National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Cryptek, Inc. • Sterling, VA

Diamond *TEK*™ 2.4

Report Number: CCEVS-VR-05-0139
Dated: 30 December 2005
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Mr. Daniel P. Faigin
The Aerospace Corporation
El Segundo, California

The Validation Team also thanks Ms. Kathleen Cunningham, *Department of Defense*, for the work she performed when she was Lead Validator, and Mr. Kenneth Elliott for his work as Senior Validator.

Common Criteria Testing Laboratory

Ms. Cynthia Reese, Lead Evaluator
Mr. Tony Apted
Ms. Shukrat Abbas
Ms. Colleen Glass
Science Applications International Corporation
Columbia, Maryland

Much of the material in this report was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report were extracted from the Cryptek Diamond*TEK* 2.4 Security Target.

Table of Contents

1 Executive Summary 1
2 Identification 4
3 Security Policy 6
3.1 User Data Protection 6
3.1.1 Association Security Policy 6
3.1.2 Mandatory Security Policy 7
3.1.3 Packet Filter Policy 9
3.2 Identification and Authentication 10
3.3 Security Audit 11
3.4 Security Management 11
3.5 Protection of the TOE Security Functions 11
4 Assumptions 13
4.1 Usage Assumptions 13
4.2 Environmental Assumptions 13
4.3 Clarification of Scope 13
4.3.1 Overarching Policies 13
4.3.2 Threats Countered and Not Countered 14
5 Architectural Information 15
5.1 TOE Components 15
5.2 TOE Boundaries 16
5.3 Architecture 18
5.3.1 NSC Subsystem 19
5.3.2 NSD Subsystem 19
5.4 IT Security Environment 21
6 Documentation 21
6.1 Design documentation 21
6.2 Guidance documentation 22
6.3 Configuration Management and Lifecycle documentation 22
6.4 Delivery and Operation documentation 22
6.5 Test documentation 22
6.6 Vulnerability Assessment documentation 23
6.7 Security Target 23
7 IT Product Testing 23
7.1 Developer Testing 23
7.2 Evaluation Team Independent Testing 24
7.3 Evaluation Team Penetration Testing 25
8 Evaluated Configuration 25
9 Results of the Evaluation 26
9.1 Evaluation of the Security Target (ASE) 26
9.2 Evaluation of the Configuration Management Capabilities (ACM) 27
9.3 Evaluation of the Delivery and Operation Documents (ADO) 27
9.4 Evaluation of the Development (ADV) 27

9.5 Evaluation of the Guidance Documents (AGD) 28
9.6 Evaluation of the Life Cycle Support Activities (ALC) 28
9.7 Evaluation of the Test Documentation and the Test Activity (ATE) 28
9.8 Vulnerability Assessment Activity (AVA) 29
9.9 Summary of Evaluation Results 29
10 Validator Comments/Recommendations 29
11 Annexes 30
12 Security Target 30
13 Glossary 30
14 Bibliography 33

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cryptek Diamond*TEK* 2.4.[1] It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in December 2005. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Conformant and Part 3 Conformant**, and meets the assurance requirements of Evaluation Assurance Level (EAL) 4. All security functional requirements are derived from Part 2 of the Common Criteria.

Diamond*TEK* is an access control system that provides protection for enterprise data, applications, and networks by employing end-to-end security and access control at the data level to create a secure access path. It is composed of the following interoperable hardware appliances:

- **Diamond*Central.*** A centralized GUI security configuration and management station. This device consists of a Network Security Controller (NSC) integrated with a special Network Security Device (NSD) known as NSD-Prime (and associated driver).
- **Diamond*Link*.** A drop-in appliance for securing individual nodes.
- **Diamond*Pak*.** A multi-channel rack appliance for protecting servers.
- **Diamond*SAT.*** A drop-in network appliance with integrated network acceleration for securing groups of nodes connected via high-latency devices (e.g., satellites).
- **Diamond*UTC.*** A secure ultra-thin client desktop integrating a SunRay™ operating system[2] with a Diamond*TEK* network security device.
- **Diamond*VPN*.** A drop-in network appliance for securing groups of nodes.

Diamond*TEK* enforces a centrally defined security policy for the flow, encryption, and auditing of data packets transferred between nodes in a network. This policy provides for mandatory access control (i.e., data separation based on security labels), association access control (i.e., discretionary access control between hosts), and packet filtering.

[1] "Cryptek Diamond*TEK* 2.4" is a shorthand used for the complete product reference, which consists of the following components: Diamond*Central*, Diamond*Link*, Diamond*Pak*, Diamond*VPN*, Diamond*SAT*, and Diamond*UTC*. A complete list of components, with version numbers and part numbers, may be found in Table 2-1 (Page 5).

[2] This operating system is not covered by this evaluation.

Diamond*TEK* also provides auditing, identification, and authentication at both the network nodes and at the administrative interface.

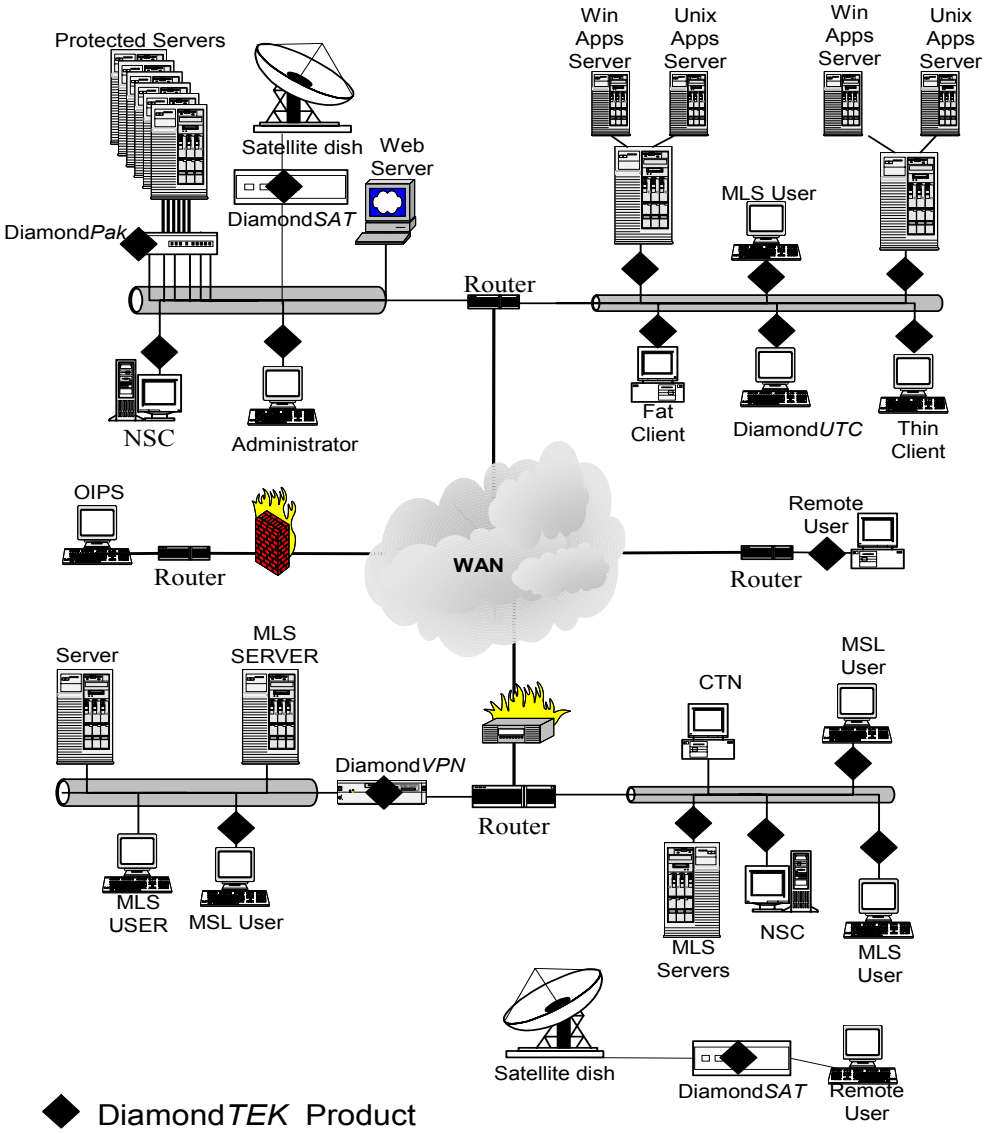

Figure 1-1. Diamond*TEK* Devices in a Network

Figure 1-1 illustrates the placement of Diamond*TEK* components in a network. In this figure, a "Node" is represented as a single computer, a collection of servers, and an entire network. The network security devices could be any of the supported variations, and would be selected to appropriately support the attached "Node." Note also that the

"Physical Network" need not be protected itself, as the NSDs can be configured to encrypt network traffic.

Each NSD 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; such NSDs are called No-Card Nodes. This option is used for fixed, permanent network entities (e.g., servers, sub-networks) where a user will be defined exclusively to represent the Node in the Diamond*TEK* system.

Note that while the Diamond*TEK* 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. 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.

This validation assumes the TOE has been configured as described in the following documents:

- Diamond*TEK*™ 10/100 Secure Network Administration, Version 2.4, May 12, 2005
- NSC/NSD Release Notes, Version 0.3, 27 July 2005
- Diamond*TEK*™ 10/100 Secure Network Commands Manual, Version 2.4, May 12, 2004
- CL100 User Pamphlet, Revision 1.0 May 12, 2005
- CP102/104/106 User Pamphlet, Revision 1.0 May 12, 2005
- CS101/102 User Pamphlet, Revision 1.0 May 12, 2005
- CV100 User Pamphlet, Revision 1.0 May 12, 2005
- CT100 User Pamphlet, Revision 1.0 May 12 2005
- Diamond*TEK*™ 10/100 Quick Start Guide Version 2.4, May 12, 2005

Note that, for the Diamond*Central* and Diamond*UTC* products, the TOE is a subset of the appropriately configured product, since the product includes hardware and software that falls outside the scope of the TOE, and hence has not been evaluated.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the

conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level 4 have been met.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC, the Cryptek Diamond*TEK* 2.4 Security Target, and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 2-1. Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	The Diamond*TEK* TOE consists of the following components: • **Diamond*Central*®** (also sold under the name CC200) *Part number:* DC1-C, DC2-C, DC3-C[3], CC200-C *NSC Application Software*: version 2.4.0.5 *NSD-Prime Firmware:* version 2.4.0.3 • **Diamond*Link*™** (also sold under the name CL100) *Part number:* DL100-C, DL100F-C[4], CL100-C, CL100-Fiber *Firmware:* version 2.4.0.3 • **Diamond*Pak*™** (also sold under the names CP102, CP104, CP106) *Part number:* DP200-C, DP400-C, DP600-C[5], CP102-C, CP104-C, CP106-C *Firmware:* version 2.4.0.3 • **Diamond*VPN*™** (also sold under the name CV100) *Part number:* DV100-C, CV100-C *Firmware:* version 2.4.0.3 • **Diamond*SAT*™** (also sold under the names CS101, CS102) *Part number:* DS100-C, DS200-C, CS101, CS102 *Firmware:* version 2.4.0.3 • **Diamond*UTC*™** (also sold under the name CT100) *Part number:* DU100-C, CT100-C *Firmware:* version 2.4.0.3 The Diamond*TEK* TOE also consists of the following Guidance Documents: • Diamond*TEK*™ 10/100 Secure Network Administration, Version 2.4, May 12, 2005 • NSC/NSD Release Notes, Version 0.3, 27 July 2005 • Diamond*TEK*™ 10/100 Secure Network Commands Manual, Version 2.4, May 12, 2004 • CL100 User Pamphlet , Revision 1.0 May 12, 2005 • CP102/104/106 User Pamphlet, Revision 1.0 May 12, 2005 • CS101/102 User Pamphlet, Revision 1.0 May 12, 2005 • CV100 User Pamphlet, Revision 1.0 May 12, 2005 • CT100 User Pamphlet, Revision 1.0 May 12 2005 • Diamond*TEK*™ 10/100 Quick Start Guide Version 2.4, May 12, 2005

[3] DC1-C supports 250 Diamond*TEK* nodes. DC2-C supports 1000 Diamond*TEK* nodes. DC3-C supports unlimited Diamon*dTEK* nodes.
[4] DL100-C/CL100-C supports RJ-45 copper network interface. DL100F-C/CL100-Fiber supports a fiber optic network interface.
[5] DP200-C/CP102-C supports two servers. DP400-C/CP104-C supports four servers. DP600-C/CP106-C supports six servers.

Item	Identifier
Protection Profile	The ST contains no claim of PP compliance
ST:	*Cryptek DiamondTEK 2.4 Security Target,* Version 2.0, 30 December 2005
Evaluation Technical Report	• *Final Evaluation Technical Report for the DiamondTEK™ Product (DiamondCentral®: NSC Application S/W version 2.4.0.5; NSD-Prime F/W version 2.4.0.3) and NSD (DiamondLink™, DiamondPak™, DiamondVPN™, DiamondSAT™, DiamondUTC™) F/W version 2.4.0.3, Part 1 (Non-Proprietary)*, Version 1.0, 30 December 2005 • *Final Evaluation Technical Report for the DiamondTEK™ Product (DiamondCentral®: NSC Application S/W version 2.4.0.5; NSD-Prime F/W version 2.4.0.3) and NSD (DiamondLink™, DiamondPak™, DiamondVPN™, DiamondSAT™, DiamondUTC™) F/W version 2.4.0.3, Part 1 (Proprietary)*, Version 1.0, 30 December 2005 • *Final Evaluation Technical Report for the DiamondTEK™ Product (DiamondCentral®: NSC Application S/W version 2.4.0.5; NSD-Prime F/W version 2.4.0.3) and NSD (DiamondLink™, DiamondPak™, DiamondVPN™, DiamondSAT™, DiamondUTC™) F/W version 2.4.0.3, Part 2 (Proprietary)*, Version 1.0, 30 December 2005
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.1
Conformance Result	CC Part 2 conformant, CC Part 3 conformant
Sponsor	Cryptek, Inc, Sterling VA, USA
Developer	Cryptek, Inc, Sterling VA, USA
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD, USA
CCEVS Validators	Daniel P. Faigin, The Aerospace Corporation, El Segundo, CA

3 Security Policy

The Security Functional Policies (SFPs) implemented by Diamond*TEK* 2.4 permit protection of user data, provide for authenticated user access, provide accountability for actions, and protect the mechanism that provides the security policies.

Note: Much of the description of the Diamond*TEK* 2.4 security policy has been extracted and reworked from the Diamond*TEK* 2.4 Security Target.

3.1 User Data Protection

Diamond*TEK* provides three distinct user data security polices: an Association Security Policy, a Mandatory Security Policy, and a Packet Filter Policy.

3.1.1 Association Security Policy

The Association Security Policy allows each Node to communicate exclusively with other authorized nodes based on an Association Profile. The Network Security Manager (NSM)

can explicitly define three types of associations in an Association Profile: NSD-to-NSD, NSD-to-OIPS, and NSD-to-CTN. Both the NSD-to-NSD and NSD-to-OIPS associations generally require that encryption is used when transferring information.

When a user logs[6] 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 that NSD's local association table. The association lookup can use either destination IP addresses or Ethernet addresses (on the local subnet). Each association lookup results in one of the following decisions: unavailable association (Association Security Policy failure), encrypted association (only encrypted packets are permitted), or clear text association. If the association is not permitted, the NSD sends an audit record to its 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 in a transitional state (i.e., while starting) it can be configured to allow Dynamic Host Configuration Protocol (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 not fully online; when the NSD goes fully online DHCP traffic is constrained by all of the information policy rules.

Additionally, a Network Security Manager can configure settings that apply to otherwise unidentified IT entities. This permits an administrator to restrict communication to only 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. This applies to all of the information flow policies.

3.1.2 Mandatory Security Policy

The Mandatory Security Policy allows a Node to communicate with another Node only when it has an appropriate security label[7] relationship with that Node. Each Node labels

[6] 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.

[7] There are 256 security levels and 65,535 security categories that can be used to construct a security label.

each packet (either explicitly or implicitly) that is placed on the network; 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, the packets are discarded and corresponding audit records are generated.

Within a Node's Operational Profile is a Security Profile that defines the 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. 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. 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, the Operational Profile selected by the user must satisfy the security constraints associated with the NSD.

It is the responsibility of the NSM to assign Security Profiles to NSDs and to assign Operational Profiles to users. 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 the window defined in the Security Profile assigned to the NSD.

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 Transmit Categories set includes one or more categories, or to 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 Receive Categories set includes one or more categories, or to 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.

Similarly to 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.

3.1.3 Packet Filter Policy

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.

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 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 not fully online, 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 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.

3.2 Identification and Authentication

Diamond*TEK* 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:

- NSMs are required to log in to the NSC application itself 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.
- NSD 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 the selected NSD is configured to require one]. For static network devices, the NSM may configure a NSD to be associated with a user representing the attached Host and to not require a card to be present to operate.[8] When such a user is created, it must be assigned exclusively to a single NSD.[9] Note that a user remains associated with a NSD after logging on until they log off 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.

The NSM defines users at the NSC. Each user has the following attributes:

- An Authentication Card (for authentication at a NSD) that contains identification and authentication information.[10]
- A set of Operational Profiles, each including an Association Profile and Security Profile.
- Security Violation Thresholds.

The NSM is defined by identity and authentication data managed by the NSC. In addition to logging into the NSC application, the NSM must also have physical and logical access to the host (IT environment) of the NSC.

[8] When such a device is configured, the assigned User is automatically logged on, with its default Operational Profile, whenever the device is reset.
[9] Effectively, the administrator has procedurally authenticated the user by explicitly and exclusively assigning the user to be used whenever the associated NSD is online.
[10] 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.

3.3 Security Audit

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

Each NSC audit record includes an audit type, date and type, identification of the current NSM, and audit data specific to the audit type. Each NSD audit record includes the audit type, a date and time (applied when the message is received at the NSC), the user at the NSD, and source and destination network addresses and ports (in most cases). Note that NSD audit records are transmitted across the network to the NSC to be recorded; hence, there is a small risk that the message will be lost in transit.

The NSC restricts unauthorized access to its database and hence the audit trail.[11] 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. It is formally assumed that only the NSM has physical access to the NSC and its IT environment and that all network connections must pass through the TOE; this ensures that the NSM can only access the audit trail using the NSC commands. Access through the TOE is protected by the NSC application requiring users to logon before offering the capability to access the audit trail and the NSC preventing 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 NSC also provides the ability for 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. The review tools offer dialogs where the administrator can search and sort the audit log based on any combination of the user identity, type of audited event, date and time, and other characteristics specific to the whether the event was generated on the NSC or a NSD.

3.4 Security Management

All Diamond*TEK* 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 Diamond*TEK* system.

3.5 Protection of the TOE Security Functions

Much of the protection of the TOE Security Functions is provided through the usage assumptions about the product. These assume that access to the NSC is appropriately restricted, that the developer packages the NSC with an appropriate IT environment, and

[11] A key assumption for this product is that the Network Security Controller has physical access restricted to authorized administrators. The TOE is packaged by the developer with an operating system (separately evaluated) that provides access controls, but said access controls are not depended upon for protection.

that NSDs remain appropriately connected to the hosts they are intended to protect. There is also the assumption that the network is constructed such that all Hosts requiring protection are connected to the network only through their NSDs. This ensures that the only logical points of entry to the Diamond*TEK* system are the host-to-NSD interfaces and network-to-NSD interfaces.

However, the TOE does make contributions to help protect itself. Consider the NSC, which is 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. The NSD-Prime (as well as the NSDs that connect other Hosts) serves to protect the TSF by limiting and controlling the functions that they offer to the uncontrolled network environment.

NSDs are self-contained devices that ensure that any communication between their host-side and network-side interfaces is subject to the appropriate mediation. While it might be possible to remove an NSD, the non-bypassability of the information flow policies is based on appropriately connected nodes. In the case of the NSC, physical protection limits access to the console to authorized administrators, but those administrators are still required to logon to the TSF before accessing its functions. Furthermore, the NSD-Prime serves to logically isolate the NSC by ensuring that the NSC can only communicate with its associated NSDs for the purposes of configuration and reporting.

In a Cryptek Diamond*TEK* system, TSF data is passed across the network while the TOE is operational. This means that the network must either be physically-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 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.

When any NSD interacts with the NSD-Prime, the Association Security Policy mechanism is used to protect the applicable TSF information. However, all traffic to and from the NSD-Prime implicitly (as opposed to an explicit policy setting) must always be encrypted via that mechanism to ensure its secrecy and integrity.

4 Assumptions

The following assumptions underlie the evaluation of Cryptek Diamond*TEK* 2.4:

4.1 Usage Assumptions

First and foremost, it is assumed that all users will follow the written guidance they are provided. This applies to both users at NSDs, as well as the NSM at the NSC. This includes providing physical protection to any access cards, as well as not attempting to bypass the TOE via the IT environment.

It is also assumed that administrators, who do have privileged access to the NSC, are non-hostile.

4.2 Environmental Assumptions

A key environmental assumption is physical security. It is assumed that NSDs remain attached to their associated Hosts, and that only authorized administrators can access the management console. The latter restriction obviates the need for the TOE to depend upon any security features that may (or may not) be provided by the non-TOE portions of the Diamond*Central* product. Additional protections may be offered by hardware and software underlying the NSC, but such protections are not relied upon by the TOE, nor are they covered by this validation.

A second environmental assumption is that information cannot flow between the internal and external networks/hosts unless it passes through the TOE. In this assumption, the notion of an internal network/hosts represents a Host or network protected by a NSD and the notion of an external network represents the network to which a given NSD is attached.

A third environment assumption concerns the packaging of the Diamond*Central* product. Specifically, it is assumed that the developer packages the NSC software with an IT environment that will be suitable to support the correct operation of the TOE. Said environment is one that will not negatively affect the security functions of the TOE. Specifically, this environment must be capable of provide an execution environment for the NSC software, some network connectivity, the ability to reliably store and retrieve information, to facilitate a human user interface, and to provide a reliable time stamp. The hosting operating system (including any non-TOE software running on the operating system) is one that is security neutral and will not intentionally or unintentionally subvert any of the claimed TOE security functions.

4.3 Clarification of Scope

4.3.1 Overarching Policies

The security requirements enforced by the TOE were designed based on the following overarching security policies:

1. The TOE must limit access to information based on sensitivity of information and the clearance of subjects. The rules being enforced have to be able to 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.

2. The TOE must ensure that information can only flow between nodes as explicitly allowed by an Administrator. Each allowable communication path must be explicitly defined by an authorized administrator, and 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 with which it is configured.
3. 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.

The ST classifies these are "Organizational Security Policies"; however, they are not policies imposed by the organization actually operating the TOE. Rather, they are policies that the developer assumed to be in place at operating organizations.

4.3.2 Threats Countered and Not Countered

The TOE is designed to fully or partially counter the following threats:

- That 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.
- That an unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
- That an unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.
- That an unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
- That 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.
- That persons might not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
- That an unauthorized person may read, modify, or destroy security critical TOE configuration data.

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

However, users of the TOE should be cautioned that:

- The TOE *does not* counter the threat of loss of audit records during transmission from an NSD to the NSC.
- The TOE *does not* counter the threats of delays in network transmission resulting in incorrect timestamps on audit records received from an NSD. The latter may increase the difficulty of correlation of audit records.
- The TOE *does not* counter the insider threat; i.e., the threat of malicious authorized users disobeying written guidance to disable or bypass TOE protections.
- The TOE *does not* counter the threats of attacks on the authentication cards; i.e., that such cards may be reverse-engineered or modified.
- The TOE *does not* counter the threat of malicious smart card reader used to read the cards used for the Diamond*UTC* product at the Network Security Controller.

Some, but not all, of the above uncountered threats are addressed somewhat through usage assumptions.

5 Architectural Information

Note: The following architectural description is based on the description presented in Part I Evaluation Technical Report for the DiamondTEK 2.4 TOE and in the DiamondTEK 2.4 Security Target.

5.1 TOE Components

As shown in Figure 1-1 (Page 2), Diamond*TEK* consists of a number of components:

- **Network Security Devices.** Each protected entity is connected to the physical network via a NSD. For a single Host, the NSD is a Diamond*Link* that is installed between any NIC and a physical network or the Host. The Diamond*Link* could be replaced by a Diamond*UTC* (a product combining a commodity host with a DiamondTEK device).

  When dealing with multiple nodes (e.g., a sub-network or group of servers), the NSD may be either a Diamond*VPN* or (when the environment is high-latency) a Diamond*SAT* – these are installed as a single point of control for all of the nodes (collectively referred to as a Host) that may be attached to them. Alternately, the NSD may be a rack-mounted Diamond*Pak* that serves to protect a set of collocated Hosts (e.g., servers) each with its own Operational Profile. Lastly, the NSD may be

one of two Diamond*SAT* models: (1) the DSAT-100[12], which is essentially a high-latency-capable Diamond*VPN* device, or (2) the DSAT-200, which includes an additional dedicated Diamond*VPN* device so that it can encrypt traffic on both its extra- and intra-network connections (meaning it has two distinct NSDs).

- **Integrated Card Reader.** Each NSD 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.
- **Network Security Controller.** 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 (referred to as an 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.

Note that while a Diamond*TEK* 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.

5.2 TOE Boundaries

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 Server or Window 2003 Server operating system (with SQL Server installed) and can offer any support that the operating platform can provide (e.g., removable media, printer). The developer packages Windows 2000 Server or Windows 2003 Server (with SQL Server installed), together with appropriate hardware, as part of the product; however, these components are considered to be part of the IT environment.

The NSC application communicates with associated NSDs via its own special NSD (and associated driver), known as NSD-Prime. The NSC application also utilizes a card reader/writer device (and associated driver) in order to create User Authentication cards and NSD Installation cards. This device and the associated driver are considered to be part of the TSF. Note that when a Diamond*TEK* system includes Diamond*UTC* appliances, the NSC requires an additional smart card reader that will support reading additional types of cards (i.e., Galatic, Oberthur Cosmopolic, Open Platform, Java Bridge, Schlumberger Cyberflex® Access32 and Access64, and Schlumberger Test CAC Cards). This additional

[12] DSAT-100 and DSAT-200 are also sold under the product names CS101 and CS102.

smart card reader (and its driver) is accessed via Windows 2000 Server or Window 2003 Server services and is part of the IT environment.

The NSDs come in five basic types: Diamond*Link*, Diamond*VPN,* Diamond*SAT,* Diamond*UTC,* and Diamond*Pak*.

- **Diamond*Link***. For this type of device, the physical interfaces are a standard network connection to a NIC installed on the associated Host and the connection to the physical network. An integrated 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.
- **Diamond*UTC***. For this type of device, the physical interfaces are a standard network connection to a NIC integrated in the Sun Microsystems' Sun Ray™ Host and the connection to the physical network.[13] The integrated Diamond*TEK* NSD is actually a Diamond*Link*; as such, it has an integrated card reader.
- **Diamond*VPN*** and **Diamond*SAT***. For these types of devices, the physical interfaces include two networks – one over which Diamond*TEK* controls 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. These devices have an integrated card reader, but this reader is used solely for installation.
- **Diamond*Pak***. For this type of device, 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. This device has an integrated card reader, but the reader is used solely for installation.

The TOE Boundaries are illustrated in Figure 5-1 (Page 18). In this figure, the shaded boxes show the components that constitute the TSF, with the heavier lines illustrating TOE boundaries.

[13] Note that the Sun Ray Host and integrated NIC are outside the scope of the TOE though they are considered part of the product. The TOE, in this configuration, is the Diamond*TEK* device between the Sun Ray Host NIC and the connected network.

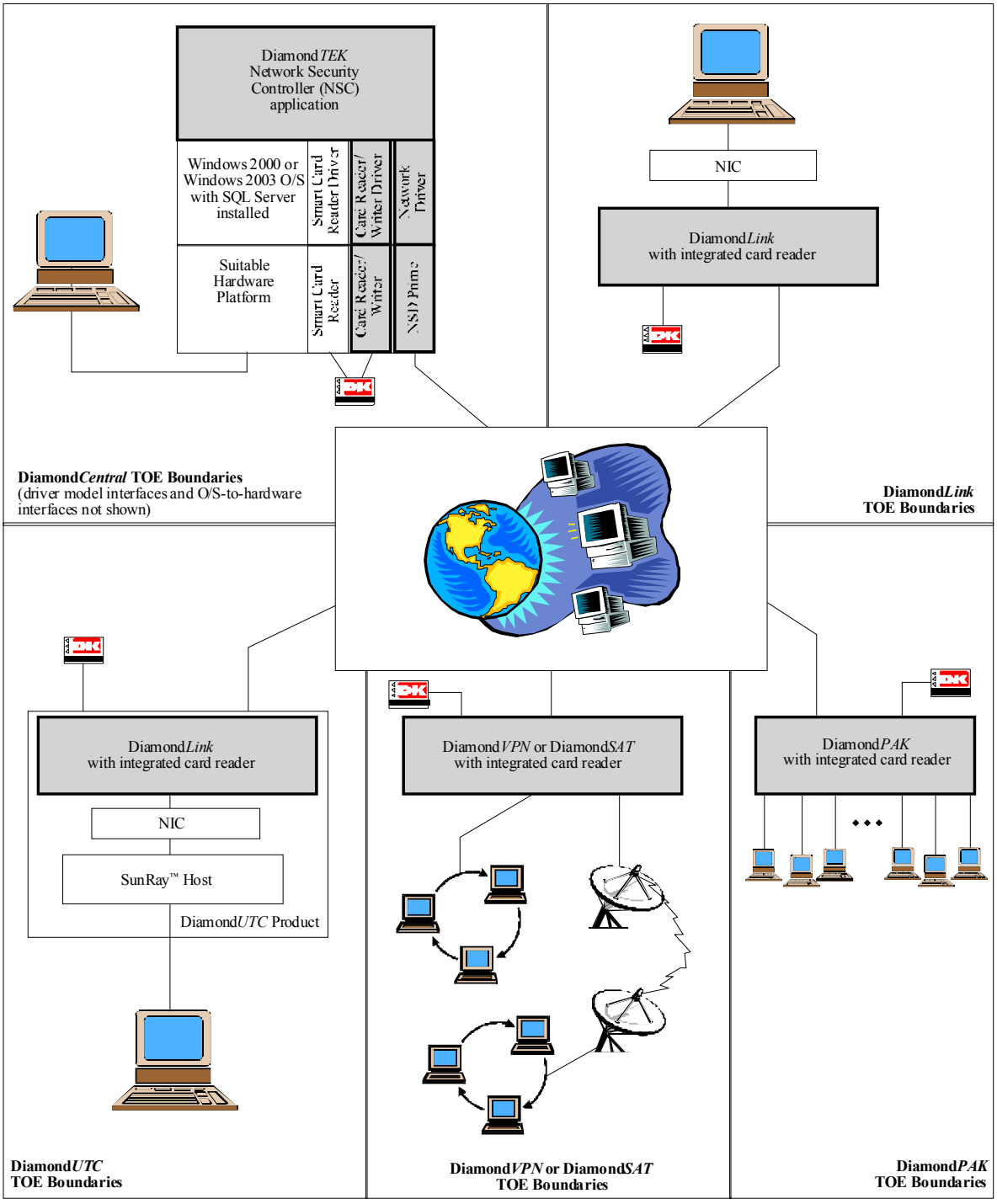

Figure 5-1. TOE Boundaries in the Diamond*TEK* 2.4 Product

5.3 Architecture

Architecturally, Cryptek Diamond*TEK* TOE consists of two subsystems: the Network Security Controller (NSC) subsystem and the Network Security Device (NSD) subsystem.

Each Diamond*TEK* system includes a single NSC subsystem and any number of instances of NSD subsystems, all connected to each other via a network. While NSDs are designed to communicate with each other as well as other designated network nodes, the NSC can only communicate with NSDs that are under its control. This restriction of interface between the NSC and its associated NSDs is enforced by the NSD-prime included in the NSC and is accomplished by rejecting any traffic not originating from a known NSD, sending traffic only to known NSDs, and by requiring that all such communication be transmitted using IPsec to ensure both integrity and privacy.

5.3.1 NSC Subsystem

The NSC subsystem consists of an application, an NSD-prime device, a card reader/writer device, and driver to allow the application to communicate with the devices – all developed by Cryptek. These components are designed to be installed in a Windows workstation. The application stores data in files managed by Windows, it stores audit records in a SQL Server database on Windows, communicates with NSDs through an attached NSD-prime, and generates User Authentication and NSD Installation cards through an attached card reader/writer device. The NSD-prime is a NSD configured such that it will communicate only with other known NSDs. The Windows platform is required to provide an operational application environment including process management, data storage (files and memory), and console input and output. The Windows platform is also required to provide the reliable time stamp to the NSC. The developer packages the NSC with an appropriate Windows version.

The NSC application maintains numerous information tables that define the various network nodes, policies, users, administrators (i.e., NSMs), etc. The administrator Graphic User Interface (GUI) commands is generally designed to provide access to manage these tables (as well as their associations with each other) and other aspects of the Diamond*TEK* system (e.g., suspending and continuing network operations).

The NSC configuration tables defines the policy at each NSD including what nodes the NSD is allowed to communicate with and the maximum security level and the minimum security level of information that is allowed to flow through the NSD. The NSC configuration tables also define the audit thresholds for each NSD.

In addition to the NSC configuration tables, the NSC also maintains a set of state information. Among this information, the NSC keeps track of whether each User and NSD is online, offline, or otherwise suspended.

5.3.2 NSD Subsystem

Each NSD is connected to the network, but is also connected to a host (e.g., computer or network) that it is configured to protect. A NSD can be connected to a host either using standard network traffic via a network connection to a NIC already present in the host, or the NSD can be installed in the host, via a PCI bus, in place of a NIC card. In addition to the NSD-host interface and NSD-network interface, each NSD includes a user interface in

the form of a card reader. The former two interface types are used to control the flow of information between a host and the network, while the latter interface is used to either install a new NSD or to allow a user to log into the NSD so that it will begin to allow information to flow under its control. Each NSD is designed specifically to control the flow of information between its attached host and network. Note that the Diamond*UTC* is packaged with its host (a Sun Ray™ system), where the host NIC is wired directly to the NSD.

The NSD subsystem consists of the NSD device that has distinct host and network interfaces and a card reader. The ability for the NSD to communicate with NSD-Prime (or the NSC) has been described earlier. This section will describe details of the Card Reader and the NSD device as it relates to both the host and network. The host and network interfaces of the NSD subsystem are based on standard protocols.

The NSD primarily inspects network traffic as it passes through in order to enforce access control policies. Except when traffic is rejected, the NSD is designed to be transparent to both the host and the network. In performing its functions, the NSD does not modify the data included in network traffic, except in the case of performing cryptographic transformations (and even then the operation is transparent to the host). Traffic headers might also be modified, though not for security reasons (other than IPsec headers), but rather to facilitate proper routing and non-IP encapsulation.

The operation of the NSD network and host interfaces is dependent upon the state of the NSD. The NSD can be offline, online, or suspended. The primary difference between being suspended and offline is that a suspended NSD can resume operation (when so commanded by the NSC), whereas an offline NSD requires a user to subsequently be authenticated prior to going back online. Another difference is that an offline NSD generally does not have a link with the network (in other words, the network link is turned off). A suspended NSD, however, still has a network link and can receive a resume command from the NSC. While both offline and suspended NSDs will not generally allow network traffic to pass through, an online NSD is fully functional, within the parameters of its operational profile.

The NSD sends audit records to the NSC when its state changes, when policy violations are detected, and for other network activity based on selectable audit event types (i.e., statistical, broadcast, and TCP connections). The NSD does not include the date or time; the NSC adds this information when each audit record is received. The NSD enforces the audit selection provided by the NSC by only auditing the selectable audit events indicated by the NSC. The NSD does not have the ability to protect audit data from loss in transit.

The NSD requires that a user be identified and authenticated before going online and allowing traffic to flow through the device in accordance with the information flow policies. If a NSD is configured to not require a User Authentication card, it will come online automatically after a power-cycle as the user that the NSM assigned to that NSD. If a NSD is configured to require a User Authentication card, an appropriate card must be inserted and (if required) the user must provide the correct PIN. If the information is valid,

the NSD will come online with the user identified on the User Authentication card and subsequent operations will be accountable to that User. The user logs off by simply removing the User Authentication card.

5.4 IT Security Environment

The Cryptek Diamond*TEK* TOE requires an IT environment suitable to support the operation of the NSC. Specifically, the NSC application is designed to operate on a Windows operating system (with SQL Server installed). The NSC application relies on Windows to instantiate itself as a process, to manage memory, to manage files, to access time and date information, store audit records, and to provide access to various input/output devices – keyboard, mouse, and display. In addition, the NSC application relies on the Windows driver model, which has been used to create the driver that allows the NSC application to communicate with the NSD-prime. The developer ensures that a suitable environment is available by how it packages the Diamond*Central* product.

With regard to physical interfaces, the NSD-prime requires that the hardware hosting the Windows operating system provide a suitable PCI bus for installation of the NSD-prime card. The NSC card reader/writer is connected to the NSD-prime card and does not otherwise have an IT environment interface. Note the Diamond*UTC* comes packaged with a host (specifically a Sun Microsystems' Sun Ray™) providing an integrated secure ultra-thin client desktop. The Diamond*UTC* host is not part of the TOE while part of the product.

Of all of these dependencies, the only dependencies that are directly related to security functions are the Windows provisions of time and date information.

6 Documentation

The following documentation was used as evidence for the evaluation of the Diamond*TEK* 2.4:[14]

6.1 Design documentation

Document	Revision	Date
DiamondTEK Functional Specification	1.4	2005-09-30
DiamondTEK High-level Design Specification	1.3	2005-09-30
DiamondTEK Low-level Design Specification	1.1	2005-05-17
Network Security Center (NSC) Software Specification Cryptek Secure Network	10.3	2005-07-19
10/100 NSD System Design Document	2.2.1	2005-10-03
DiamondTEK Security Policy Model	1.0	2004-02-23
Source code subset	2.4.0.5 – NSC 2.4.0.3 – NSD	(none provided)

[14] This documentation list is based on the list provided in the Evaluation Technical Report, Part 1, developed by SAIC.

6.2 Guidance documentation

Document	Revision	Date
DiamondTEK™ 10/100 Secure Network Administration	2.4	2005-05-12
NSC/NSD Release Notes	0.3	2005-07-27
DiamondTEK™ 10/100 Secure Network Commands Manual	2.4	2005-04-29
CL100 User Pamphlet	1.0	2005-05-12
CP102/104/106 User Pamphlet	1.0	2005-05-12
CS101/102 User Pamphlet	1.0	2005-05-12
CV100 User Pamphlet	1.0	2005-05-12
CT100 User Pamphlet	1.0	2005-05-12
Diamond*TEK*™ 10/100 Quick Start Guide	2.4	2005-05-12

6.3 Configuration Management and Lifecycle documentation

Document	Revision	Date
DiamondTEK Configuration Management Plan	1.5	2005-12-30
DiamondTEK Life Cycle Management Plan	1.1	2004-08-27

6.4 Delivery and Operation documentation

Document	Revision	Date
Cryptek Delivery and Operation Procedures	1.1	2004-08-27

6.5 Test documentation

Document	Revision	Date
DiamondTEK High-level Design Specification, Appendix A: Test Case Descriptions (Spreadsheet)	3.0.0	2005-04-18
NSC Functional Specification & High-Level Design Test Plan NSC 2.4. 5[15]	3.0.1	2005-07-22
NSD Functional Specification & High-Level Design Test Plan Part NSD 2.4. 3 [16]	3.0.2	2005-09-03
Test Equipment Settings Functional Specification & High-Level Design Test Plan	3.0.1	2005-06
Test Cases NSC 2.4. 5 & 2.4. 3[17]	3.0.0	2005-04

[15] This document has a typo in the title, and really refers to NSC version 2.4.0.5. The vendor has been informed of this typo.
[16] This document has a typo in the title, and really refers to NSD version 2.4.0.3. The vendor has been informed of this typo.
[17] This document has a typo in the title, and really refers to NSC version 2.4.0.5 and NSD version 2.4.0.3. The vendor has been informed of this typo.

6.6 Vulnerability Assessment documentation

Document	Revision	Date
DiamondTEK Misuse Analysis	1.1	2004-04-20
DiamondTEK Vulnerability Analysis	1.0	2004-04-30

6.7 Security Target

Document	Revision	Date
DiamondTEK 2.4 Security Target	2.0	2005-12-30

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Plan, contained in Part II of the ETR, and has been reviewed to ensure it does not contain vendor proprietary information.

7.1 Developer Testing

Evaluator analysis of the developer's test plans, test scripts, and test results indicated that the developer's testing is adequate to satisfy the requirements of EAL4.

The developer's tests were completely manual. The developer's test approach consists of two parts. Each part is designed to address each of the two major subsystems of a DiamondTEK system.

Part I includes tests for the NSC subsystem and Part II includes tests for the NSD subsystem (and interaction between the NSC and NSD). As such, Part I is primarily directed at testing the security-relevant operation of all of the available Security Management functions and the audit of the use of those functions.

Part II is primarily directed at testing the security functions available through the NSD interfaces. These functions are primarily the User Data Protection, TSF Protection, and Identification and Authentication functions. Additionally, the internal interfaces are tested via their associated external interfaces.

The functions tested in both parts include all of the information flow policies (Mandatory, Association, and Packet Filtering), the Security Management, identification and authentication, TOE self-protection, as well as audit events generated by the NSD. Both parts of the test plan are organized to directly correspond with the test cases described in the Diamond*TEK* Functional Specification and High-level Design documentation.

The evaluation team verified that the test coverage was suitable through analysis of the developer-provided test coverage argument. This argument mapped test cases to interfaces and components of the high-level design.

For each of the developer tests, the evaluators analyzed the test procedures to determine whether the procedures were relevant to, and sufficient for the function being tested. They also verified that the test documentation showed results that were consistent with the expected results for each test script.

7.2 Evaluation Team Independent Testing

In addition to developer testing, the CCTL conducted its own suite of tests. Tests were conducted on a configuration that included a Diamond*Central* NSC and an instance of each type of Diamond*TEK* NSD (Link, UTC, PAK, SAT, and VPN). The CCTL verified that each of these components was running the TOE version of the firmware and the software.

The CCTL installed the TOE and configured it in accordance with the provided guidance. The NSC was installed in accordance with Chapters 4 through 6 of *DiamondTEK 10/100 Secure Network Administration*. During installation, the following options were selected:

- Keep Alive Mode
- Overwrite the Audit Log when full

The NSD was installed in accordance with the *DiamondTEK 10/100 User Pamphlet*, the *DiamondTEK UTC User Pamphlet*, and the *DiamondTEK 10/ 100 Secure Network User's Pamphlet*.

During its testing, the evaluation team reran a portion of the vendor test suite. The evaluation team determined which vendor tests to include in the sample set based on coverage of security functions and coverage of subsystems. The subset of tests demonstrated the functionality of each TOE subsystem (NSD and NSC). The test subset also tested each type of external interface. Overall, 21.6 % of test suite was rerun. The team verified that all the selected tests passed, or a justification was provided as to why that test was not required to pass in the evaluated configuration.

The evaluation team also developed nine (9) independent tests. The team tests developed were primarily based upon the evaluation team's analysis of the design documentation, user guidance, security target, and test documentation. Focus was placed upon areas where the developer test documentation did not cover completely. The validator reviewed theses independent tests and felt that they provided sufficient supplemental coverage to the vendor tests. The evaluation team used the exact configuration (including the policy settings) documented in the vendor test documentation and used to perform the vendor test subset was used to perform the team test. The evaluation team also used the same test tools such as the packet generators and sniffers documented in the vendor test documentation and used to perform the vendor test subset.

These tests identified some discrepancies between the actual implementation and the implementation documented in the ST. The ST was updated to reflect the actual implementation, as the evaluation team felt that the test failures did not introduce a security risk.

7.3 Evaluation Team Penetration Testing

The CCTL also conducted penetration testing, using the same setup used for the independent team tests.

Prior to developing its tests, the CCTL followed well-established penetration test development procedures. This effort considered design documentation evaluation, guidance documentation evaluation, test documentation evaluation, code review, vulnerability analysis evaluation. It was revisited subsequent to the running of a portion of the vendor test subset. Therefore, it took advantage of TOE knowledge gained from each of these activities.

This resulted in a set of seven (7) penetration tests. The validator reviewed these tests, and felt that they adequately explored areas of potential vulnerability. Execution of these tests resulted in some documentation clarifications, but identified no security vulnerabilities.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, consists of the following components configured in accordance with the Guidance Documentation in the TOE:

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

- **Diamond*Central*®** (also sold under the name CC200).
  Part number: DC1-C, DC2-C, DC3-C[18], CC200-C.
  NSC Application Software: version 2.4.0.5
  NSD-Prime Firmware: version 2.4.0.3
- **Diamond*Link*™** (also sold under the name CL100)
  Part number: DL100-C, DL100F-C[19], CL100-C, CL100-Fiber
  Firmware: version 2.4.0.3
- **Diamond*Pak*™** (also sold under the name CP102, CP104, CP106)
  Part number: DP200-C, DP400-C, DP600-C[20], CP102-C CP104-C, CP106-C
  Firmware: version 2.4.0.3
- **Diamond*VPN*™** (also sold under the name CV100)
  Part number: DV100-C, CV100-C
  Firmware: version 2.4.0.3
- **Diamond*SAT*™** (also sold under the name CS101, CS102)
  Part number: DS100-C, DS200-C, CS101, CS102
  Firmware: version 2.4.0.3

[18] DC1-C supports 250 Diamond*TEK* nodes. DC2-C supports 1000 Diamond*TEK* nodes. DC3-C supports unlimited Diamond*TEK* nodes.
[19] DL100-C/CL100-C supports RJ-45 copper network interface. DL100F-C/CL100-Fiber supports a fiber optic network interface.
[20] DP200-C/CP102-C supports two servers. DP400-C/CP104-C supports four servers. DP600-C/CP106-C supports six servers.

- **Diamond*UTC*™** (also sold under the name CT100)
  Part number: DU100-C, CT100-C
  Firmware: version 2.4.0.3

9 Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 2.1, dated August 1999 [1,2,3,4]; the Common Evaluation Methodology (CEM), Version 1.0, dated August 1999 [6]; and all applicable International Interpretations in effect on 18 February 2004. The evaluation confirmed that the Cryptek Diamond*TEK* 2.4 product (specifically, *DiamondCentral®: NSC Application S/W version 2.4.0.5; NSD-Prime F/W version 2.4.0.3) and NSD (DiamondLink™, DiamondPak™, DiamondVPN™, DiamondSAT™, DiamondUTC™) F/W version 2.4.0.3)* is compliant with the Common Criteria Version 2.1, functional requirements (Part 2) and assurance requirements (Part 3) for EAL4. The details of the evaluation are recorded in the CCTL's evaluation technical report, *Final Evaluation Technical Report for the DiamondTEK™ Product (DiamondCentral®: NSC Application S/W version 2.4.0.5; NSD-Prime F/W version 2.4.0.3) and NSD (DiamondLink™, DiamondPak™, DiamondVPN™, DiamondSAT™, DiamondUTC™) F/W version 2.4.0.3*, Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the Cryptek Diamond*TEK* 2.4 Security Target v2.0, 30 December 2005.

The validator followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The validator has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validator therefore concludes that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Diamond*TEK* product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 4 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation. To support the ACM evaluation, the evaluation team received Configuration Management (CM) records from Cryptek and performed a CM audit.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 4 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer. The evaluation team followed the Configuration Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 4 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification, a high-level design document, a low-level design document, and a security policy model. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

Additionally, the evaluation team ensured that the security policy model document clearly describes the security policy rules that were found to be consistent with the design documentation.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was

conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 4 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 4 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The evaluation team ensured the procedures described the life-cycle model and tools used to develop and maintain the TOE. To support the ALC evaluation, the evaluation team performed an audit of the security measures at Cryptek.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.8 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 4 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.9 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

- This validation hinges a large percentage of its TOE protection argument on the physical protection and access restrictions for TOE components. It is assumed that only authorized Network Security Managers will have access to the Diamond*Central* components, and will use the underlying Windows operating system in an authorized manner, installing no additional applications and following other guidance provided. Users of this product need to ensure that all the assumptions about the environment of use are met.
- The ST defines a single role, Network Security Manager, for simplicity of presentation. In reality, there are some reduced privilege roles available that are NSM-subsets: operator and crypto-operator. Although this is compliant with the CC, users should be aware of these additional roles as they may affect staffing loads.
- Audit records generated at the Network Security Devices are not time-stamped at the time of generation, but at the time they are received at the Network Security Console. Given that network delays in transmission are possible, this may increase the difficulty of correlation of the event with the actual action.

  Additionally, records from the NSDs are transmitted across the network to the NSC, introducing the risk that they might not be received at all, due to network problems.

- This validation assumes that users will follow guidance and protect their authentication cards, and not attempt to reverse engineer the information on those cards. Given that these cards are critical for authentication purposes, users should be provided education to emphasize their need to protect the cards.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *Cryptek DiamondTEK 2.4 Security Target,* Version 2.0, 30 December 2005.

13 Glossary

The following definitions are used throughout this document:

- **Association Profile**. The profile associated with each user[21] 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.
- **Authentication.** Verification of the identity of a user.
- **Clear Text Node (CTN)**. A node that does not require encryption in order to send or receive information.
- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Common IP Security Option (CIPSO)**. FIPS 188
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Diamond*Central***. The network entity used by the NSM to manage the Diamond*TEK* system. Note: The product is also sold under the name CC200.
- **Diamond*Link***. One type of NSD used to protect and control a single Host that already has an installed NIC. Note: This product is also sold under the name CL100.

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

- **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. Note: This product is also sold under the names CP102, CP104, and CP106.
- **Diamond*SAT*.** One type of NSD used to combine the functions of a Diamond*VPN* with built-in network acceleration to support VPN tunnels in high latency environments (e.g., across satellites). Note: This product is also sold under the names CS101, and CS102.
- **Diamond*TEK***. The TOE; a collection of network Nodes (i.e., NSDs attached to Hosts) and a Diamond*Central* (CC200).
- **Diamond*UTC***. One type of NSD that combines the capabilities of a Sun Microsystems' Sun Ray™ and Diamond*Link* capabilities into an integrated secure ultra-thin client desktop. Note: This product is also sold under the name CT100.
- **Diamond*VPN*.** One type of NSD used to protect and control a fixed network entity or collection of such entities (e.g., sub-network). Note: This product is also sold under the name CV100.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **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.
- **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.** The 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.** The 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.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **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.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.

- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 2.1, August 1999. CCIMB-99-031.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 2.1, August 1999. CCIMB-99-032.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 2.1, August 1999. CCIMB-99-033.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 11 January 1997.

[5] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 1.0, August 1999.

[6] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[7] Science Applications International Corporation. *Cryptek DiamondTEK 2.4 Security Target,* Version 2.0, 30 December 2005

[8] Science Applications International Corporation. *Final Evaluation Technical Report for the DiamondTEK™ Product (DiamondCentral®: NSC Application S/W version 2.4.0.5; NSD-Prime F/W version 2.4.0.3) and NSD (DiamondLink™, DiamondPak™, DiamondVPN™, DiamondSAT™, DiamondUTC™) F/W version 2.4.0.3, Part 1 (Non-Proprietary)*, Version 1.0, 30 December 2005

[9] Science Applications International Corporation. *Final Evaluation Technical Report for the DiamondTEK™ Product (DiamondCentral®: NSC Application S/W version 2.4.0.5; NSD-Prime F/W version 2.4.0.3) and NSD (DiamondLink™, DiamondPak™, DiamondVPN™, DiamondSAT™, DiamondUTC™) F/W version 2.4.0.3, Part 2 (Proprietary)*, Version 1.0, 30 December 2005

Note: This document was used only to obtain the description of the test effort.