National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Thales e-Security Datacryptor SONET/SDH with Element Manager and Gigabit Ethernet with Element Manager

Report Number: CCEVS-VR-VID10189-2009

Dated: 07 April 2009

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 6757
Fort George G. Meade, MD 20755

ACKNOWLEDGEMENTS

Validation Team

Dianne Hale (Lead Validator)

NSA

Franklin Haskell (Senior Validator)

Mitre Corporation

Bedford, Massachusetts

Common Criteria Testing Laboratory

COACT CAFÉ Laboratory

Columbia, Maryland

Table of Contents

1. EXECUTIVE SUMMARY 1

1.1. INTERPRETATIONS 2

2. IDENTIFICATION 4

TABLE 1: EVALUATION IDENTIFIERS 4

3. SECURITY POLICY 6

3.1. AUTHENTICATION 6
3.2. SECURITY AUDIT 6
3.3. INFORMATION FLOW CONTROL 6
3.4. SECURITY MANAGEMENT 7
3.5. PROTECTION OF SECURITY FUNCTIONS 7

4. ASSUMPTIONS AND CLARIFICATION OF SCOPE 7

4.1. PHYSICAL SECURITY ASSUMPTIONS 7
4.2. PERSONNEL SECURITY ASSUMPTIONS 7
4.3. OPERATIONAL SECURITY ASSUMPTIONS 7
4.4. THREATS COUNTERED AND NOT COUNTERED 7
4.5. ORGANIZATIONAL SECURITY POLICIES 8
4.6. CLARIFICATION OF SCOPE 8
4.7. EVALUATED CONFIGURATIONS 10
4.7.1. Evaluator Test Setup Assumptions 11
4.7.2. Test Assumptions 11

5. DOCUMENTATION 12

6. IT PRODUCT TESTING 15

6.1. DEVELOPER TESTING 15
6.2. FUNCTIONAL TEST RESULTS 15
6.3. EVALUATOR INDEPENDENT TESTING 15
6.4. EVALUATOR PENETRATION TESTS 16
6.5. TEST RESULTS 17

7. EVALUATED CONFIGURATION 17

8. RESULTS OF THE EVALUATION 18

9. VALIDATOR COMMENTS 18

10. SECURITY TARGET 18

11. GLOSSARY 19

12. ACRONYM LIST 20

13. BIBLIOGRAPHY 21

1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated. Prospective users should read the Validator Comments in Section 10 carefully.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Thales e-Security Datacryptor SONET/SDH with Element Manager and Gigabit Ethernet with Element Manager, the target of evaluation (TOE), conducted by the CAFÉ Laboratory of COACT Incorporated, the Common Criteria Testing Laboratory (CCTL). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation by COACT was performed in accordance with the United States evaluation scheme and was completed on February 9th, 2009. The information in this report is largely derived from the ST, Evaluation Technical Report (ETR) and the functional testing report. The ST was written by COACT, Inc. The evaluation was performed to conform with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005 Evaluation Assurance Level 3 (EAL 3) and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.3, August 2005.

Thales e-Security Datacryptor SONET/SDH with Element Manager and Gigabit Ethernet with Element Manager Target of Evaluation (TOE) provides point-to-point encryption to another Datacryptor over untrusted networks. Each TOE includes Element Manager, which is a GUI application for management and configuration of the Datacryptor SONET/SDH device via the 10/100 Ethernet Management port. Each TOE provides strong encryption at Layer 2, robust key management, detailed auditing, and comprehensive management capabilities to provide security for the most demanding service requirements.

SONET/SDH Technology Overview

SONET/SDH is a transmission technology for fibre optic telecommunications. The SONET standard was originally developed as an American National Standards Institute (ANSI) specification. The standard was internationalized as SDH by the Consultative Committee on International Telegraphy and Telephony (CCITT), now the International Telecommunications Union (ITU). While native SONET and SDH are very similar, there are a number of structural differences between the protocols used by each standard, including the manner by which the Synchronous Payload Envelopes (SPEs) in SONET and the

Virtual Containers (VCs) in SDH are constructed, as well as a number of differences in their respective header characteristics[1].

Datacryptor SONET/SDH Description

The Thales Datacryptor SONET/SDH implements security features for data flows over a Synchronous Optical Network (SONET). The primary security function of the TOE is to provide confidentiality services for data flows over optical networks, and the other functions of the TOE support this primary function. The TOE is deployed at the edge of an untrusted optical network with the intent to provide secure communications between two trusted networks that are physically separated.

Potential areas of application include scenarios where distant PBX devices, routers (POS) or switches are connected via SONET/SDH links vulnerable to interception and alteration. The Datacryptor SONET/SDH encryption appliance delivers high performance and confidentiality to these usage applications.

The TOE encrypts unencrypted data flows that enter the device from the trusted network side before they are forwarded across the untrusted optical network. When the encrypted data flow reaches the remote device, the TOE decrypts the data before forwarding it to the remote trusted network. In short, data is encrypted at one device's outbound interface and decrypted at the other device’s inbound interface.

Datacryptor Gigabit Ethernet Description

The Thales Datacryptor Gigabit Ethernet implements security features for data flows over an Ethernet network. The primary security function of the TOE is to provide confidentiality services for data flows over untrusted networks, and the other functions of the TOE support this primary function. The TOE is deployed at the edge of an untrusted network with the intent to provide secure communications between two trusted networks that are physically separated.

The TOE encrypts unencrypted data flows that enter the device from the trusted network side before they are forwarded across the untrusted network. When the encrypted data flow reaches the remote device, the TOE decrypts the data before forwarding it to the remote trusted network. In short, data is encrypted at one device's outbound interface and decrypted at the other device’s inbound interface.

1.1. Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that no international interpretations issued by the Common

[1] Recognizing these differences, it is important to note that from an encryption perspective, the Datacryptor SONET/SDH is transparent to these differing characteristics.

Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation. The TOE is also compliant with all International interpretations with effective dates on or before January 26, 2007.

The Evaluation Team determined that the following NIAP interpretations applied at the time of the start of the evaluation:

I-0418 – Evaluation of the TOE Summary Specification: Part 1 Vs Part 3

I-0426 – Content of PP Claims Rationale

I-0427 – Identification of Standards

2. IDENTIFICATION

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

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT 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;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Thales e-Security Datacryptor SONET/SDH Release 4.0 with Element Manager and Thales e-Security Datacryptor Gigabit Ethernet Release 4.0 with Element Manager Target of Evaluation
Protection Profile	None
Security Target	Thales e-Security Datacryptor SONET/SDH Release 4.0 with Element Manager and Thales e-Security Datacryptor Gigabit Ethernet with Element Manager Security Target
Dates of evaluation	September 2006 through February 2009
Evaluation Technical Report	Evaluation Technical Report for Thales e-Security Datacryptor SONET/SDH Release 4.0 with Element Manager and Thales e-Security Datacryptor Gigabit Ethernet Release 4.0 with Element Manager. Document No. F3-0309-003, Dated 27 March 2009.
Conformance Result	Part 2 and Part 3 conformant, EAL 3

Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 2.3, August 2005 and all applicable NIAP and International Interpretations effective on January 26, 2007
Common Evaluation Methodology (CEM) version	CEM version 2.3, August 2005 and all applicable NIAP and International Interpretations effective on January 26, 2007
Sponsor	Thales e-Security, Inc. 2200 North Commerce Parkway, Suite 200 Weston, Florida 33326
Developer	Thales e-Security, Inc. 2200 North Commerce Parkway, Suite 200 Weston, Florida 33326
Evaluators	Bob Roland, Greg Beaver and Pascal Patin of COACT Incorporated
Validation Team	Dianne Hale (NSA), Franklin Haskell (MITRE)

3. SECURITY POLICY

Each TOE is comprised of two subsystems, the Datacryptor subsystem and the Element Manager subsystem. The former is an appliance that sends, receives, and processes plaintext and encrypted traffic for transmission to a secure network or over an untrusted network. The latter is a GUI management application that is used to configure the Datacryptor. The TOE does not include the operating system hosting the Element Manager, the trusted network, or the untrusted network.

For the Datacryptor subsystem, the physical boundary is the Datacryptor SONET/SDH and Datacryptor Gigabit Ethernet itself. The TOE is completely self-contained; it contains all software and hardware required to perform all security functions. The TOE operating system controls all data encryption and management functions.

The following SONET/SDH hardware models are included in the evaluation:

- OC-3 SONET/SDH
- OC-12 SONET/SDH
- OC-48 SONET/SDH
- OC-192 SONET/SDH

The following Gigabit Ethernet hardware models are included in the evaluation:

- 1 Gigabit Ethernet
- 10 Gigabit Ethernet

The security functions provided by the TOE and are described in the following sections.

3.1. Authentication

The TOE (via Element Manger) supports authentication of an authorized administrator, who manages the TOE locally or remotely. The administrator is required to authenticate via password before configuring TOE security functions. The password is used to decrypt various parameters used to verify authentication and encrypt the link between the Element Manager subsystem and the Datacryptor subsystem.

3.2. Security Audit

The TOE provides one log that reports management operations and errors. This log is stored in the Datacryptor and is viewed by an administrator via Element Manager.

3.3. Information Flow Control

The TOE provides encryption for data traversing from the trusted network to a remote trusted network, and each Datacryptor allows traffic to flow between subjects (e.g., instances of the TOE connected via an untrusted network and IT Systems connected via the trusted network). The configuration for this data encryption is specified in an Information Flow Control policy.

3.4. Security Management

The TOE is managed via GUI interface called Element Manager, which interfaces with the Datacryptor via the Ethernet interface. The TOE provides an administrators with the capabilities to configure, monitor and manage the TOE to fulfill the security objectives if the TOE. Security Management principles relate to Security Audit, Information Flow Control, and Cryptographic Support.

3.5. Protection of Security Functions

The TOE provides various protection mechanisms for its security functions, the enforcement of the information flow control policy and authentication rules at the applicable interfaces. The TOE also ensures that the TSF is protected against interference and tampering by untrusted subjects.

4. ASSUMPTIONS AND CLARIFICATION OF SCOPE

4.1. Physical Security Assumptions

A key environmental assumption is physical security, for it is assumed appropriate physical security protection will be applied to the TOE hardware and software commensurate with the value of the IT assets. Specifically, the TOE is assumed to be located in a secure location providing physical protection and limited access to administrators only.

4.2. Personnel Security Assumptions

It is assumed that all authorized administrators are properly trained, not careless, not willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation.

4.3. Operational Security Assumptions

It is assumed that the TOE will be installed in a network infrastructure such that it can effectively control the flow of applicable information

4.4. Threats Countered and Not Countered

The TOE and Operating IT Environment are designed to fully or partially counter the following threats:

T.ASSUME_ID_PKI_VER A user may assume the identity of another user in order to verify a PKI signature.

T.ATTACK An attacker (whether an insider or outsider) may gain access to the TOE and compromise its security functions by altering its configuration.

T.COMP_MANAGE Data may be compromised while traversing the connection between the Datacryptor subsystem and the Element Manager subsystem

T.MISCONFIG A malicious user might intentionally configure TOE security policy mechanisms incorrectly.

T.NO_ACCOUNT An administrator might perform actions for which they are not accountable.

T.NO_DETECT An unauthorized user, process or application attempts to mount an attack against the TOE security functions and/or associated data, which succeeds without detection.

T.SEC_BYPASS_DC The Datacryptor subsystem might be subject to malicious tampering or bypass of its security mechanisms.

T.SEC_BYPASS_EM The Element Manager subsystem might be subject to malicious tampering or bypass of its security mechanisms.

T.UNTRUSTED_PATH An attacker may attempt to disclose, modify or modify frame flows transmitted/received by the TOE over an untrusted network. If such an attack was successful, then the confidentiality of frame flows transmitted/received over an untrusted path would be compromised.

4.5. Organizational Security Policies

There are no applicable organizational security policies

4.6. Clarification of Scope

The following features are outside the scope of the TSF and thus are not evaluated:

- The ability to upgrade software/firmware components of the Datacryptor and Element Manager
- The use of SNMP for viewing of basic status and configuration details; SNMP must be disabled in the evaluated configuration.
- MAC address filtering
- Enhanced password security (Legacy password security in enabled by default, which requires passwords to be a minimum of 8 characters and a maximum of 20)

- The CLI is used for basic system provisioning and does not have access to security-relevant data; therefore, the CLI is not to be used after the TOE is configured per Administration Guidance

- The Certificate Manager is used in the initial provisioning of a Datacryptor and is not used again once the TOE is configured for evaluated configuration. The Certificate Manager can be used to generate Certificate Authority data, which can be backed up to removable media, including USB “thumb-drives” or floppy disks. Certificate Manager is not connected to the Datacryptor; the Certificate Manager resides on a stand-alone PC. The Administrator would transfer the data to the Element Manager to be loaded into the unit.

4.7. Evaluated Configurations

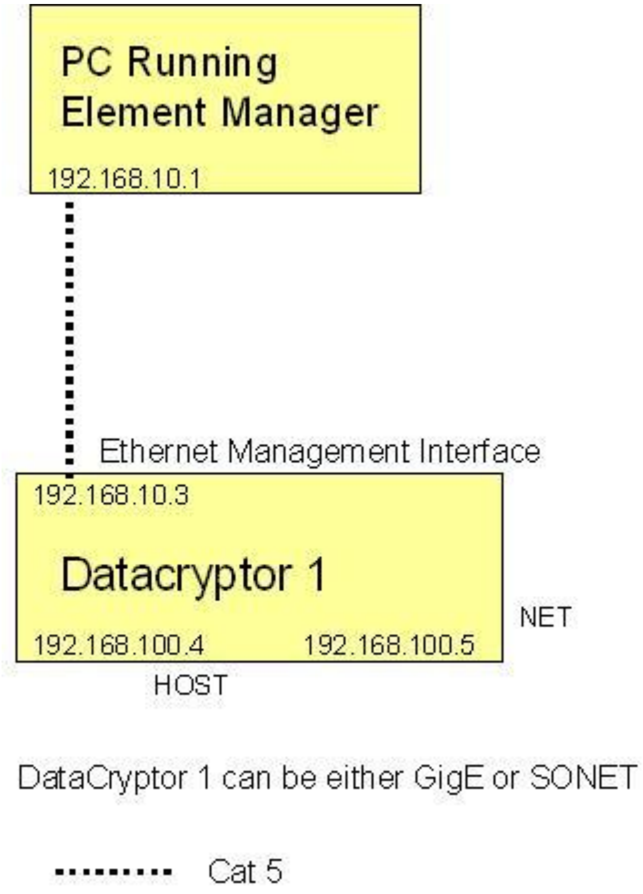

Figure 1 - Evaluator Test Setup 1 – Single Datacryptor Configuration

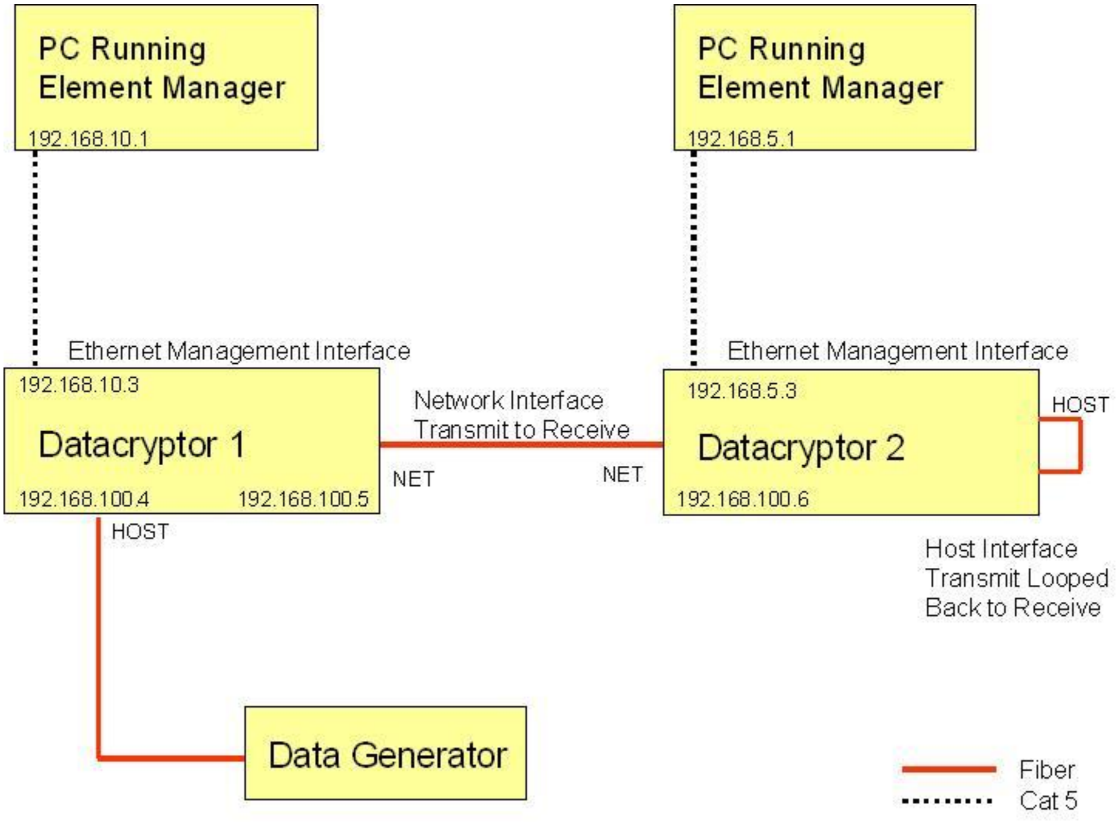
PC Running Element Manager
192.168.10.1
PC Running Element Manager
192.168.5.1
Ethernet Management Interface
192.168.10.3
Datacryptor 1
192.168.100.4
192.168.100.5
HOST
Network Interface Transmit to Receive
NET
NET
Ethernet Management Interface
192.168.5.3
Datacryptor 2
192.168.100.6
HOST
Host Interface Transmit Looped Back to Receive
Data Generator
Fiber
Cat 5

Figure 2 - **Evaluator Test Setup 2 – Two Datacryptor Configuration**

4.7.1. Evaluator Test Setup Assumptions

These assumptions are specific to the Evaluator Test Setup configurations.

A) Evaluator Test Setup 1 – Tests were conducted using both the GigE and the SONET Datacryptors. The line speeds are not critical to these tests.

B) Evaluator Test Setup 2 – Tests were conducted using both the GigE and the SONET Datacryptors. The line speeds are not critical to these tests and any line speed may be used as long as both Datacryptors have the same line speed. The Data Generator will be specific to each technology used.

C) The Element Manager is installed on a PC running Windows XP SP2.

4.7.2. Test Assumptions

The test configurations shown above were used by the evaluators to run the set of Evaluator Independent tests. The following list identifies the assumptions and steps required to place the TOE in the evaluated configuration.

A) Two instances of the TOE were required in order to transmit and receive encrypted data. This requirement included two Datacryptors and two PCs with the Element Manager installed. Each Datacryptor was controlled by its own PC with Element Manager installed.

B) The network for the Ethernet Management Port on the Datacryptor was separate from the trusted HOST network.

C) SNMP was disabled through Element Manager.

D) MAC Address Filtering is not used through Element Manager.

E) The Enhanced Security checkbox in the Gigibit Element Manager Configuration tab is unchecked.

F) Only Legacy password security is used, (requires passwords to be a minimum of 8 characters and a maximum of 20).

G) The CLI and the RS-232 port are not used after the TOE is configured for evaluated configuration.

H) Ports on the dedicated workstation running Element Manager that are unnecessary to the operation of the TOE (e.g., FTP, Telnet) should be disabled.

I) All tests were conducted while the Datacryptor was in the Encrypted Mode of operation.

J) Tests requiring the two Datacryptor configuration have the specific Data Generator and Datacryptor type identified in the assumptions identified for each test.

5. DOCUMENTATION

This section details the documentation that is delivered to the customer or was used as evidence for the evaluation of the Thales e-Security Datacryptor SONET/SDH Release 4.0 with Element Manager and Thales e-Security Datacryptor Gigabit Ethernet Release 4.0 with Element Manager. Documentation items A through V have been evaluated.

A) Security Target for Common Criteria Evaluation: Thales e-Security Datacryptor SONET/SDH and Gigabit Ethernet with Element Manager, Version 1.9, dated February 26, 2009;

B) Research and Development (R&D) Datacryptor SONET/SDH OC-3/12/48/192 Datacryptor Gig Ethernet Configuration Management Plan, January 31 2008;

C) Datacryptor SONET/SDH Network Encryptor – Security Operating Procedures, 1270A458-001, December 2006;

D) Datacryptor Gig Ethernet Network Encryptor – Security Operating Procedures, 1270A459-001, December 2006;

E) Thales Datacryptor SONET/SDH User Manual, Revision 1270A427-005, December 2006;

F) Thales Datacryptor Gig Ethernet User Manual, Revision 1270A450-002, August 2006;

G) Administrative Guidance and Installation, Generation, and Startup Procedures: Thales Datacryptor Gigabit Ethernet with Element Manager, Version 1.4, March 23, 2009;

H) Administrative Guidance and Installation, Generation, and Startup Procedures: Thales Datacryptor SONET/SDH with Element Manager, Version 1.3, March 23, 2009;

I) Secure Delivery Processes and Procedures: Thales e-Security Datacryptor Gigabit Ethernet Version 4.0 with Element Manager, Version 1.1, April 8, 2009

J) Secure Delivery Processes and Procedures: Thales e-Security Datacryptor SONET/SDH Version 4.0 with Element Manager, Version 1.1, March 15, 2007;

K) High Level Design and Correspondence Analysis: Thales Datacryptor Gigabit Ethernet with Element Manager, Version 1.4, February 27, 2009;

L) High Level Design and Correspondence Analysis: Thales Datacryptor SONET/SDH with Element Manager, Version 1.5, February 27, 2009;

M) Functional Specification: Thales Datacryptor Gigabit Ethernet with Element Manager, Version 1.7, February 27, 2009;

N) Functional Specification: Thales Datacryptor SONET/SDH with Element Manager, Version 1.6, February 27, 2009;

O) Identification of Security Measures: Thales Datacryptor Gigabit Ethernet with Element Manager, Version 1.4, April 8, 2008;

P) Identification of Security Measures: Thales Datacryptor SONET/SDH with Element Manager, Version 1.2, February 8, 2008;

Q) Datacryptor SONET/SDH & Datacryptor GigE Common Software Release 4.0 (1515 SONET & GigE Common Code program) System Test Plan, July 29, 2008;

R) Datacryptor SONET/SDH & Datacryptor GigE Common Software Release 4.0 (1515 SONET & GigE Common Code program) System Test Procedure, July 15, 2008;

S) Datacryptor SONET/SDH & Datacryptor GigE Common Software Release 4.0.11 (1515 SONET & GigE Common Code program) Test Report, July 29, 2008;

T) Test Coverage Analysis: Thales e-Security Datacryptor SONET/SDH with Element Manager and Gigabit Ethernet with Element Manager, Version 1.1, April 8, 2009;

U) Strength of Function Analysis: Thales Datacryptor SONET/SDH with Element Manager and Gigabit Ethernet with Element Manager, Version 1.2, July 21, 2008;

V) Vulnerability assessment: Thales Datacryptor SONET/SDH with Element Manager and Gigabit Ethernet with Element Manager, Version 1.1, April 8, 2009

The following is shipped with the product:

CD-ROM disk of Element Manager/FPV to include the Ethernet Quick Start Guide for 100M, Ethernet Quick Start Guide for 10 Gig, SONET Quick Start Guide for OC3-12-48, SONET Quick Start Guide for OC192, Ethernet User Manual, and SONET User Manual (all which are part of the evaluation).

A hard copy of the Release Notes.

Power supply cables and RS232 cable.

6. IT PRODUCT TESTING

This section describes the testing efforts of the Developer and the evaluation team.

6.1. Developer testing

Since the Evaluation team repeated all of the security testing accomplished by the developer, the test descriptions presented below under the Evaluation Team testing provide the documentation of the developer's effort.

The Developer and evaluation team tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. Each test case was identified by a number that correlates to the expected test results in the TOE Test Plan.

The evaluation team analyzed the Developer's testing to ensure adequate coverage for EAL 3. The evaluation team determined that the Developer's actual test results matched the Developer's expected test results.

Figures 1 & 2 in Section 4.7 shows the test configurations that were used by the Developers and the Evaluators. The Evaluators assessed that the test environment used by the Developers was appropriate and mirrored the test configuration during Independent testing.

6.2. Functional Test Results

The repeated developer test suite includes the developer functional tests. Additionally, each of the Security Functions and developer tested TSFIs are included in the CCTL test suite. The results are found in the Thales e-Security Datacryptor SONET/SDH Release 4.0 with Element Manager and Thales e-Security Datacryptor Gigabit Ethernet Release 4.0 with Element Manager Functional Test Report, Document No. F3-0309-002, dated 27 March 2009.

6.3. Evaluator Independent Testing

The tests chosen for independent testing allow the evaluation team to exercise the TOE in a different manner than that of the developer's testing. The intent of the independent tests is to give the evaluation team confidence that the TOE operates correctly in a wider range of conditions than would be possible purely using the developer's own efforts, given a fixed level of resource. The selected independent tests allow for a finer level of granularity of testing compared to the developer's testing, or provide additional testing of functions that were not exhaustively tested by the developer. The tests allow specific functions and functionality to be tested. The tests reflect knowledge of the TOE gained from performing other work units in the evaluation. The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests.

6.4. Evaluator Penetration Tests

The evaluators examined each of the obvious vulnerabilities identified during the developer’s vulnerability analysis. After consulting the sources identified by the developer used during the initial vulnerability analysis, the evaluator consulted other vulnerability relevant sources of information to verify that the developer considered all available information when developing the non-exploitation rationale. These additional sources include:

Table 11: Internet Web Site Vulnerability Searches

Site	Keywords Used for the Searches
http://www.kb.cert.org/vuls/	Xilinx VirtexII-Pro XC2VP30-6FF896C, Thales Element Manager, Thales Datacryptor, Senetas CypherNET SONET/SDH Encryptor (competing technology), Senetas CypherNET Ethernet (10/100 and 1 GbE) Encryptor (competing technology)
http://cve.mitre.org/cve/	Xilinx VirtexII-Pro XC2VP30-6FF896C, Thales Element Manager, Thales Datacryptor, Senetas CypherNET SONET/SDH Encryptor (competing technology), Senetas CypherNET Ethernet (10/100 and 1 GbE) Encryptor (competing technology)
http://nvd.nist.goNv/nvd.cfm	Xilinx VirtexII-Pro XC2VP30-6FF896C, Thales Element Manager, Thales Datacryptor, Senetas CypherNET SONET/SDH Encryptor (competing technology), Senetas CypherNET Ethernet (10/100 and 1 GbE) Encryptor (competing technology)

Site	Keywords Used for the Searches
http://www.securityfocus.com/bid	Xilinx VirtexII-Pro XC2VP30-6FF896C, Thales Element Manager, Thales Datacryptor, Senetas CypherNET SONET/SDH Encryptor (competing technology), Senetas CypherNET Ethernet (10/100 and 1 GbE) Encryptor (competing technology)

After verifying that the developer's analysis approach sufficiently included all of the necessary available information regarding the identified vulnerabilities, the evaluator made an assessment of the rationales provided by the developer indicting that the vulnerability is non-exploitable in the intended environment of the TOE.

While verifying the information found in the developer's vulnerability assessment the evaluators conducted a search to verify if additional obvious vulnerabilities exist for the TOE. Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerability.

The evaluator determined that the rationales provided by the developer indicate that the vulnerabilities identified are non-exploitable in the intended environment of the TOE.

6.5. Test Results

The end result of the testing activities was that all tests gave expected (correct) results. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to all the potential vulnerabilities identified by the evaluator. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities in the final evaluated version. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

7. EVALUATED CONFIGURATION

The evaluated configuration of the Thales e-Security Datacryptor SONET/SDH and Gigabit Ethernet with Element Manager Product, as defined in the Security Target, are shown in Figures 1 & 2 in Section 4.7.

8. RESULTS OF THE EVALUATION

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 2.3. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.3.

COACT CAFÉ Laboratory has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 3. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished February 2009. A final Validation Oversight Review (VOR) was held in March 2009 and final changes to the ST, ETR and VR were completed in April 2009.

9. VALIDATOR COMMENTS

The TOE developer and sponsor, and the Evaluation Team are commended for their effort in developing tests for the Thales e-Security Datacryptor SONET/SDH and Gigabit Ethernet with Element Manager. All test plans were clear, complete, and comprehensible.

The validation team would like to highlight the importance of using the product in accordance with all evaluated guidance documented in this report. In addition, the validation team notes the following:

- The Element Manager Host Platform TOE component must be installed on a PC running Microsoft NT, Windows 2000, or XP operating systems. Microsoft Vista is not a claimed operating system. The vendor did perform some tests with the Element Manager installed on a PC running Microsoft Vista, however, some issues were identified and the test results were unsuccessful.
- The cryptography used in this product has not been FIPS certified. It is only asserted by the CCTL that the cryptography is tested. No further claims are made.

10. SECURITY TARGET

Thales e-Security Datacryptor SONET/SDH with Element Manager and Gigabit Ethernet with Element Manager Security Target, Version 1.9 dated February 26, 2009.

11. GLOSSARY

Authentication: Verification of the identity of a user.

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.

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.

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.

Threat: Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.

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.

Vulnerabilities: A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

12. ACRONYM LIST

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CA	Certificate Authority
CAVP	Crytpographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
DEK	Data Encryption Key
DH ESK	Diffie-Hellman Encrypted Secret Key
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
IT	Information Technology
ITU	International Telecommunications Unit
KEK	Key Encryption Key
LAN	Local Area Network
NIAP	National Information Assurance Partnership
OC	Optical Carrier
PP	Protection Profile
RFC	Request for Comment
RIP	Routing Information Protocol
RTC	Real Time Clock
SDH	Syncronous Digital Hierarchy
SHA	Secure Hashing Algorithm
SHS	Secure Hashing Standard
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
SONET	Syncronous Optical NETwork
SPE	Synchronous Payload Envelope
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSFI	TSF Interface
TSP	TOE Security Policy
VC	Virtual Container
WAN	Wide Area Network

13. BIBLIOGRAPHY

1.) *Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model*, Version 2.3, dated August 2005, CCMB-2005-08-001

2.) *Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements*, Version 2.3, dated August 2005, CCMB-2005-08-002

3.) *Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements*, Version 2.3, dated August 2005, CCMB-2005-08-003

4.) *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, Version 2.3, dated August 2005, CCMB-2005-08-004

5.) *Guide for the Production of PPs and STs*, Version 0.9, dated January 2000

6.) T*hales e-Security Datacryptor SONET/SDH with Element Manager and Gigabit Ethernet with Element Manager Security Target*, Version 1.9 dated February 26, 2009

7.) CAFÉ Laboratory of COACT Incorporated, *Evaluation Technical Report for Thales e-Security Datacryptor SONET/SDH Release 4.0 with Element Manager and Thales e-Security Datacryptor Gigabit Ethernet Release 4.0 with Element Manager*, March 27, 2009, Document No. F3-0309-003