories in its label to be acceptable even if the mandatory category set includes one or more categories.
    - Note that the NSM can configure the TOE such that it will not enforce mandatory category checks, as long as the traffic contains no categories.

Before an NSD will receive a packet the following conditions must be satisfied:

- The packet must be appropriately labeled using a CIPSO format, or the label will be assumed based on the Security Profile of the source node (as defined in the Operational Profile).
- The security level of the packet must be less than or equal to the Maximum Receive Level and greater than or equal to the Minimum Receive Level.
- The categories of the packet must be contained in the categories in the Allowable Receive Categories set, must not contain any categories in the Disallowed Receive Categories set, and must contain the categories in the Mandatory Receive Categories set. As an exception, the security window can be configured to allow traffic without categories in its label to be acceptable even if the mandatory category set includes one or more categories.
    - Note that the NSM can configure the TOE such that it will not enforce mandatory category checks, as long as the traffic contains no categories.

In order for the NSM to change a Security Profile, the Security Profile must not be in use. This effectively means that associated NSDs must be off-line and users must not be currently using an Operational Profile that includes the Security Profile.

Note that like the Association Security Policy, Mandatory Security Policy decisions are always made when data is sent and received by an NSD. However, the Mandatory Security Policy only applies to unicast IP type traffic since other traffic does not support the required labeling conventions. In addition, if data is being sent from a NSD to a CTN or OIPS, the NSD will also make a receive decision on behalf of the CTN or OIPS. This decision is based on the Security Profile the Operational Profile associated with the CTN or OIPS. If this decision fails, it is treated as if a receiving NSD failed to accept the information and the information is dropped and appropriate audit records are sent to the NSC.

#### 6.1.2.3 Packet Filter Policy

The Packet Filter Policy is implemented as an extension to the Association Security Policy. For any given association defined in an Association Profile, the Association Profile includes a Port Profile that defines network protocols and services that are either allowed or not allowed relative to transmit, receive, and TCP Open operations. The checks for packet filtering are performed in conjunction with those for the Association Security Policy for IP traffic. However, for non-IP traffic, decisions are based simply on the protocol (i.e., IP or not).

Note also that no information flows are allowed by default. NSDs are designed to prevent inappropriate information flows before and after a user logs on. When a NSD is offline, only limited control traffic (i.e., DHCP requests) can pass through the NSD, and only when explicitly allowed by the NSM. When a NSD is online, the selected Operational Profile is used to enforce all of the information flow policies. The NSM must explicitly define each information flow that is allowed before it can be used. Before a node (e.g., NSD) can effectively be used it must be defined, with an associated Security Profile. Whenever a new node is defined, it is added to each Association Profile, by default, such that it is initially not allowed to communicate with other nodes. When the NSM configures the node to allow transmit and/or receive operations, a Port Profile can also be assigned.

#### 6.1.2.4 Cryptographic Support

In order to support the encryption requirements, Diamond*TEK* includes a number of cryptographic implementations, as well as suitable pseudo random number generation and zeroization capabilities. These cryptographic capabilities are designed to conform with published standards as follows:

- The pseudo random number generation and zeroization capabilities are designed to meet FIPS 140-1 requirements.
- There are three cryptographic operations provided, all designed to conform with published standards:
  - Data encryption services – DES and triple DES (3DES)
  - Hashing – SHA-1
  - Key Exchange – Diffie-Hellman

Compliance with these cryptographic standards is demonstrated by independent third party testing. FIPS conformance is tested by the Cryptographic Module Validation (CMV) Program sponsored by NIST. IPsec testing (including Diffie-Hellman key exchange) is tested by the Virtual Private Network Consortium (VPNC).

| **Cryptographic Standard/Feature** | **Evaluation** | **Certificates** |
|---|---|---|
| Pseudo random number generation | FIPS 140-1 | #187, #213, others pending |
| Zeroization | FIPS 140-1 | #187, #213, others pending |
| DES | FIPS 46-3 | #132 |
| 3DES | FIPS 46-3 | #71 |
| SHA-1 | FIPS 180-1 | #63 |
| Diffie-Hellman | VPNC conformance testing | N/A |

The User Data Protection function is designed to satisfy the following security functional requirements:

- Association Security Policy
  - FDP_IFC.1(b)
  - FDP_IFF.1(a)
- Mandatory Security Policy
  - FDP_IFC.1(a)
  - FDP_IFF.2
- Packet Filter Policy
  - FDP_IFC.1(c)
  - FDP_IFF.1(b)
- Cryptographic Support
  - FCS_CKM.1
  - FCS_CKM.4
  - FCS_COP.1(a)

  - FCS_COP.1(b)
  - FCS_COP.1(c)

### 6.1.3 Identification and Authentication

DiamondTEK requires that NSMs and users must be identified and authenticated before they are allowed to perform any security-relevant actions on the network. Each of the identified roles is treated differently, however.

- NSMs are required to log in to the NSC application itself; both with a user ID and password. The NSM role is recognized only on the NSC and is therefore not valid for any NSD. Note that a NSM remains associated with the NSC after logging on until they log off.
- Users are identified and authenticated by inserting a personal authentication card into a NSD's card reader, selecting an Operational Profile, and entering Personal Identification Number (PIN), if configured to be required for the selected NSD. Alternately, for static network devices, the NSM can configure a NSD to be associated with a user representing the attached Host and to not require a card to be present to operate[14]. When such a user is created, it must be assigned exclusively to a single NSD[15]. Note that a user remains associated with a NSD after logging on until they log off (e.g., by removing their card). There is no mechanism to allow a user to log in to the NSC.

It is possible for a given user to serve in more than one of the identified roles. In that case, the user must meet the requirements of each of the applicable identification and authentication mechanisms as described above.

The NSM is able to configure a threshold for each user that defines how many failed attempts to log onto a NSD will be tolerated, after which the user account will be disabled.

The NSM must define users at the NSC. Each user is implicitly associated with the user role and has the following attributes defined in the TSF data managed by the NSC:

- Authentication Card (for authentication at a NSD) including identification and authentication information[16].
- A set of Operational Profiles – each including an Association Profile and Security Profile.
- Security Violation Thresholds.

The NSM, also implicitly associated with the NSM role, is defined simply by an identity and authentication data managed by the NSC. In addition to logging into the NSC application, the NSM must also have access to the host (IT environment) of the NSC.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_AFL.1
- FIA_ATD.1
- FIA_UAU.2
- FIA_UID.2
- FIA_USB.1

[14] When such a device is configured, the assigned User is automatically logged on, with its default Operational Profile, whenever the device is reset.

[15] Effectively, the administrator has procedurally authenticated the user by explicitly and exclusively assigning the user to be used whenever the associated NSD is online.

[16] Note that the Authentication Card itself is a physical device and is managed by the NSC only in the sense that the NSC defines its contents and stores it on the card when created.

### 6.1.4 Security Management

The notion of roles is realized in the sense that only users can log into NSDs and only administrators (i.e., NSMs) can log into the NSC.

All DiamondTEK security management tools are implemented on the NSC. In order to access any of the tools, a Network Security Manager must first be identified and authenticated by the NSC. The NSC provides commands to manage all aspects of the network state of operation, time and date, security audit function, Mandatory Security Policy, Association Security Policy, Packet Filter Policy, as well as to add, remove and configure NSDs, users, and NSMs in the DiamondTEK system.

Each of the information flow policies is designed to be restrictive by default. Each NSD must be assigned a security window before it can be initialized; hence the Mandatory Security Policy is restrictive in the sense that the NSM must assign security labels before any information can flow through a NSD. Alternately, no information is allowed to flow through a NSD unless it is explicitly allowed by an association profile. Hence, both the Association Security Policy and Packet Filter Policy are both restrictive in the sense that the NSM must explicitly allow an information flow before it can occur and each such allowance (i.e., association) includes source and destination address, encryption properties, as well as network protocol and service settings. Additionally, the configuration tools (i.e., commands) are designed to only allow secure values in the sense that only valid values are accepted for any of the configuration settings. Note that the various cryptographic evaluations (see Section 6.1.2.4) are assumed to have ensured that only appropriately secure values can be entered for cryptographic functions.

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1
- FMT_MSA.1(a)
- FMT_MSA.1(b)
- FMT_MSA.1(c)
- FMT_MSA.2
- FMT_MSA.3(a)
- FMT_MSA.3(b)
- FMT_MSA.3(c)
- FMT_MTD.1
- FMT_SMR.1

### 6.1.5 Protection of the TSF

The physical protection of the TSF is largely accomplished via protection of its environment, and logically the operating system is trusted to not negatively impact the TOE security functions given the assumption on the environment, A.Pltfrm. The only logical points of entry to the Diamond*TEK* system are the host-to-NSD interfaces and network-to-NSD interfaces. In order to send data to another host on a network, each host must send its data through its associated NSD. Physical protection must be adequate to ensure that NSDs remain appropriately connected to the hosts they are intended to protect. Note that the NSC is also connected to the network by a special NSD, NSD-Prime. The interfaces provided by the NSD-Prime are very limited and designed to support only minimal operational requirements (i.e., communication among the distributed TSF). For example, the NSD-Prime does not offer any functions related to security management of the Diamond*TEK* system. Both NSD and the NSD-Prime serve to protect the TSF by limiting and controlling the functions that they offer to the uncontrolled network environment.

Since TSF data is passed across the network while the TOE is operational, the network must either be protected or the traffic must be encrypted to ensure that there is no inappropriate disclosure or modification. The Association

Security Policy, and associated Cryptographic Support, enables the encryption of traffic. The NSD-Prime is designed such that it will only communicate with known NSDs and then only using encrypted network traffic. Similarly, NSDs are designed to send TSF data (e.g., audit records, logon requests) only to the NSC that was used to install them. Hence, TSF data is always protected by encryption.

The "subjects" in the Diamond*TEK* system are effectively logged on Network Security Managers and Users. There is a single NSM interface provided by the NSC and as such only a single NSM can be logged in at once. Similarly, only a single User can be logged into a NSD at any given time. These restrictions ensure that the domains of the subjects are appropriately separated.

In addition to ensuring that the TSF is appropriately protected, the IT environment is expected to provide reliable timestamps for use by the TSF. In particular, in conjunction with the Security Audit function. This is accomplished by providing access to a real-time clock that can be accessed by the TSF and managed (e.g., change the time) only by the NSM via the NSC.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_RVM.1
- FPT_SEP.1

The following security functional requirements are additionally satisfied by the IT environment:

- FPT_STM.1

## 6.2 TOE Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL4 assurance requirements:

- Process Assurance;
- Delivery and Guidance;
- Design Documentation;
- Tests; and,
- Vulnerability Assessment.

### 6.2.1 Process Assurance

The configuration management measures applied by Cryptek ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Cryptek ensures changes to the implementation representation are controlled with the support of automated tools and that TOE associated configuration item modifications are properly controlled. Cryptek performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, life-cycle documentation, vulnerability analysis documentation, configuration management documentation, and security flaws.

Cryptek ensures the adequacy of the procedures used during the development and maintenance of the TOE through the use of a comprehensive life-cycle management plan. Cryptek includes security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure operation of the TOE. Cryptek achieves this through the use of a documented model of the TOE life cycle and well-defined development tools that yield consistent and predictable results.

These procedures are documented in:

- Diamond*TEK* Configuration Management Plan
- Diamond*TEK* Life Cycle Management Plan

The Process Assurance measures satisfy the following Assurance requirements:

- ACM_AUT.1;
- ACM_CAP.4;
- ACM_SCP.2;
- ALC_DVS.1;
- ALC_LCD.1; and,
- ALC_TAT.1.

### 6.2.2 Delivery and Guidance

Cryptek provides delivery documentation and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. Cryptek's delivery procedures describe the electronic and non-electronic procedures to be used to detect modification to the TOE. These procedures are documented in:

- Cryptek Delivery and Operation Procedures

Cryptek provides administrator and user guidance on how to utilize the TOE security functions and warnings to Network Security Managers and users about actions that can compromise the security of the TOE. The installation and generation procedures, included in the administrator guidance, describe the steps necessary to install Diamond*TEK* in accordance with the evaluated configuration. administrator and user guidance is documented in:

- Diamond*TEK* 10/100 Secure Network Administration
- Release Notes for Diamond*TEK*™ 10/100 Secure Network Administration
- Diamond*TEK* 10/100 User Pamphlet
- Diamond*TEK* User's Guide

The Delivery and Guidance assurance measure satisfies the following Assurance requirements:

- ADO_DEL.2;
- ADO_IGS.1;
- AGD_ADM.1; and,
- AGD_USR.1.

### 6.2.3 Development

The Design Documentation security assurance measure satisfies the following security assurance requirement:

- ADV_FSP.2: The Diamond*TEK* Functional Specification fully describes all interfaces to the TSF.
- ADV_HLD.2: The Diamond*TEK* High-level Design Specification satisfies the requirement for decomposing the TOE into subsystems and fully describes each subsystem, including inter-subsytem interfaces.
- ADV_LLD.1: The Diamond*TEK* Low-level Design Specification satisfies the requirement to decompose each subsystem into modules and fully describes each module.
- ADV_IMP.1: A subset of the source code and hardware diagrams used to generate the TOE satisfies this requirement.

- ADV_RCR.1: Most of the correspondence between the various design documentation is implicit to the way in which the documentation is structured. The way that this correspondence is evident within the design documentation is:
    - ST-TSS to FSP: The Diamond*TEK* Functional Specification describes how the interfaces correspond with the security functions in the ST.
    - FSP to HLD: The Diamond*TEK* High-level Design Specification describes how the various security behaviour in the Diamond*TEK* Functional Specification are further refined.
    - HLD to LLD: The Diamond*TEK* Low-level Design Specification describes how the various security behaviour in the Diamond*TEK* High-level Design Specification are further refined.
    - LLD to IMP: The Diamond*TEK* Low-level Design Specification also serves to correspond modules with their specific implementations.
- ADV_SPM.1: The Diamond*TEK* Security Policy Model models the entities and rules related to the policies for identification and authentication, audit, and all of the information flow policies. Additionally, correspondence with the Diamond*TEK* Functional Specification is described.

## 6.2.4 Tests

The Tests assurance measure satisfies the following assurance requirements:

- ATE_COV.2: The test case descriptions (in the Diamond*TEK* Functional Specification) describe the test cases for each of the security-relevant interfaces of the TOE. The descriptions indicate which tests are used to satisfy the test cases identified for each interface.
- ATE_DPT.1: The test case descriptions (in the Diamond*TEK* High-level Design Specification) include more detailed test case descriptions that demonstrate that all of the corresponding interfaces are appropriately exercised.
- ATE_FUN.1: The Functional Specification & High-level Design Test Plan, Parts I and II, describes the security functions to be tested, how to successfully test all of them, the expected results, and the actual test results after exercising all of the tests.
- ATE_IND.2: The TOE and test documentation will be available for independent testing.

## 6.2.5 Vulnerability Assessment

### 6.2.5.1 Evaluation of Misuse

The Diamond*TEK* 10/100 Secure Network Administration guide and Diamond*TEK* 10/100 User Pamphlet describe the operation of Diamond*TEK* and how to maintain a secure state. These guides also describe all operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references. These guides are documented in:

- Diamond*TEK* 10/100 Secure Network Administration
- Diamond*TEK* 10/100 User Pamphlet
- Diamond*TEK* User’s Guide

The misuse analysis shows that the administrative and user guidance completely addresses managing the TOE in a secure configuration.

- The Diamond*TEK* Misuse Analysis

#### 6.2.5.2 Strength of TOE Security Functions and Vulnerability Analysis

Cryptek performs vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE. All of the SOF claims are based primarily on cryptographic functions and based on the SOF rationale in this ST, a separate SOF analysis is not applicable. The vulnerability analysis is documented in:

- The Diamond*TEK* Vulnerability Analysis

The Vulnerability Assessment assurance measure satisfies the following assurance requirements:

- AVA_MSU.2;
- AVA_SOF.1; and,
- AVA_VLA.2.

# 7. Protection Profile Claims

There is no claimed PP conformance.

# 8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- TOE Summary Specification;
- Security Functional Requirement Dependencies; and
- Internal Consistency.

## 8.1 Security Objectives Rationale

This section shows that all threats, secure usage assumptions, and organizational security policies are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

### 8.1.1 Security Objectives for IT Environment Rationale

This section provides evidence demonstrating the coverage of threats and organizational policies by the IT security objectives.

| Objectives<br>Environment | O.MAC1 | O.MAC2 | O.MAC3 | O.AAC1 | O.AAC2 | O.AAC3 | O.Thresh | O.Idauth | O.Repeat | O.Mediat | O.Secsta | O.Selpro | O.Audrec | O.Accoun | O.Secfun | O.Limext | O.Audsaf | O.Audlos | OE.Usract | OE.Admins | OE.Guidan | OE.Protct | OIE.Time | OIE.Audsup |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T.Noauth | | | | | | | | X | | | X | | | | X | X | | | | | | | | |
| T.Repeat | | | | | | | X | | X | | | | | | | | | | | | | | | |
| T.Aspoof | | | | | | | | | | X | | | | | | | | | | | | | | |
| T.Mediat | | | | | | | | | | X | | | | | | | | | | | | | | |
| T.Oldinf | | | | | | | | | | X | | | | | | | | | | | | | | |
| T.Procom | | | | | | X | | | | | | | | | | | | | | | | | | |
| T.Audacc | | | | | | | | | | | | | | X | | | X | | | | | | | X |
| T.Selpro | | | | | | | | X | | | X | X | | | | | | | | | | | | |
| T.Audful | | | | | | | | | | | | X | | | X | | | X | | | | | | |
| T.Tusage | | | | | | | | | | | | | X | X | | | | | | | | | X | X |
| P.Clsify | X | X | X | | | | | | | X | | | | | | | | | | | | | | |
| P.Asciat | | | | X | X | X | | | | X | | | | | | | | | | | | | | |
| P.Athrzd | | | | | | | | X | | | | | | | | | | | | | | | | |
| A.Usract | | | | | | | | | | | | | | | | | | | X | | | | | |
| A.Noevil | | | | | | | | | | | | | | | | | | | | X | | | | |
| A.Physec | | | | | | | | | | | | | | | | | | | | | | X | | |

| Objectives<br>Environment | O.MAC1 | O.MAC2 | O.MAC3 | O.AAC1 | O.AAC2 | O.AAC3 | O.Thresh | O.Idauth | O.Repeat | O.Mediat | O.Secsta | O.Selpro | O.Audrec | O.Accoun | O.Secfun | O.Limext | O.Audsaf | O.Audlos | OE.Usract | OE.Admins | OE.Guidan | OE.Protct | OIE.Time | OIE.Audsup |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A.Singen | | | | | | | | | | | | | | | | | | | | | X | | | |
| A.Pltfrm | | | | | | | | | | | | | | | | | | | | | X | X | | |
| A.Exttim | | | | | | | | | | | | | | | | | | | | | | | X | |

Table 4 Environment to Objective Correspondence

#### 8.1.1.1 T.Noauth

*An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.*

This threat is countered by ensuring that

- Users and administrators must be identified and authenticated before they can perform any other function (O.Idauth).
- upon start-up the TOE appropriately enforces its security policies (O.Secsta),
- only authorized administrators can manage the security functions (O.Secfun), and
- limiting external access to TOE security functions (O.Limext).

#### 8.1.1.2 T. Repeat

*An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.*

This threat is countered by ensuring that

- administrators can establish thresholds to signal when such an event may have happened (O.Thresh), and
- by requiring the TOE to automatically disable user accounts when defined thresholds are exceeded (O.Repeat).

#### 8.1.1.3 T. Aspoof

*An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.*

This threat is countered by ensuring that

- all information flows are mediated by the TOE (O.Mediat).

#### 8.1.1.4 T. Mediat

*An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.*

This threat is countered by ensuring that

- all information flows are mediated by the TOE (O.Mediat).

#### 8.1.1.5 T. Oldinf

*Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.*

This threat is countered by ensuring that

- no residual information is ever retransmitted (O.Mediat).

#### 8.1.1.6 T. Procom

*An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between separate parts of the TSF.*

This threat is countered by ensuring that

- All TSF data is protected while being transferred between parts of the TOE (O.AAC3).

#### 8.1.1.7 T. Audacc

*Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.*

This threat is countered by ensuring that

- User and administrator actions are audited (O.Accoun),
- an audit trail is provided that can be effectively reviewed (OIE.Audsup), and
- the audit trail is protected so that only an administrator can view or modify its contents (O.Audsaf).

#### 8.1.1.8 T. Selpro

*An unauthorized person may read, modify, or destroy security critical TOE configuration data.*

This threat is countered by ensuring that

- upon start-up the TOE appropriately enforces its security policies (O.Secsta),
- security functions cannot be deactivated or bypassed (O.Selpro), and
- administrators can only perform management functions after being identified and authenticated (O.Idauth).

#### 8.1.1.9 T. Audful

*An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.*

This threat is countered by ensuring that

- security functions cannot be deactivated or bypassed (O.Selpro),
- only authorized administrators can manage the security functions (O.Secfun), and
- the TOE can limit the loss of audit information (O.Audlos).

#### 8.1.1.10 T. Tusage

*The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.*

This threat is countered by ensuring that

- administrator actions are auditable (O.Accoun),
- reliable time stamps are available for the audit trail (OIE.Time),
- an audit trail records security-reletated events (O.Audrec), and
- an audit trail is provided that can be effectively reviewed (OIE.Audsup).

#### 8.1.1.11 P.Clsify

*The TOE must limit access to information based on sensitivity of information and the clearance of subjects. The access rules must prevent a subject from accessing information which is of a higher or non-comparable sensitivity than it is cleared to process. The method for classification of information and clearance of subjects is set forth by the organization. The determination of classification and clearance is outside the scope of the TOE; the TOE is expected only to enforce the access rules.*

This policy is satisfied by ensuring that

- all network nodes and users are assigned security labels (O.MAC1),

- information can flow between network nodes only if allowed based on the security labels of the associated users and information being communicated (O.MAC2),
- users can only use network nodes that can process information in a range that includes the entire processing range of the user (O.MAC3), and
- the security policy enforcing functions cannot be bypassed or otherwise subverted (O.Mediat).

#### 8.1.1.12 P.Asciat

*The TOE will ensure that information can only flow between nodes as explicitly allowed by an Administrator. Unlike the Classification policy, the association policy is based on a simple matching criteria. Each allowable communication path must be explicitly defined by an authorized administrator. Furthermore, the authorized administrator must be able to specify whether the information is further protected (e.g., using encryption) while it is in transit across the TSF boundary. The determination of which communication paths should be allowed is outside the scope of the TOE; the TOE is expected only to enforce the associations it is configured with.*

This policy is satisfied by ensuring that

- the security policy enforcing functions cannot be bypassed or otherwise subverted (O.Mediat),
- an administrator can authorize information to flow to a network node (O.AAC1),
- information can only flow to a network node if explicitly authorized by an administrator (O.AAC2), and
- information will be encrypted when outside the control of the TSF when necessary (i.e., at the administrator option) (O.AAC3).

#### 8.1.1.13 P.Athrzd

*A user must be identified and authenticated at each node before it can send or receive traffic on the physical network. The determination of whether a user should be allowed to access the TOE is outside the scope of the TOE; the TOE is expected only to ensure that the identification and authentication information provided by the user is consistent information that has been configured in the TOE by an authorized administrator.*

This policy is satisfied by ensuring that

- Users must be identified and authenticated before they can perform any other function (O.Idauth).

#### 8.1.1.14 A.Usract

*Users will follow provided guidance and will not attempt to violate the information flow policies by entering data at the user interface that is not appropriate for the associated network node.*

This assumption is addressed by the non-IT environment objective that users will be appropriately trained and will follow prescribed procedures (OE.Usract).

#### 8.1.1.15 A.Noevil

*Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.*

This assumption is addressed by the non-IT environment objective that administrators will be competent, appropriately trained, and not malicious (OE.Admins).

#### 8.1.1.16 A.Physec

*The TOE is physically secure; specifically, to ensure that NSDs remain attached to their associated Hosts and to ensure that only authorized administrators can access the management console.*

This assumption is addressed by the non-IT environment objective that the TOE will be appropriately physically protected (OE.Protct).

#### 8.1.1.17 A.Singen

*Information cannot flow among the internal and external networks (or hosts) unless it passes through the TOE.*

This assumption is addressed by the non-IT environment objective that the TOE will be installed and operated in a manner that maintains security (OE.Guidan).

#### 8.1.1.18 A.Pltfrm

*The IT environment will be suitable to support the correct operation of the TOE that will not negatively affect the security functions of the TOE.*

This assumption must primarily be addressed by the operating platform that hosts the TOE. While that is outside the scope of the TOE, this assumption is addressed to some extent by the non-IT environment objectives that the TOE will be installed and operated in a manner that maintains security (OE.Guidan) and that the TOE will be appropriately physically protected (OE.Protct).

#### 8.1.1.19 A.Exttim

*The IT environment will provide a time resource that can be used by the TOE to reliably represent the date and time of day.*

This assumption is addressed by the IT environment objective that the environment must provide reliable time information (OIE.Time).

## 8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that Table 5 indicates the requirements that effectively satisfy the individual objectives. Objectives for the IT environment are satisfied only by requirements for the IT environment, however some of those requirements also support, in some relatively small way, the TOE security objectives.

### 8.2.1 Security Functional Requirements Rationale

| Requirements<br>Objectives | FAU_ARP.1 | FAU_GEN.1 | FAU_GEN.2 | FAU_SAA.1 | FAU_SAR.1 | FAU_SAR.2 | FAU_SEL.1 | FAU_STG.1 | FAU_STG.4 | FCS_CKM.1 | FCS_CKM.4 | FCS_COP.1(a) | FCS_COP.1(b) | FCS_COP.1(c) | FDP_IFC.1(a) | FDP_IFC.1(b) | FDP_IFC.1(c) | FDP_IFF.1(a) | FDP_IFF.1(b) | FDP_IFF.2 | FIA_AFL.1 | FAI_ATD.1 | FIA_UAU.2 | FIA_UID.2 | FIA_USB.1 | FMT_MOF.1 | FMT_MSA.1(a) | FMT_MSA.1(b) | FMT_MSA.1(c) | FMT_MSA.2 | FMT_MSA.3(a) | FMT_MSA.3(b) | FMT_MSA.3(c) | FMT_MTD.1 | FMT_SMR.1 | FPT_RVM.1 | FPT_SEP.1 | FPT_STM.1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O.MAC1 | | | | | | | | | | | | | | | | | | | | X | | | | | | | | | | | | | | | | | | |
| O.MAC2 | | | | | | | | | | | | | | | X | | | | | X | | | | | | | | | | | | | | | | | | |
| O.MAC3 | | | | | | | | | | | | | | | X | | | | | X | | | | | | | | | | | | | | | | | | |
| O.AAC1 | | | | | | | | | | | | | | | | | | | X | | | | | | | | | | | | | | | | | | | |
| O.AAC2 | | | | | | | | | | | | | | | | X | | | X | | | | | | | | | | | | | | | | | | | |
| O.AAC3 | | | | | | | | | | X | X | X | X | X | | | | | X | | | | | | | | | | | | | | | | | | | |
| O.Thresh | X | | | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.Idauth | | | | | | | | | | | | | | | | | | | | | | X | X | X | X | | | | | | | | | | | | | |
| O.Repeat | | | | | | | | | | | | | | | | | | | | | X | | | | | | | | | | | | | | | | | |
| O.Mediat | | | | | | | | | | | | | | | X | X | X | X | X | X | | | | | | | X | X | X | X | X | X | X | | | | | |
| O.Secsta | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | |
| O.Selpro | | | | | | | | X | X | | | | | | | | | | | | X | | | | | | | | | | | | | | | X | X | |
| O.Audrec | | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.Accoun | | X | X | | | | | | | | | | | | | | | | | | | | | X | | | | | | | | | | | | | | |
| O.Secfun | | | | | | X | | X | | | | | | | | | | | | | | | | | | X | X | X | X | | X | X | X | X | X | | | |
| O.Limext | | | | | | | | | | | | | | | | | | | | | | | | | | X | | | | | | | | X | | | | |
| O.Audsaf | | | | | | X | | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| Requirements<br>Objectives | FAU_ARP.1 | FAU_GEN.1 | FAU_GEN.2 | FAU_SAA.1 | FAU_SAR.1 | FAU_SAR.2 | FAU_SEL.1 | FAU_STG.1 | FAU_STG.4 | FCS_CKM.1 | FCS_CKM.4 | FCS_COP.1(a) | FCS_COP.1(b) | FCS_COP.1(c) | FDP_IFC.1(a) | FDP_IFC.1(b) | FDP_IFC.1(c) | FDP_IFF.1(a) | FDP_IFF.1(b) | FDP_IFF.2 | FIA_AFL.1 | FAI_ATD.1 | FIA_UAU.2 | FIA_UID.2 | FIA_USB.1 | FMT_MOF.1 | FMT_MSA.1(a) | FMT_MSA.1(b) | FMT_MSA.1(c) | FMT_MSA.2 | FMT_MSA.3(a) | FMT_MSA.3(b) | FMT_MSA.3(c) | FMT_MTD.1 | FMT_SMR.1 | FPT_RVM.1 | FPT_SEP.1 | FPT_STM.1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O.AudIos | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OE.Usract | Addressed by the environment and assurance requirements, see below. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OE.Admins | Addressed by the environment and assurance requirements, see below. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OE.Guidan | Addressed by the environment and assurance requirements, see below. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OE.Protct | Addressed by the environment and assurance requirements, see below. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OIE.Time | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X |
| OIE.Audsup | | | | | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Table 5 Objective to Requirement Correspondence

### 8.2.1.1 O.MAC1

*The TSF shall allow an authorized administrator to assign security labels and categories to network nodes and users.*

This objective is satisfied by requiring that subjects and objects must have security labels (FDP_IFF.2).

### 8.2.1.2 O.MAC2

*The TSF shall restrict the flow of information between network nodes based on security labels of associated users and information that is being communicated.*

This objective is satisfied by requiring that information can only flow based on the relationship of subject and object labels (FDP_IFF.2) and by requiring that all information flows are subject to this policy (FDP_IFC.1(a)).

### 8.2.1.3 O.MAC3

*The TSF shall restrict a user to using only network nodes that allow a range of security labels that include those of the user.*

This objective is satisfied indirectly by requiring that information can only flow based on the relationship of subject and object labels (FDP_IFF.2). The relationship is indirect since there is no direct requirement addressing the user-NSD relationship, but since both the user and NSD are subjects and they must both simultaneously conform to the requirement regarding information flow it is necessary that the user's effective security labels cannot exceed those of the NSD where he is logged in.

### 8.2.1.4 O.AAC1

*The TSF shall allow an authorized administrator to explicitly define allowed information flows between specific network nodes.*

This objective is satisfied by requiring that a table of allowed flows between source and destination subjects must be configured (FDP_IFF.1(a)).

### 8.2.1.5 O.AAC2

*The TSF shall restrict all information flows except those explicitly allowed by an authorized administrator.*

This objective is satisfied by requiring that information can only flow based on the configured association tables (FDP_IFF.1(a)) and by requiring that all information flows are subject to this policy (FDP_IFC.1(b)).

### 8.2.1.6 O.AAC3

*The TSF shall be able to protect information, using encryption, while it is in transit between parts of the TOE. All TSF data must be protected while outside the control of the TOE.*

This objective is satisfied by requiring that information must be encrypted before it can flow when indicated in the configured association tables (FDP_IFF.1(a)) and by requiring that all information flows are subject to this policy (FDP_IFC.1(b)).

### 8.2.1.7 O.Thresh

*The TSF shall allow audit thresholds to be defined that will trigger alarms when attempted policy violations exceed the defined thresholds.*

This objective is satisfied by requiring that administrators can define thresholds and the TOE will use those thresholds to detect potential security violations (FAU_SAA.1) and by requiring that the TOE must issue an alarm when such a violation has been detected (FAU_ARP.1).

### 8.2.1.8 O.Idauth

*The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.*

This objective is satisfied by requiring that users (including administrators) are assigned identifying attributes (FIA_ATD.1), by requiring that users must be identified and authenticated before they can use any other TSF functions (FIA_UAU.2 and FIA_UID.2), and by requiring that the user's identity is continuously associated with the user after being authenticated (FIA_USB.1).

### 8.2.1.9 O.Repeat

*The TSF shall ensure that if a user repeatedly fails to be authenticated, the user account will be disabled automatically.*

This objective is satisfied by requiring that the TOE will disable a users account after a defined number of failed authentication attempts (FIA_AFL.1).

### 8.2.1.10 O.Mediat

*The TOE must mediate the flow of all information from users on a connected network to users on another connected network, and must ensure that residual information from a previous information flow is not transmitted in any way.*

This objective is satisfied by requiring that each of the information flow security policies is based on a defined set of rules (FDP_IFF.1(*) and FDP_IFF.2), by requiring that the policies are enforced for all information flows (FDP_IFC.1(*)), by requiring that the information flows are restrictive by default (FMT_MSA.3(*)), by requiring that only an administrator can modify the behavior of the information flows (FMT_MSA.1(*)), by requiring administrators to enter secure values (FMT_MSA.2), and by requiring encryption capabilities to protect TSF data and other information when it passes outside the control of the TOE (FCS_COP.1(*), FCS_CKM.1.

### 8.2.1.11 O.Secsta

*Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.*

This requirement is satisfied by requiring that each of the information flow security policies is assigned restrictive values by default (FMT_MSA.3(*)).

### 8.2.1.12 O.Selpro

*The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.*

This objective is satisfied by requiring that the audit trail is protected and the TOE must limit the number of audit records that can be lost when the audit trail becomes full (FAU_STG.1 and FAU_STG.4), by requiring that users accounts must be locked after repeated failed authentication attempts (FIA_AFL.1), and by requiring that the TOE security enforcement functions must be invoked before the function can be performed and that the TOE must protect itself from tampering (FPT_RVM.1 and FPT_SEP.1).

### 8.2.1.13 O.Audrec

*The TOE must provide a means to record an audit trail of security-related events, with accurate dates and times.*

This objective is satisfied by requiring the TOE to generate records of security-related audit events and apply time stamps to the audit records that are generated (FAU_GEN.1).

### 8.2.1.14 O.Accoun

*The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.*

This objective is satisfied by requiring that all users are identified before they can perform any other TOE functions (FIA_UID.2), by requiring that security relevant user and administrator actions are audited (FAU_GEN.1), and by requiring that audit events indicate which user caused the action (FAU_GEN.1 and FAU_GEN.2).

### 8.2.1.15 O.Secfun

*The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.*

This objective is satisfied by requiring that there is an administrator role (FMT_SMR.1), by requiring that administrative functions are available only to administrators (FMT_MOF.1, FMT_MSA.1(*), FMT_MTD.1, FAU_SAR.2, and FAU_STG.1), and by requiring that administrator functions must be available (FMT_MSA.3(*)).

### 8.2.1.16 O.Limext

*The TOE must provide the means to control and limit access to TOE security functions by an authorized external IT entity.*

This objective is satisfied by requiring that only an authorized administrator can perform administration functions (FMT_MOF.1 and FMT_MTD.1).

### 8.2.1.17 O.Audsaf

*The TSF shall protect the audit trail so that only an authorized administrator can read or modify the audit trail. The TSF shall also provide the ability to effectively review the audit trail.*

This objective is satisfied by requiring that only authorized users can read the audit records (FAU_SAR.2) and by requiring that audit records must be protected for unauthorized deletion or modification (FAU_STG.1).

### 8.2.1.18 O.Audlos

*The TSF shall be configurable to limit the potential loss of audit information.*

This objective is satisfied by requiring that an administrator can select a subset of audit events to collect in the audit trail (FAU_SEL.1), requiring that only appropriately authorized users can delete audit records and audit record loss will be limited (FAU_STG.1), and by requiring that the administrator can configure the system to shut down Nodes if the audit trail becomes full (FAU_STG.4).

#### 8.2.1.19 OE.Usract

*Individuals intended to use the TOE will follow procedures applicable to the TOE's operation.*

This objective must be satisfied by the environment but is supported by the requirement for user guidance (AGD_USR.1).

#### 8.2.1.20 OE.Admins

*Individuals responsible for installing and managing the TOE will be competent and non-malicious.*

This objective must be satisfied by the environment but is supported by the requirement for administrator guidance (AGD_ADM.1).

#### 8.2.1.21 OE.Guidan

*The TOE must be delivered, installed, administered, and operated in a manner that maintains security.*

This objective must be satisfied by the environment but is supported by the requirement for administrator guidance (AGD_ADM.1) and delivery and installation guidance (ADO_DEL.2, ADO_IGS.1).

#### 8.2.1.22 OE.Protct

*The TOE shall be appropriately physically protected.*

This objective must be satisfied by the environment but is supported by the requirement for administrator guidance (AGD_ADM.1) and delivery and installation guidance (ADO_DEL.2, ADO_IGS.1).

#### 8.2.1.23 OIE.Time

*The environment shall provide a means to obtain reliable time information.*

This objective is satisfied by requiring that reliable time stamps are available to the TSF (FPT_STM.1).

#### 8.2.1.24 OIE.Audsup

*The environment shall provide features necessary to effectively review the audit trail.*

This objective is satisfied by requiring that audit records can be stored and effectively reviewed using features of the IT environment supporting the TSF (FAU_SAR.1)

## 8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL4 assurance package and is based on good rigorous commercial development practices. This ST has been developed for a generalized environment with a medium level of risk to the assets. The Security Objectives for the TOE were reviewed and EAL4 was found to be sufficient to address them.

## 8.4 Requirement Dependency Rationale

The ST satisfies all the requirement dependencies of the Common Criteria, except as noted below. Table 6 Requirement Dependency Rationale lists each requirement from Section 5.1 with a dependency and indicates which requirement was included to satisfy the dependency, if any. For each dependency not included, a justification is provided.

| **Functional Component** | **Dependency** | **Included** |
|---|---|---|
| Security alarms (**FAU_ARP.1**) | FAU_SAA.1 | FAU_SAA.1 |
| Audit data generation (**FAU_GEN.1**) | FPT_STM.1 | FPT_STM.1 |
| User identity association (**FAU_GEN.2**) | FAU_GEN.1 | FAU_GEN.1 |
| | FIA_UID.1 | FIA_UID.2[*] |
| Potential violation analysis (**FAU_SAA.1**) | FAU_GEN.1 | FAU_GEN.1 |
| Audit review (**FAU_SAR.1**) | FAU_GEN.1 | FAU_GEN.1 |
| Restricted audit review (**FAU_SAR.2**) | FAU_SAR.1 | FAU_SAR.1 |
| Selective audit (**FAU_SEL.1**) | FAU_GEN.1 | FAU_GEN.1 |
| | FMT_MTD.1 | FMT_MTD.1 |
| Protected audit trail storage (**FAU_STG.1**) | FAU_GEN.1 | FAU_GEN.1 |
| Prevention of audit data loss (**FAU_STG.4**) | FAU_STG.1 | FAU_STG.1 |
| Cryptographic key generation (**FCS_CKM.1**) | FCS_CKM.2 or FCS_COP.1 | FCS_COP.1(*) |
| | FCS_CKM.4 | FCS_CKM.4 |
| | FMT_MSA.2 | FMT_MSA.2 |
| Cryptographic key destruction (**FCS_CKM.4**) | FDP_ITC.1 or FCS_CKM.1 | FCS_CKM.1 |
| | FMT_MSA.2 | FMT_MSA.2 |
| Cryptographic operation (**FCS_COP.1(a)**) | FDP_ITC.1 or FCS_CKM.1 | FCS_CKM.1 |
| | FCS_CKM.4 | FCS_CKM.4 |
| | FMT_MSA.2 | FMT_MSA.2 |
| Cryptographic operation (**FCS_COP.1(b)**) | FDP_ITC.1 or FCS_CKM.1 | FCS_CKM.1 |
| | FCS_CKM.4 | FCS_CKM.4 |
| | FMT_MSA.2 | FMT_MSA.2 |
| Cryptographic operation (**FCS_COP.1(c)**) | FDP_ITC.1 or FCS_CKM.1 | FCS_CKM.1 |
| | FCS_CKM.4 | FCS_CKM.4 |
| | FMT_MSA.2 | FMT_MSA.2 |
| Complete information flow control (**FDP_IFC.1(a)**) | FDP_IFF.1 | FDP_IFF.2[*] |
| Complete information flow control (**FDP_IFC.1(b)**) | FDP_IFF.1 | FDP_IFF.1(a) |
| Complete information flow control (**FDP_IFC.1(c)**) | FDP_IFF.1 | FDP_IFF.1(b) |
| Simple security attributes (**FDP_IFF.1(a)**) | FDP_IFC.1 | FDP_IFC. 1(b)[*] |
| | FMT_MSA.3 | FMT_MSA.3(b) |
| Simple security attributes (**FDP_IFF.1(b)**) | FDP_IFC.1 | FDP_IFC.1(c)[*] |
| | FMT_MSA.3 | FMT_MSA.3(c) |
| Hierarchical security attributes (**FDP_IFF.2**) | FDP_IFC.1 | FDP_IFC.1(a)[*] |
| | FMT_MSA.3 | FMT_MSA.3(a) |
| Authentication failure handling (**FIA_AFL.1**) | FIA_UAU.1 | FIA_UAU.2[*] |
| User attribute definition (**FIA_ATD.1**) | none | - |
| User authentication before any action (**FIA_UAU.2**) | FIA_UID.1 | FIA_UID.2[*] |
| User identification before any action (**FIA_UID.2**) | none | - |
| User-subject binding (**FIA_USB.1**) | FIA_ATD.1 | FIA_ATD.1 |
| Management of security functions behaviour (**FMT_MOF.1**) | FMT_SMR.1 | FMT_SMR.1 |
| Secure security attributes (**FMT_MSA.2**) | ADV_SPM.1 | ADV_SPM.1 |
| | FDP_ACC.1 or FDP_IFC.1 | (See below) |
| | FMT_MSA.1 | (See below) |
| | FMR_SMR.1 | FMT_SMR.1 |
| Management of security attributes (**FMT_MSA.1(a)**) | FDP_ACC.1 or FDP_IFC.1 | FDP_IFC.1(a)[*] |
| | FMR_SMR.1 | FMT_SMR.1 |
| Management of security attributes (**FMT_MSA.1(b)**) | FDP_ACC.1 or FDP_IFC.1 | FDP_IFC.1(b)[*] |
| | FMR_SMR.1 | FMT_SMR.1 |
| Management of security attributes (**FMT_MSA.1(c)**) | FDP_ACC.1 or FDP_IFC.1 | FDP_IFC.1(c)[*] |
| | FMR_SMR.1 | FMT_SMR.1 |
| Static attribute initialization (**FMT_MSA.3(a)**) | FMT_SMR.1 | FMT_SMR.1 |
| | FMT_MSA.1 | FMT_MSA.1(a) |
| Static attribute initialization (**FMT_MSA.3(b)**) | FMT_SMR.1 | FMT_SMR.1 |
| | FMT_MSA.1 | FMT_MSA.1(b) |
| Static attribute initialization (**FMT_MSA.3(c)**) | FMT_SMR.1 | FMT_SMR.1 |
| | FMT_MSA.1 | FMT_MSA.1(c) |

[*] This dependency is satisfied by a component that is hierarchically greater, according to CC Part 2, than is required.

| **Functional Component** | **Dependency** | **Included** |
|---|---|---|
| Management of TSF data (**FMT_MTD.1**) | FMT_SMR.1 | FMT_SMR.1 |
| Security roles (**FMT_SMR.1**) | FIA_UID.1 | FIA_UID.2* |
| Non-bypassability of the TSP (**FPT_RVM.1**) | none | - |
| TSF domain separation (**FPT_SEP.1**) | none | - |
| Reliable time stamps (**FPT_STM.1**) | none | - |

Table 6 Requirement Dependency Rationales

According to the CC Part 2, FDP_ACC.1 or FDP_IFC.1, and FMT_MSA.1, is required as a dependency for FMT_MSA.2. However, FMT_MSA.2 is included in this security target as a result of including cryptographic requirements and not information flow or access control requirements. This security target does include multiple information flow policies and their associated requirements and therefore technically satisfies the dependency. However, while this requirement should only be relevant to attributes associated with cryptographic operations, there seems to be no way to limit the scope of the requirement as taken from the CC v2.1.

## 8.5 Explicitly Stated Requirements Rationale

All requirements in this ST are reproduced relative to the requirements defined in CC v2.1, using the conventions described in Section 1.4.1.

In the context of CC v2.1 and International Interpretations of the CC (as of the date of this ST), the ST does not contain any explicitly stated requirements.

In the context of U.S. National interpretations of the CC (as of the date of this ST), the ST does not contain any explicitly stated requirements. However, it should be noted that one interpreted requirement has been *refined* (in accordance with the CC refinement rules) to its original form defined in CC v2.1.

- *Protected audit trail storage (FAU_STG.1)*: U.S National interpretations I-0422 and I-0423 serve to modify the original requirement by making it clear that the requirement is limited to unauthorized modifications and deletion or modification of audit records in the audit trail. Both of these changes serve to make implications in the CC explicit in the requirement and might also serve to narrow the scope (i.e., it can be argued that if the original requirement is satisfied, the interpretation would necessarily always be satisfied) of the requirements. Given that the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments uses the original version of this requirement from the CC v2.1, it was decided to use that version in this ST as well. Since the version of the requirement in this ST has a broader scope, any TOE meeting the requirement in this ST would meet the interpretations. The requirement stated in this ST is effectively a refinement of the version represented in the interpretations and is not an explicitly stated requirement.

## 8.6 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

## 8.7 Strength of Function (SOF) Rationale

The claimed SOF-medium level is primarily intended to be commensurate with the relative assurance afforded by EAL 4. Given that the TOE is intended to protect information as it passes through uncontrolled environments, SOF-basic is inadequate, however going beyond SOF-medium would seem to demand an assurance level beyond EAL 4, essentially the highest commercially available security. Hence, SOF-medium was selected. However, as indicated below, this claim is largely academic since all of the application mechanisms are entirely or primarily based on cryptography and procedural assumptions, which are outside the scope of a Common Criteria SOF analysis.

This security target includes a number of probabilistic or permutational functions. The list of relevant security functions and security functional requirements includes:

- User Data Protection/Cryptographic Support
    - FCS_COP.1(a) – Data Encryption
    - FCS_COP.1(b) - Hashing
    - FCS_COP.1(c) – Key Exchange
- User Data Protection/Association Security Policy
    - FDP_IFF.1(a) – Association Security Policy (encryption aspect)
- Identification and Authentication
    - FIA_UAU.2 – Authentication of administrators and users
- Protection of the TSF
    - FPT_SEP.1 – Protection of TSF data outside control of the TOE

Of these requirements, all but FIA_UAU.2 are immediately outside the scope of SOF analysis since they are entirely based on cryptography (see Section 6.1). The strength of the functions claimed to satisfy the corresponding security functional requirements are based on a FIPS 140-1 evaluation of those functions.

There are two distinct authentication mechanisms associated with FIA_UAU.2: one for administrators and another for users.

The authentication mechanism for administrators is a password of 1 to 24 characters in length where the allowable alphabet consists of 63 distinct characters. The administrator guide warns to change default passwords, change the password at least every 6 months, avoid using passwords including information relevant to the administrator, avoid using single words, and do not share or write down passwords. However in the worst-case scenario, the password space is 63 possible passwords. That means an attacker using random guesses would likely guess the password in 63/2, or 32 attempts. However, the administrator must ensure that the administrator console (NSC) is physically restricted so access is limited to authorized administrators. This means an attacker has no potential to make random guesses. Given the attacker has no potential to attack the password mechanism, the SOF-level is high and the claimed SOF-medium level is satisfied.

The authentication mechanism for users is primarily a cryptographic Authentication card that must be inserted into the card reader of a Network Security Device (NSD). Given this cryptographic nature, strength of function is not directly applicable. However, in order to mitigate the risk that a user might lose their card, an administrator can configure NSDs to require that a PIN be entered in addition to the Authentication card. The PIN can be 4 to 17 numbers normally, and with the use of a keyboard attached to the card reader the PIN can be 4 to 17 alphanumeric characters. Also, by default, a user will be disabled after 3 failed logon attempts, until reset by an administrator. The PIN is considered optional and therefore not necessary to satisfy the SOF requirement, which is satisfied by the Authentication card alone.

## 8.8 PP Claims Rationale

There is no claimed PP conformance.