National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Diamond*TEK*™ Product

(Diamond*Central*®: NSC Application S/W version 2.0.1; NSD-Prime F/W version 2.1.4) and NSD (Diamond*Link*™, Diamond*Pak*™, Diamond*VPN*™) F/W version 2.1.4

Report Number:	**CCEVS-VR-02-0021**
Dated:	**28 June 2002**
Version:	**3.0**

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

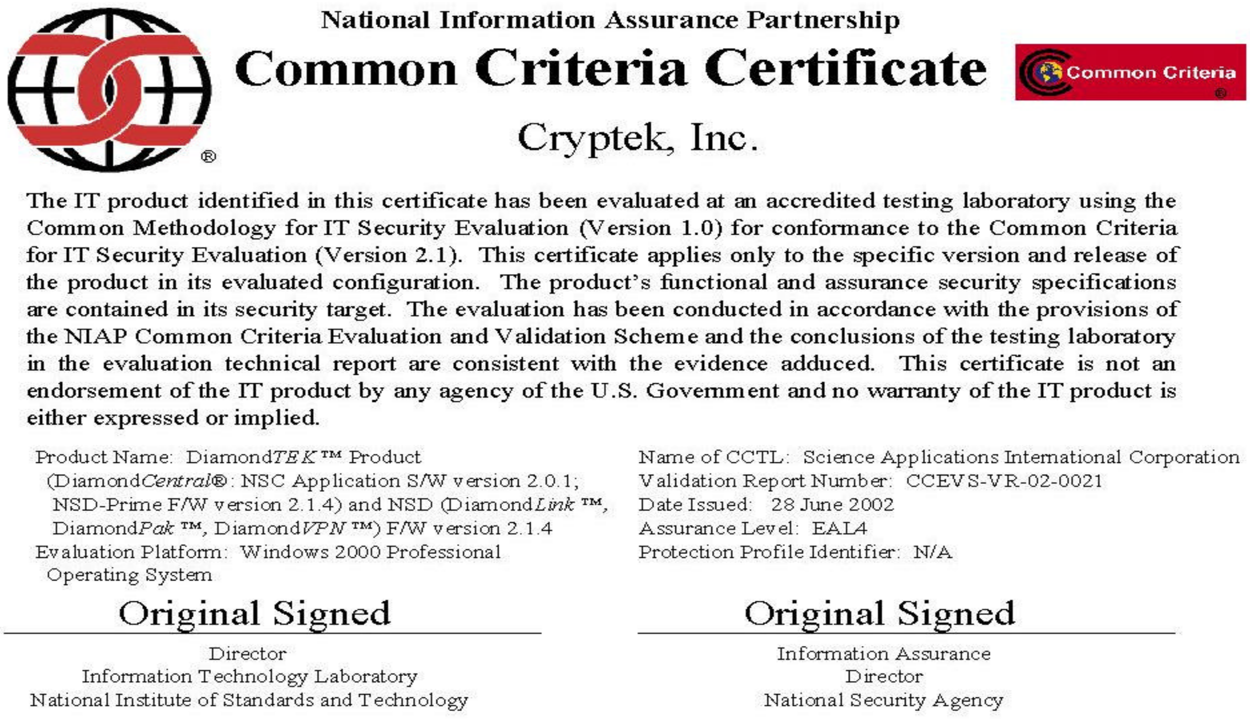
ACKNOWLEDGEMENTS

Validation Team

Elizabeth A. Foreman
Donald W. Phillips
S. Meg Weinberg
Mitretek Systems Inc.,
Falls Church, VA

Common Criteria Testing Laboratory

Science Applications International Corporation
Columbia, Maryland



National Information Assurance Partnership

Common Criteria Certificate

Common Criteria

Cryptek, Inc.

The IT product identified in this certificate has been evaluated at an accredited 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 certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. 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 adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name: Diamond*TEK* ™ Product
(Diamond*Central*®: NSC Application S/W version 2.0.1;
NSD-Prime F/W version 2.1.4) and NSD (Diamond*Link* ™,
Diamond*Pak* ™, Diamond*VPN* ™) F/W version 2.1.4
Evaluation Platform: Windows 2000 Professional
Operating System

Name of CCTL: Science Applications International Corporation
Validation Report Number: CCEVS-VR-02-0021
Date Issued: 28 June 2002
Assurance Level: EAL4
Protection Profile Identifier: N/A

Original Signed
Director
Information Technology Laboratory
National Institute of Standards and Technology

Original Signed
Information Assurance
Director
National Security Agency

Table of Contents

1 Executive Summary

The evaluation of the Diamond*TEK*™ Product (Diamond*Central*®: NSC Application S/W version 2.0.1; NSD-Prime F/W version 2.1.4) and NSD (Diamond*Link*™, Diamond*Pak*™, Diamond*VPN*™) F/W version 2.1.4 was performed by Science Applications International Corporation (SAIC) in the United States and was completed on 26 June 2002. The evaluation was conducted in accordance with the requirements of the Common Criteria, version 2.1, and the Common Methodology for IT Security Evaluation (CEM) (Version 1.0).

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 (EAL4) have been met.

This Validation Report is not an endorsement of the Diamond*TEK* product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) produced by SAIC.

1.1 Evaluation Details

Evaluated Product: Diamond*TEK*™ Product (Diamond*Central*®: NSC Application S/W version 2.0.1; NSD-Prime F/W version 2.1.4) and NSD (Diamond*Link*™, Diamond*Pak*™, Diamond*VPN*™) F/W version 2.1.4

Developer: Cryptek, Inc.
1501 Moran Road, Sterling, VA 20166

CCTL: SAIC, 7125 Columbia Gateway Drive, Suite 300
Columbia, MD 22102-3305

Validation Team: Elizabeth A. Foreman, Donald W. Phillips and S. Meg Weinberg, Mitretek Systems, Inc., 3150 Fairview Park South, Falls Church, VA 22042-4519

EAL: EAL4

Completion Date: 26 June 2002

1.2 Interpretations

The Evaluation Team performed an analysis of the international and national interpretations regarding the CC and the CEM and determined that the following NIAP Interpretations were applicable to this evaluation:

1. User Attributes To Be Bound Should Be Specified (0351)
2. Scope Of Permitted Refinements (0362)
3. Identification Of Standards (0427)
4. Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3 (0418)
5. Clarification Of ``Audit Records'' (0422)
6. Settable Failure Limits Are Permitted (0425)
7. Association Of Information Flow Attributes W/Subjects And Information (0417)
8. Some Modifications To The Audit Trail Are Authorized (0423)
9. American English Is An Acceptable Refinement (0405)
10. A Completely Evaluated ST Is Not Required When TOE (0393)

The Evaluation Team determined that the following CCIMB interpretations were applicable to this evaluation:

1. Separate Objectives for TOE and Environment (084)
2. Level of Detail Required for Hardware Descriptions (025)

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.

1.3 Threats to Security

The Security Target identified the following threats that the evaluated product addresses:

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.

2. Identification

2.1 ST and TOE Identification

ST – Diamond*TEK* Security Target, Revision 1.0, 25 June 2002

TOE Identification – The TOE includes 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
- And one or more of the following NSDs:
  - Diamond*Link* (part number: DL100, DL100F), F/W version 2.1.4
  - Diamond*Pak* (part number: DP200, DP400, DP600), F/W version 2.1.4
  - Diamond*VPN* (part number: DV100), F/W version 2.1.4
  - NSD-Prime F/W version 2.1.4
- Applicable Guidance Documents:
  - 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, 11/1/01

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

CEM Identification – *Common Evaluation Methodology for Information Technology Security*, Part 1: Introduction and General Model, Version 0.6, January 1997; *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Version 1.0, August 1999.

Although the ST, the developer's evaluation evidence documents, and the developer's product literature often refer to the TOE as a "system," the developer and Evaluation Team have emphasized throughout the evaluation that the TOE fits the CC definition of a product – "a package of IT software, firmware and/or hardware, providing functionality

[1] Not all of Diamond*Central* is in the TOE. Only the indicated portions (NSC Application and NSD-Prime) are TOE components.

designed for use or incorporation within a multiplicity of systems" – and not that of a system – "a specific IT installation, with a particular purpose and operational environment" [CC, Part 1, Section 2.3, Glossary].

For the remainder of this report, the TOE (Diamond*Central*: NSC Application S/W version 2.0.1; NSD-Prime F/W version 2.1.4) and NSD (Diamond*Link*, Diamond*Pak*, Diamond*VPN*) F/W version 2.1.4) will be referred to as the "Diamond*TEK* TOE." The Diamond*TEK* product, which contains additional components that are not part of the TOE, will be referred to as the "Diamond*TEK* product."

The Diamond*TEK* product that is delivered to a customer has two major hardware/firmware/software components: The Network Security Controller (NSC) and the Network Security Device (NSD). Each is described below.

The NSC is a rack-mountable network management workstation into which Cryptek® has installed the following:

- NSC Application
- Windows 2000 Professional operating system on which the NSC Application runs and on which the Diamond*TEK* security attributes, audit records, and configuration data reside[2]
- NSD-Prime
- Card reader/writer device
- Driver on the Windows 2000 operating system platform that allows the NSC Application to communicate with the other NSC components
- Hardware platform on which the OS executes[3]

The consumer needs to provide the monitor, keyboard, and mouse to access the NSC Application.

The NSD is a device that connects a host computer, server, or other IT device to a network and controls the flow of information between that host and network according to a set of security policies defined for the host. There are three types of NSDs based on the particular network configuration(s):

- Diamond*Link* controls access to desk-top computers and other IT devices (e.g., printers, fax machines)

- Diamond*Pak* protects multiple servers each with its own Operational Profile

- Diamond*VPN* protects LAN or WAN perimeters

[2] The Windows 2000 Professional operating system product is not part of the TOE.
[3] The hardware platform is not part of the TOE.

To acquire the Diamond*TEK* TOE, consumers must specify the part number of the type of NSC that they require based on the number of users and/or nodes to be supported:

NSC Type	Part Number
Diamond*Central*	DC1: 10 users and 250 Diamond*TEK* nodes
	DC2: 10 users and 1000 Diamond*TEK* nodes
	DC3: 10 users and unlimited Diamond*TEK* nodes

and one or more types of NSDs and their part numbers:

NSD Type	Part Number
Diamond*Link*	DL100: support for RJ-45 copper network interface DL100F: support for fiber-optic network interface
Diamond*Pak*	DP200: support for 2 servers DP400: support for 4 servers
	DP600: support for 6 servers
Diamond*VPN*	DV100

2.2 IT Security Environment

The Diamond*TEK* TOE requires an IT environment suitable to support the operation of the NSC. Specifically, the NSC Application is designed to operate using features offered by a Windows 2000 Professional operating system. The NSC Application relies on Windows 2000 to instantiate itself as a process, to manage memory, to manage files, to access time and date information, store and review audit records, and to provide access to various input/output devices – keyboard, mouse, and display. In addition, the NSC Application relies on the Windows 2000 driver model, which has been used to create the driver that allows the NSC Application to communicate with the NSD-Prime.
With regard to physical interfaces, the NSD-Prime requires that the hardware hosting the Windows 2000 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.

Of all of these dependencies, the only dependencies that are directly related to security functions are the Windows 2000 provisions of time and date information as well as storage and review or audit records.

3. Security Policy

The Diamond*TEK* TOE provides five security services. Their descriptions in the following sections were taken from the ETR, Part 1[4] (Non-Proprietary version).

3.1 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 the audit records received from NSDs as well as the audit records related to security management of the Diamond*TEK* TOE that are generated by the NSC itself.

3.2 Information Flow Protection

The Diamond*TEK* TOE 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

[4] This section, for the most part, was taken verbatim from the ETR except for its use of the terms, "Diamond*TEK*" and "Diamond*TEK* system," which the Validation Team has clarified to refer to the Diamond*TEK* TOE or the Diamond*TEK* product.

(which deals with source and destination address) that will be used to decide whether to allow network packets to be sent and received.

3.3 Identification and Authentication

The Diamond*TEK* TOE requires each user to be identified and authenticated prior to allowing the user to perform any other security functions. There are two roles supported by the Diamond*TEK* TOE 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.

3.4 Security Management

The Diamond*TEK* TOE 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.

3.5 TOE Self Protection

The physical protection of the TOE Security Functions (TSF) is largely accomplished via protection of its environment, and the operating system is trusted to not negatively impact the TOE security functions given the assumption on the environment A.Pltfrm. 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 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.

The “subjects” in the Diamond*TEK* TOE 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.

Logically, each NSD is protected largely by virtue of the fact that its interface is limited to primarily only support network traffic. A physical card reader device that limits any potential for logical attacks provides the identification and authentication interface of the NSD. 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 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.

4. Assumptions

4.1 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.

4.2 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. [5]

4.3 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.

[5] Since the Diamond*TEK* product 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.

5. Architectural Information

The Diamond*TEK*™ product is a secure network product that enforces centrally defined security policies for the flow, encryption, and auditing of data transmitted between computers residing on a network. The Diamond*TEK* product operates at the network layer of the Open Systems Interconnection (OSI) protocol stack using Internet Protocol Version 4 (IPv4) networking. Non-IP based protocols are supported by tunneling across the IP network. The Diamond*TEK* product 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.

The Diamond*TEK* product consists of two subsystems: the Network Security Console (NSC) and the Network Security Device (NSD).

Each Diamond*TEK* product includes a single NSC subsystem and one or more instances of a NSD subsystem – all connected to each other via a network. While NSDs are designed to communicate with each other as well as with other designated network nodes, the NSC can only communicate with the NSDs that are under its control. This restriction of interface between the NSC and its associated NSDs is enforced by the special NSD device included in the NSC called the NSD-Prime and is accomplished by rejecting any traffic not originating from a known NSD, sending traffic only to known NSDs, and requiring that all such communications be transmitted using Internet Protocol security (IPsec) to ensure both integrity and privacy.

5.1 NSC Subsystem

The NSC subsystem consists of the NSC Application, the NSD-Prime, a card reader/writer device, and a driver to allow the Application to communicate with the card reader/writer device and the NSD-Prime – all developed by Cryptek. These components have been designed to run on the Windows 2000 Professional Operating System that is provided with the NSC subsystem (but which is not a component of the TOE). The NSC Application stores the numerous information tables that define the various network nodes, policies, users, and administrators in files managed by Windows 2000. The NSC Application also stores audit records using the Windows 2000 Event Logger and date/time stamp, and it provides access to the audit log management functions of the Windows 2000 Event Viewer.

The Windows 2000 Professional operating system is required to provide an operational application environment including process management, data storage (files and memory), and console input and output. The NSC provides a graphical user interface (GUI) that allows an authorized administrator, called the Network Security Manager (NSM), to manage the information tables and network state information.

The NSC Application communicates security information to and from all of the NSDs that are known to the NSC through the NSD-Prime. The NSC can indirectly communicate with its known NSDs by means of User Authentication and NSD Installation cards that it programs using an attached card reader/writer device.

The NSC information tables define the policies for each NSD identifying, for example, the nodes with which the NSD is allowed to communicate, the maximum security level and the minimum security level of information that is allowed to flow through the NSD. The NSC tables also define the audit thresholds for each NSD.

The NSC also maintains a set of state information with which the NSC Application tracks whether each user and NSD is online, offline, or otherwise suspended.

5.2 NSD Subsystem

The NSD subsystem consists of a NSD device specific to the host or hosts (computer, printer, LAN, server) that it is configured to protect and a Card Reader. The NSD's interface to the host and its interface to the network interfaces are based on standard protocols. Figure 1 shows how the Diamond*LINK*, Diamond*VPN*, and Diamond*PAK* can be configured.

The NSD primarily inspects the network traffic that arrives at the NSD to enforce a number of access control policies. Except when traffic is rejected, the NSD is designed to be essentially 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). The NSD might also modify packet headers (other than IPsec headers), albeit not for security reasons, but rather to facilitate proper routing and non-IP encapsulation.

The operations of the NSD's network and host interfaces depend upon the state of the NSD. The NSD can be online, offline, or suspended. An online NSD is fully functional within the parameters of its operational profile. Both offline and suspended NSDs, however, will generally not allow network traffic to pass through. An offline NSD, with few exceptions, will generally not have a link with the network (i.e., the network link is turned off) and it requires the user to be authenticated before going back online. A suspended NSD still has a network link and it can resume operation when it receives a resume command from the NSC.

Each NSD is connected to the network and to the host (e.g., personal computer or network) that it is configured to protect. A NSD can be connected to a host by connecting to a Network Interface Card (NIC) already present in the host or it can be installed in the host, via a PCI bus, in place of a NIC card.

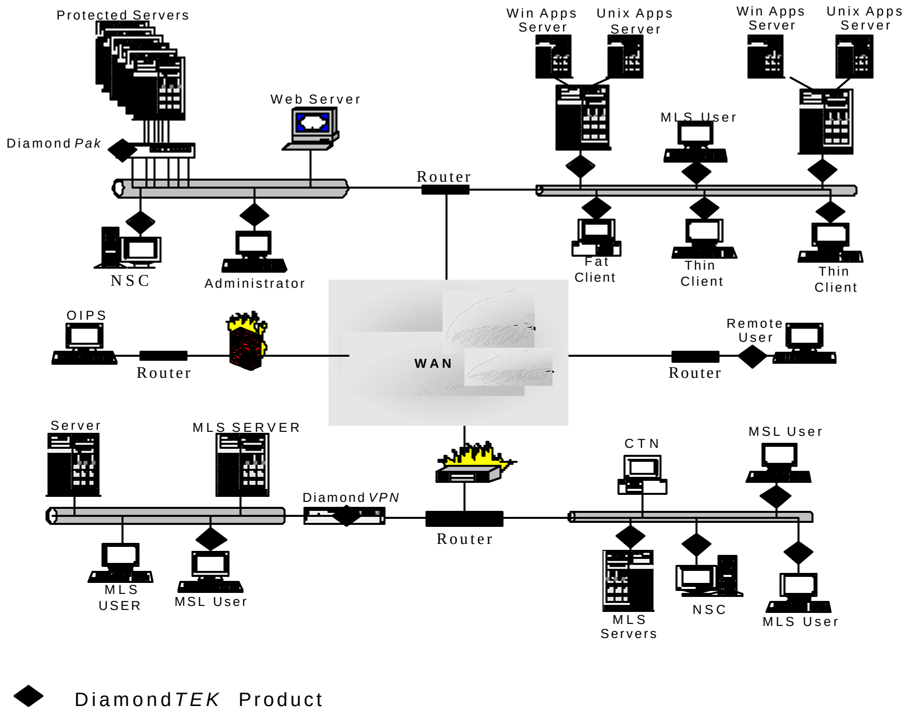


Figure 1. Sample NSD Configurations

Each NSD includes a user interface in the form of a card reader. While the NSD is used to control the flow of information between a host and the network, the card reader is used to either install a new NSD or to allow a user to log on to the NSD so that the NSD will begin to allow information to flow under its control.

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). Since the NSD does not include the date or time in its records, 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 requires that a user be identified and authenticated before it goes online and allows traffic to flow through the device in accordance with the information flow policies. If the NSD is configured to not require a User Authentication card, it will come online automatically after a power-cycle and the operations at that NSD will be accountable to the user that the NSM assigned to the NSD. If the NSD is configured to require a User Authentication card, the user must insert an appropriate card and provide the correct PIN, if required for the NSD. If the authentication information is valid, the

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

6. Documentation

Purchasers of the Diamond*TEK* product receive the following documentation:

- Diamond*TEK* 10/100 User Pamphlet, 6 March 2002
- Diamond*TEK* 10/100 Secure Network Administration, Version 2.0.1, 19 March 2002
- Diamond*TEK* Secure Network Commands Manual, Version 2.0, 1 December 2000
- Release Notes for Diamond*TEK* 10/100 Secure Network Administration, Version 2.0.1, 19 March 2002
- Diamond*TEK* User's Guide, revision 1.02, 1 November 2001

7. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

The developer designed tests to address the two major subsystems of the Diamond*TEK* TOE:

- NSC: Test the security-relevant operation of all of the available security management functions and auditing the use of those functions

- NSD: Test the security functions available through the NSD interfaces

The tests for both subsystems involved tests of the NSC and NSD interfaces identified in the Functional Specification and the High-Level Design. Each test is indirectly mapped to the security function tested.

The developer tested all of the 5 TOE Security Functions and, for the User Data Protection Security Function, the Mandatory, Association and Packet Filtering policies.

The developer's tests completed successfully and the developer archived all test results in the Configuration Management repository.

The developer's test configuration consisted of several interconnected local area networks (LAN) on which the various types of NSDs, security policies, and node types (e.g., the Clear Text Node, Other IP Security Node (OIPS)) were tested. The test configuration included a NSC and several NSDs including each of the different NSD types: Diamond*Pak*, Diamond*Link*, Diamond*VPN*. The NSC and NSDs represented a subset of the various NSC and NSD part numbers.

SAIC and the developer consider the detailed test configuration to be proprietary information. However, the Evaluation Team has included a Network Diagram, Test Equipment listing, and the initial security profiles and security configuration settings for the developer's test configuration in the ETR, Part 2.

The Evaluation Team determined that the developer's actual test results matched the developer's expected results.

7.2 Evaluation Team Independent Testing

The Evaluation Team chose to repeat a sample of the tests that the developer performed. The Evaluation Team ensured that its sample addressed all TOE Security Functions, the two subsystems (NSC and NSD), and all external interfaces.

In addition, the Evaluation Team also tested the installation, generation, and start-up procedures to determine, in accordance with ADO_IGS.1.2E, that those procedures result in a secure configuration.

The Evaluation Team used the developer's test configuration to perform the tests in its sample.

The Validation Team observed a subset of the Evaluation Team's independent testing effort and concluded that the testing was successful.

7.3 Evaluation Team Penetration Testing

For its penetration tests, the Evaluation Team conducted a brainstorming session to identify penetration test cases based on the Evaluation Team's experience with evaluating the developer's design, guidance, test and vulnerability assessment documentation, performing a code review for the ADV_IMP.1 requirement, and running a portion of the developer's tests.

The Evaluation Team used the developer's test configuration to successfully perform its penetration tests.

The Validation Team observed the Evaluation Team's penetration testing and concluded that the testing was successful.

The Evaluation Team's ETR, Part 2, provides a detailed description of the tests, the results, and the effects, if any, on the information presented in the ST or other evaluation evidence.

8. Evaluated Configuration

In Section 8 of the ETR, Part 2, "Evaluation of Class ATE: Test Documentation," the Evaluation Team reported that the test configuration was consistent with the evaluated configuration in the Security Target.

Per section 8.1.4.1 of the ETR, Part 2, the "TOE tested included each of the components identified in the ST: The NSC and each type of NSD (DPAK, DLINK, and DVPN)" – that is:

- One NSC with its TOE and non-TOE components
- Each type of NSD:
  - DLINK: Diamond*Link*
  - DPAK: Diamond*Pak*
  - DVPN: Diamond*VPN*

In section 3.1.1.3 of the ETR, Part 2, the Evaluation Team states, "Based upon the functional specification, the evaluation team has not discovered any functionality that must be turned off. This conclusion is based on the ST TSS and the functional specification."

To set up the NSC, the following option settings are supported:

- Keep Alive mode (Enable or disable): Choose either setting (ETR, Part 2, section 8.1.4.2)

- Audit Log Settings (Overwrite audit logs upon audit log overflow or Shut Down NSDs): Choose Overwrite (The Shut Down option is not included in the evaluated configuration) (ETR, Part 2, section 8.1.4.2)

- Do not create NSM "operator types" since the TOE does not support the operator role. Section 3.1.2.9 of the ETR, Part 2, states, "The operator role is not included in [the] evaluated configuration according to the ST and therefore, the Administrator Guidance (and Configuration guidance) should instruct the NSM to not create NSM "Operator Types."

To install the TOE, section 2.2.2.3 of the ETR, Part 2, (regarding ADO_IGS.1) states that the following documents "provided installation, generation, and start-up procedures that describe the steps necessary for secure installation, generation, and start-up of the TOE":

- Diamond*TEK* 10/100 Secure Network Administration Manual, version 2.0.1 (03/19/02)

- Diamond*TEK* 10/100 Secure Network Commands Manual, version 2.0 (12/01/01)

- Diamond*TEK* 10/100 User Pamphlet (03/06/02)

Section 2.2.2.3 of the ETR, Part 2, also states, "The testing activity confirmed that the installation, generation, and start-up procedures result in a secure configuration."

Based of its knowledge of the TOE components, the Validation Team has concluded that the evaluated configuration does not include the following:

- Printer and print-related administrator commands
- Windows 2000 Operating System
- Hardware platform for the Windows 2000 Operating System

9. Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL4 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Verdicts were not assigned to assurance classes.

Section 5, Results of Evaluation, in the Evaluation Team's ETR, Part 1, states:

> The evaluation determined the TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 4) requirements. The rationale supporting each CEM work unit verdict is recorded in the "Evaluation Technical Report for Diamond*TEK* Part II" which is considered proprietary.

Section 6, Conclusions, in the Evaluation Team's ETR, Part 1, states:

> 6.1 Each verdict for each CEM work unit in the ASE ETR is a "PASS". Therefore, the Diamond*TEK* ST is a CC compliant ST.
>
> 6.2 The verdicts for each CEM work unit in the ETR sections included in chapter 15 are each "PASS". Therefore, when configured according to the following guidance documentation:
>
> - Diamond*TEK*™ 10/100User Pamphlet, March 6, 2002
> - Diamond*TEK*™ 10/100 Secure Network Administration, Version 2.0.1, 19 March 2002
> - Diamond*TEK*™ Secure Network Commands Manual, Version 2.0, 1 December 2000
> - Release Notes for Diamond*TEK*™ 10/ 100 Secure Network Administration Version 2.0.1, 19 March 2002
> - Diamond*TEK*™ User's Guide, revision 1.02, November 1, 2001
>
> the Diamond*TEK* TOE (see below product identification) satisfies the Cryptek DiamondTEK Security Target, Version 1.0. Diamond*Central*

(NSC Application S/W version 2.0.1, NSD-Prime F/W version 2.1.4) and NSD (Diamond*Link*, Diamond*Pak*, Diamond*VPN*) F/W version 2.1.4.

10. Validation Comments/Recommendations

The Validation Team observed that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The Validation Team agrees that the CCTL presented appropriate rationales to support the evaluation results presented in Section 5 of the ETR and the Conclusions presented in Section 6 of the ETR.

The Validation Team, therefore, concludes that the evaluation and Pass result for the TOE identified below is complete and correct:

Diamond*TEK*™ Product

(Diamond*Central*®: NSC Application S/W version 2.0.1; NSD-Prime F/W version 2.1.4) and NSD (Diamond*Link*™, Diamond*Pak*™, Diamond*VPN*™) F/W version 2.1.4

11. Glossary

- 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).

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

- 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 – 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.

12. Bibliography

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

- *Common Criteria for Information Technology Security Evaluation*, version 2.1, august 1999, Parts 1, 2, and 3

- 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.

- *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, version 0.6, 11 January 1997.

- *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, version 1.0, August 1999.

- Cryptek Diamond*TEK* Security Target, Version 1.0, Diamond*Central* (NSC Application S/W version 2.0.1, NSD-Prime F/W version 2.1.4) and NSD (Diamond*Link*, Diamond*Pak*, Diamond*VPN* F/W version 2.1.4), 25 June 2002.

- Cryptek Diamond*TEK* High-Level Design, Revision 0.6, Diamond*Central* (NSC Application S/W version 2.0.1, NSD-Prime F/W version 2.1.4) and NSD (Diamond*Link*, Diamond*Pak*, Diamond*VPN* F/W version 2.1.4), 23 April 2002.

- Evaluation Technical Report for the Diamond*TEK* Product (Diamond*Central*®: NSC Application S/W version 2.0.1; NSD-Prime F/W version 2.1.4) and NSD (Diamond*Link*™, Diamond*Pak*™, Diamond*VPN*™) F/W version 2.1.4, Part 1 (Non-Proprietary), Version 0.4, 25 June 2002.

- Evaluation Technical Report for the Diamond*TEK* Product (Diamond*Central*®: NSC Application S/W version 2.0.1; NSD-Prime F/W version 2.1.4) and NSD (Diamond*Link*™, Diamond*Pak*™, Diamond*VPN*™) F/W version 2.1.4, Part 1 (Proprietary), Version 0.4, 25 June 2002.

- Evaluation Technical Report for the Diamond*TEK* Product (Diamond*Central*®: NSC Application S/W version 2.0.1; NSD-Prime F/W version 2.1.4) and NSD (Diamond*Link*™, Diamond*Pak*™, Diamond*VPN*™) F/W version 2.1.4, Part 2 (Proprietary), Version 0.9, 26 June 2002