National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Ingrain Networks DataSecure Appliance i416, i426 and i116 Release 4.6.2

Report Number: CCEVS-VR-VID10282-2008

Dated: 20 May 2008

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

Mike Allen (Lead Validator)

Deborah Downs (Senior Validator)

Aerospace Corporation

Columbia, Maryland

El Segundo, California

Common Criteria Testing Laboratory

InfoGard Laboratories, Inc.

San Luis Obispo, California

Table of Contents

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 and any restrictions on the evaluated configuration. Prospective users should carefully read the Validator Comments in Section 10.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Ingrian Networks DataSecure Appliance i416, i426, and i116 Release 4.6.2, the target of evaluation (TOE), conducted by InfoGard Laboratories 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. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation by InfoGard was performed in accordance with the United States evaluation scheme and was completed in November 2007. The information in this report is largely derived from the ST, the Evaluation Technical Report (ETR) and the functional testing report. The ST was prepared by Ingrian Networks. 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 2 (EAL 2) augmented with the ALC_FLR.1 life cycle assurance requirements and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.3, August 2005. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the DataSecure Appliance Security Target.

The Ingrian DataSecure Appliance provides centralized encryption and security management for network web servers, application servers and databases. The TOE resides within the network and when network servers require sensitive data processing they communicate with the TOE appliance exclusively via an XML or XML-RPC interface. Note that XML-RPC is used to communicate with File Encryption (FE) agents in the IT environment. The Ingrian TOE receives encryption/decryption requests from network clients and provides the required cryptographic functions within the appliance itself.

For example, if a server required access to sensitive information, it would contact the TOE via the XML interface and request the decryption of specific data using a specific cryptographic key. If the request is fully authenticated, then the cryptographic processing is completed within the appliance and result returned only to the requesting server. Data is only passed between the TOE and the requesting server and data cannot pass from server to server through the TOE appliance. The plaintext keys never leave the TOE appliance as all processing is done internal to the TOE, except that the TOE can also provide cryptographic keys and key metadata to FE Agents in the IT environment.

Key creation and management also takes place within the appliance providing for better security and a dedicated platform to deploy security policies for the supported network. In addition, configuration data and settings can be backed up and later restored on a DataSecure Appliance.

The TOE includes three hardware options which provide scalability options but maintain the identical software suite and associated functionality:

1. Ingrian DataSecure Appliance i116 Hardware

VIA C3 800mhz CPU, 1GB RAM, 80GB SATA drive

This hardware platform is intended for smaller deployments. It features a single processor architecture and single hard drive resource and can process more than 11000 secure cryptographic operations per second.

2. Ingrian DataSecure Appliance i416 Hardware

Single Dual Core CPU, 1U Rack Mountable Chassis, 1GB RAM, 80 GB SATA drive

This hardware platform is intended for medium sized deployments. It features a single processor architecture and single hard drive resource and can process more than 35000 secure cryptographic operations per second.

3. Ingrian DataSecure Appliance i426 Hardware

Two Dual Core CPUs, 2U Rack Mountable Chassis, 1GB RAM, 2 80GB SATA in RAID configuration.

This hardware platform is intended for larger deployments. It features a dual processor architecture and dual hard drives in a RAID-1 mirroring configuration. The drives are hot swappable. This appliance can process more than 45000 secure cryptographic operations per second.

1.1. Hardware Components

Table 1: TOE Hardware Component List

TOE or Environment	Component	Description
TOE	Ingrian DataSecure Appliance *i*416 Hardware	TOE Hardware – Single Dual Core CPU, 1U Rack Mountable Chassis, 1GB RAM, 180 GB SATA drive
	Ingrian DataSecure Appliance *i*426 Hardware	TOE Hardware – Two Dual Core CPUs, 2U Rack Mountable Chassis, 1GB RAM, 2 80GB SATA in RAID configuration
	Ingrian DataSecure Appliance *i*116 Hardware	VIA C3 800mhz CPU, 1GB RAM, 80GB SATA drive
Environment	Web Management Console Machine	Remote PC or Laptop for admin access
Environment	Workstation	Workstation for SSH, Serial, CLI Access

Environment	Web Server/Web Application/ Database NAE Clients	NAE Clients accessing the TOE for Cryptographic Services
Environment	File Encryption Agent work station	File Encryption Agent software running on a workstation

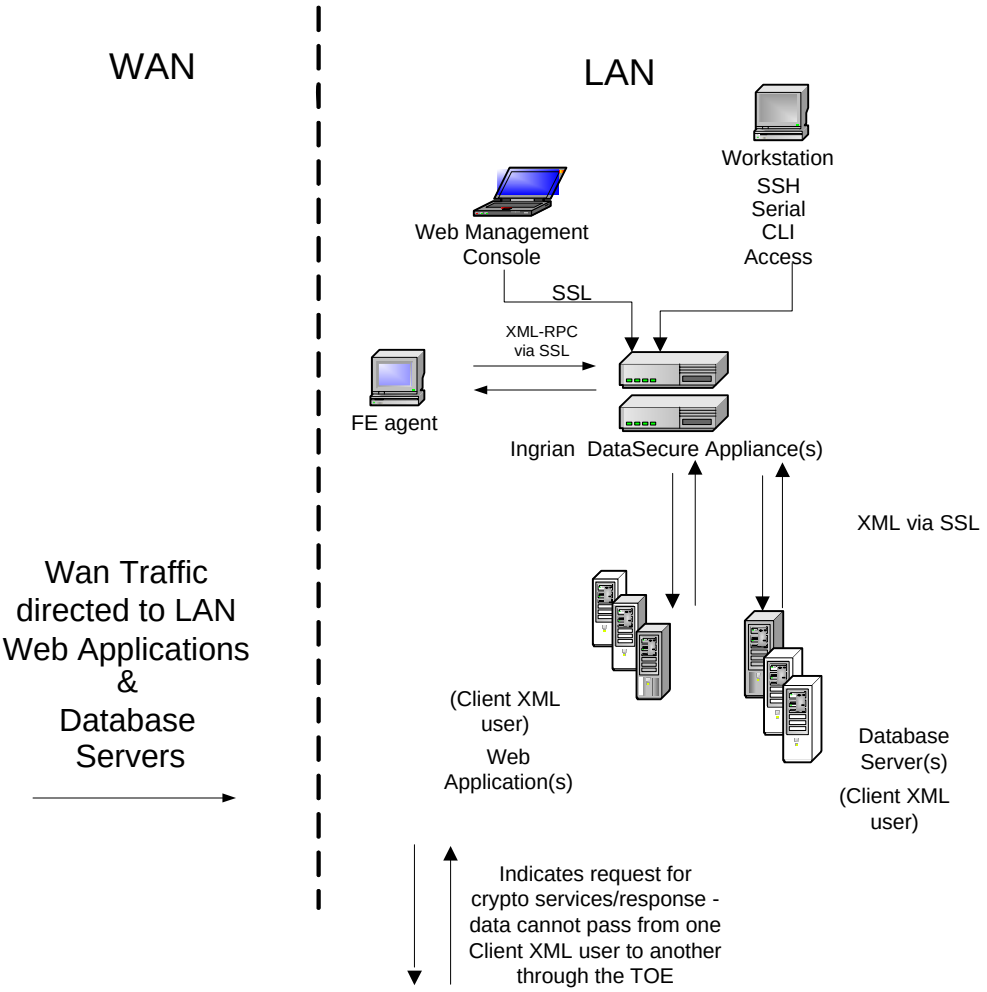

Figure 1: Typical TOE Architecture – Network Deployment

1.2. Software Components

Table 2: TOE Software Component List

TOE or Environment	Component	Description
TOE	Ingrian DataSecure software v 4.6.2	TOE application software (which includes the Linux CentOS v4.3 Operating System customized by Ingrian)
Environment	Microsoft Windows XP, Server 2003 (or) Unix/Linux any versions that support browsers listed below	Web Management Console Machine Operating System
Environment	Microsoft® Internet Explorer™, version 6.x and later (or) Netscape® Navigator™, version 7.1, Mozilla™, Firefox™	Web Management Console Machine Browser
Environment	Database NAE Clients	NAE Clients accessing the TOE for Cryptographic Services: Databases supported: IBM DB2, MS SQL Server, Oracle 8i, 9i, and 10g (or any device that can communicate XML over an SSL channel).
Environment	Web Server/Web Application NAE Clients	Supported: BEA, IBM, IIS, Oracle, Apache, SUN ONE, JBOSS (or any device that can communicate XML over an SSL channel).
Environment	File Encryption Agents	Client agent software (or any device that can communicate XML-RPC over an SSL channel)

1.3. Common Criteria Product Type

The TOE is a network appliance classified as a Sensitive Data Protection product for Common Criteria. The TOE includes both hardware and software components.

1.4. Logical Boundaries

The logical boundaries of the TOE are the product security features that are in the TOE. The following features are part of the logical boundary of the TOE:

- Identification and Authentication
- Cryptographic Services
- Audit
- Access Control
- Security Management
- Secure Communications

- Protection of the TOE

1.5. Features and Functions Excluded from the Evaluated TOE

It is important to note that the following components are excluded from the TOE. Use of these features or functions will negate the results of the evaluation and remove the product from the evaluated configuration.

- Global Keys
- Content Encryption keys and Service Engine
- Administrative options on XML interface
- FTP transport for importing certificates and downloading and restoring backup files
- LDAP authentication
- Use of the following algorithms: DES, RSA-512, RSA-768.
- XML user password management
- NAE User Administrator permission
- FTP cannot be used to import or export Certificates or Backup files
- Database Tools
- SQL parser server

1.6. Cryptographic Certifications

The following cryptographic algorithms that the TOE uses have been validated under FIPS 140-2:

Algorithm	Certificate Number
Triple-DES	565
AES	588
DSA	231
X9.31 PRNG	335
SHA	640
HMAC	306

The following cryptographic algorithms used by the TOE have not been FIPS 140-2 validated, however the vendor asserts that they operate correctly:

Algorithm
SEED
RC4

1.7. 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 Criteria Interpretations Management Board (CCIMB) are applicable to this evaluation. The TOE is also compliant with all International interpretations with effective dates on or before January 11, 2007.

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 3 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 3: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Ingrian Networks DataSecure Appliance i416, i426, and i116 Release 4.6.2
Protection Profile	None
Security Target	*Ingrian Networks© DataSecure Appliance i416, i426, and i116 Release 4.6.2 Security Target*, Version 1.8, May 7, 2008
Dates of evaluation	January 11, 2007 through November 2007
Evaluation Technical Report	*Evaluation Technical Report Ingrian Networks DataSecure Appliance i416, i426, i116 Release 4.6.2*, Version 1.2, April 29, 2008
Conformance Result	Part 2 and Part 3 conformant, EAL 2 + ALC_FLR.1
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 11, 2007
Common Evaluation Methodology (CEM) version	CEM version 2.3, August 2005 and all applicable NIAP and International Interpretations effective on January 11, 2007
Sponsor	Ingrian Networks, Inc., 350 Convention Way, Redwood City, CA 94063
Developer	Ingrian Networks, Inc., 350 Convention Way, Redwood City, CA 94063
Common Criteria Testing Lab	InfoGard Laboratories, Inc., 641 Higuera St., San Luis Obispo, CA 93401
Evaluators	Albert Chang of InfoGard Laboratories, Incorporated
Validation Team	Deborah Downs and Mike Allen of The Aerospace Corporation

3. SECURITY POLICY

The Security Functional Policies (SFPs) implemented by the Ingrian DataSecure Appliance provide a mechanism so that only the identified/authenticated administrator has access to TOE resources, provides accountability for actions by logging security events, and a protection mechanism that provides the security policies.

The Ingrian DataSecure Appliance performs the following security functions:

- Identification and Authentication
- Cryptographic Services
- Audit
- Access Control
- Security Management
- Secure Communications
- Protection of the TOE

4. ASSUMPTIONS AND CLARIFICATION OF SCOPE

4.1. Physical Security Assumptions

The following physical assumptions are identified in the Security Target:

Table 4 – Physical Assumptions

A. LOCATE	The TOE and IT Environment is located in a physically secure location with limited access and will be protected from unauthorized physical modification. Additionally, the machines that host the web browser are free from Malware.

4.2. Personnel Security Assumptions

The following personnel assumptions are identified in the Security Target:

Table 5 – Personnel Assumptions

A. ADMIN	The administrators are appropriately trained, not careless, not willfully negligent, non hostile and follow and abide by the instructions provided in the guidance documentation.

4.3. Operational Security Assumptions

The following operational security assumptions are identified in the Security Target:

Table 6 – Physical Assumptions

A. USE	The Ingrian Appliance is dedicated to its primary function and does not provide any general purpose computing or storage capabilities.

4.4. Threats Countered and Not Countered

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

Table 7 – Threats Countered

T. SEC_FUNC	Administrators may make changes to TOE security functionality without accountability.
T.MASK	An unauthorized user may masquerade as an authorized user or an authorized IT entity to gain access to data or TOE resources.
T.COMP_MANAGE	Data may be compromised while traversing the connection between the TOE components.

T.NO_ACCOUNT	An administrator might perform actions for which they are not accountable.
T.POLICY_VIOLATE	An attacker gains unauthorized use of the network by broadcasting wireless network traffic in violation of the Allowable Use Policies, without being detected.
T.SEC_BYPASS	The TOE might be subjected to malicious tampering or bypass of its security mechanisms.

4.5. Organizational Security Policies

There are no applicable organizational security policies.

4.6. Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- The Command Line Interface (CLI) is used only during the installation, initial configuration of the TOE and troubleshooting problems. Exchanges with the TOE over the CLI are not encrypted or protected, therefore the TOE and CLI terminal should only be used in a protected environment in accordance with the A.LOCATE assumption.

- The following functions and features of the DataSecure Appliance were not evaluated and should not be used in the evaluated configuration:

    - Global Keys
    - Content Encryption keys and Service Engine
    - Administrative options on XML interface
    - FTP transport for importing certificates and downloading and restoring backup files
    - LDAP authentication
    - Use of the following algorithms: DES, RSA-512, RSA-768.
    - XML user password management
    - NAE User Administrator permission
    - FTP cannot be used to import or export Certificates or Backup files
    - Database Tools
    - SQL parser server

The following cryptographic algorithms used by the TOE have not been FIPS 140-2 validated, however the vendor asserts that they operate correctly. Users of the product should consider this lack of FIPS certification for these algorithms when using this product.

Algorithm
SEED
RC4

5. ARCHITECTURAL INFORMATION

5.1. Functional Architecture

The Ingrian Appliance system architecture is divided into the following sections in this discussion:

- Management Console
- Command Line Interface (CLI)
- Admin Library
- Crypto Engine
- NAE Server
- File Encryption
- Ingrian Operating System

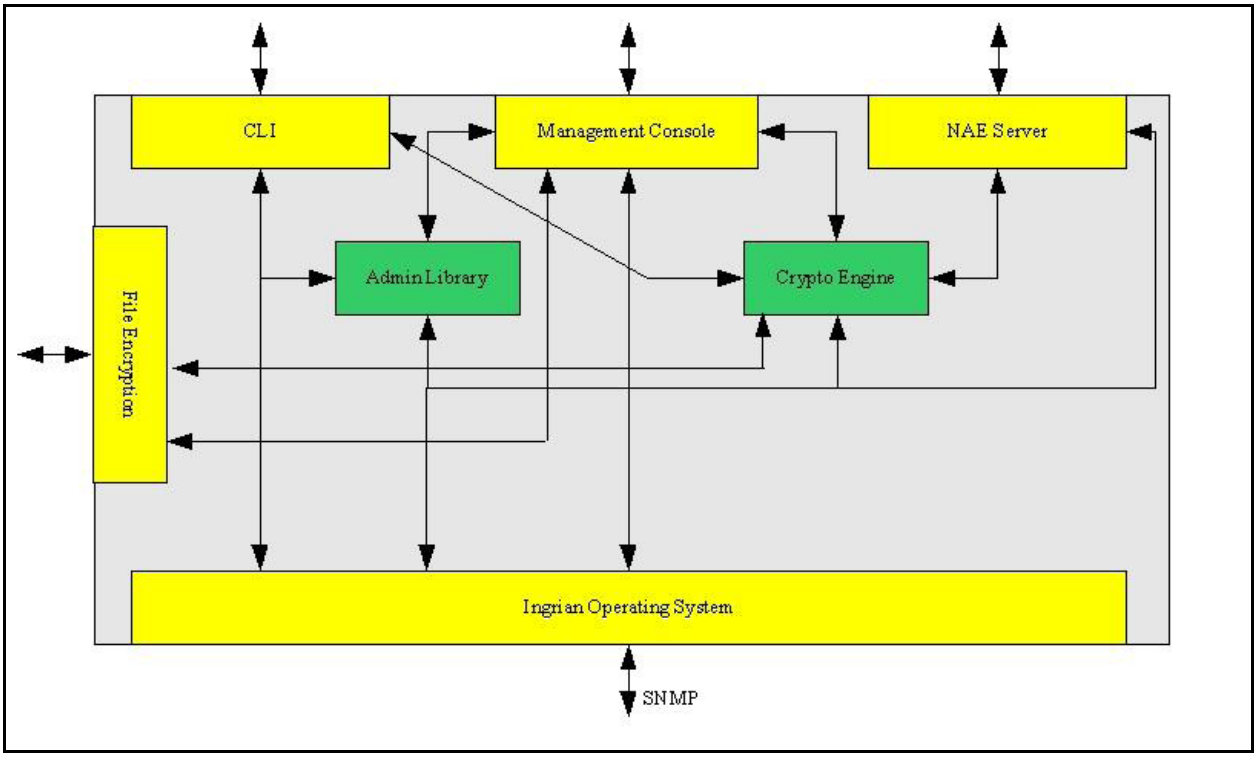

Figure 2: TOE Internal Architecture

5.1.1. Management Console

The Management Console provides the primary identification and authentication of administrator access to the TOE through a GUI based interface into the Ingrian TOE appliance. This allows administrators to access the appliance through a web console machine in the IT Environment using a standard web browser component. Management sessions through the management console are secured using SSL/TLS.

This subsystem also provides the appliance administrative functionality which allows administrators to configure the appliance, establish Client XML & Administrator accounts and create and configure security policies enforced by the appliance.

5.1.2. Command Line Interface (CLI)

The command line interface provides a subset of the functionality provided by the management console through CLI commands for both remote and local management. Administrators must establish an SSH encrypted tunnel and be authenticated by the Management Console in order to gain remote access to the TOE. The CLI is also used for local connection to the appliance through the serial connector, typically during installation and initial configuration activities.

5.1.3. Admin Library

The Admin Library interfaces with the Pluggable Authentication Module (PAM) within the Ingrian Operating System to authenticate TOE Administrators and to determine the role associated with that Administrator.

The Admin Library generates the Audit log. The Audit log is one of many logs that the Ingrian appliance generates and contains records of all configuration changes and Administrator input errors made to the Ingrian TOE, whether through the Management Console or the CLI.

The Admin Library maintains the configuration information and security policy details that define which network resource can access which key resources. The Administrator-established rules are stored by the Admin Library and these rules are accessed to validate key operation requests. The Admin Library also processes commands and input sent through both the Management Console and CLI.

5.1.4. Crypto Engine

The Ingrian Crypto Engine provides all cryptographic operations for the Ingrian TOE appliance. Operations include key generation, encryption and decryption of content, and key destruction. Requests for processing are received from the NAE Server or from Administrative functions (e.g. creating keys) through the Admin Library.

The Crypto Engine is a logical grouping of the following components: ICS, libcrypto, libssl and IKM.

The Ingrian Cryptographic Services (ICS) represents the essential set of code which implements the Crypto Engine subsystem functionality in association with the libcrypto and libssl libraries. The Ingrian Key Manager (IKM) provides key management services for the Crypto Engine subsystem.

5.1.5. NAE Server

The NAE Server subsystem interfaces with the Ingrian Crypto Engine to coordinate cryptographic key creation, management, and data encrypt/decrypt actions. In addition, the NAE Server processes all Client XML user requests through its XML interface and provides NAE Server log records for related events.

The NAE Server subsystem orchestrates initial Client XML user identification and authentication to the TOE and subsequently directs access control functions to specific TOE resources when requested by Client XML users.

5.1.6. File Encryption

The File Encryption Subsystem provides the external interface for providing keys and key metadata to file encryption (FE) client agents. It presents an XML RPC interface in which certificate based authenticated FE client agents can request and receive keys and key metadata. It should be noted that this subsystem does not perform or implement cryptographic operations (i.e. cryptographic services); it simply passes a key and key metadata when requested by an authenticated FE agent.

5.1.7. Ingrian Operating System

The underlying operating system for the appliance is based on a Linux CentOS version 4.3 and supports the operation of the aforementioned TOE subsystems. The Operating System is tailored to support the overall functionality of the Ingrian DataSecure appliance.

The Ingrian TOE Operating System includes a Pluggable Authentication Module (PAM). The pluggable authentication module running under the Ingrian Operating System is a suite of shared libraries that enable the TOE administrator to configure how Administrators authenticate to the appliance. PAM allows separation of the authentication function from the base operating system tailored on supporting cryptographic processing. Note that keys generated by the TOE Administrator for FE Agents cannot be accessed before the authentication process and setup of the SSL tunnel has been established.

5.1.8. Statement of Non-Bypassibility of the TSF

TOE security functions cannot be bypassed. All access to TOE security management functions requires Administrator level access to the TOE. Access to NAE Server resources for cryptographic operations requires identification and two factor authentication by the TOE for Client XML users. GUI access is only allowed via a standard web browser through the dedicated management interface on the TOE and is secured through the use of SSL/TLS.

Administrator access is authenticated through the underlying operating system on the appliance. CLI access to the TOE is only allowed via a properly authenticated SSH session.

5.2. TOE Boundaries

This section lists the hardware and software components of the product and denotes which are in the TOE and which are in the environment. Figure 3 shows the hardware used in a typical deployment of the TOE and indicates which devices are considered part of the TOE and which are considered in the environment.

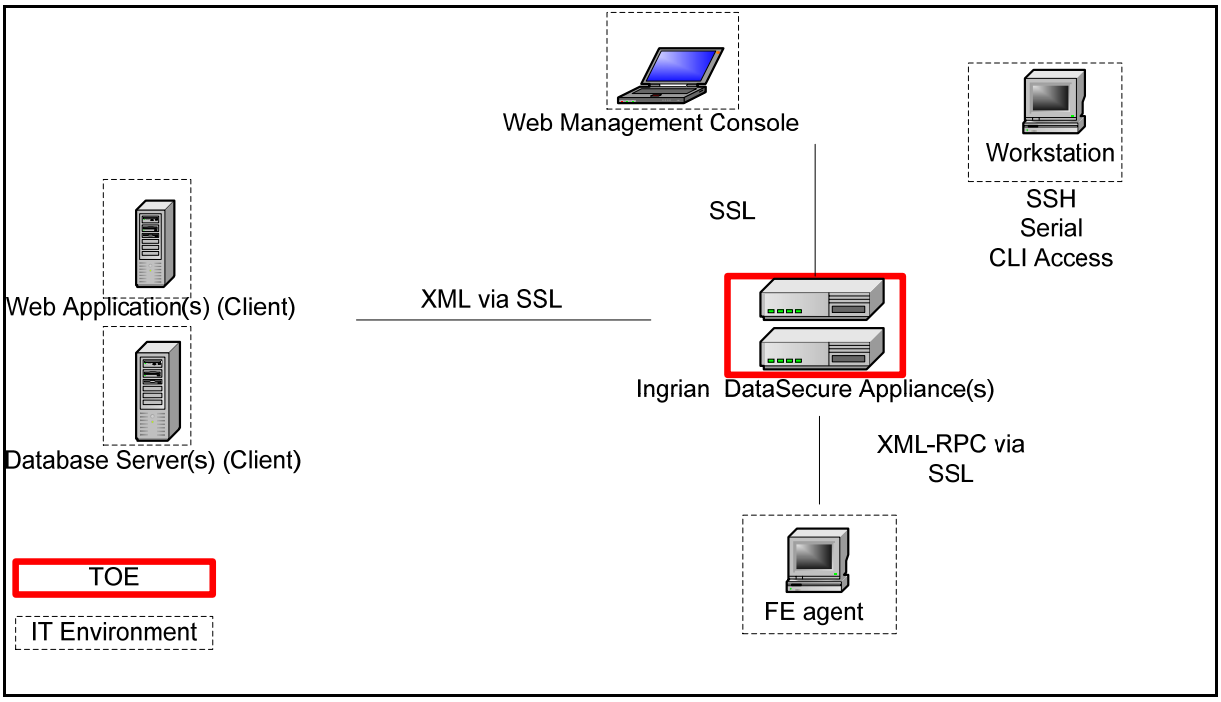

Figure 3: Physical Boundaries

In terms of logical boundaries, Table 6 enumerates the division between services provided *by* the TOE. The TOE itself does not rely on any services provided by the operating environment.

Table 8: TOE Security Functions

Functional Area	Services Provided *By* The TOE	Services Provided *To* The TOE By The Operating Environment
ID and Authentication	The Ingrian TOE requires that all users (Administrators/Client XML users/FE agents) of the TOE are identified and authenticated prior to accessing TSF resources save for the following: Client XML users may poll the appliance for status information (i.e. whether the cryptographic services are running and accepting connections), Administrators may initiate a secure session via the CLI or Management interface over SSH or SSL/TLS respectively and Client XML users may negotiate version information with the TOE via the XML interface prior to identification and authentication. All other access to the TOE and TSF resources requires positive identification and authentication prior to accessing TSF resources.	None
Cryptographic Services	The Cryptographic Services security function provides the essential cryptography functionality for the Ingrian TOE. This includes certificate creation, encryption of administrator sessions via the GUI or CLI interfaces and the key generation, key management and encryption/decryption of client data. This functionality is provided by the Crypto Engine subsystem.	None
Audit	The Ingrian TOE appliance has a comprehensive logging capability to generate audit records for all TSF configuration/changes, administrator access to the appliance, Client XML user access, FE agent access and cryptographic services request and provided to clients. Access to log records requires that Administrator use	None

	be identified and authenticated by the Management Console or CLI subsystem prior to access.	
Access Control	The Access Control functions provide access restrictions to the TOE to assure that only authorized administrators can access TOE TSF resources. All access to TSF Security Management functions (via the Management Console and CLI subsystem) requires Identification and Authentication by the appliance prior to granting access. In addition, the TOE supports role based access to specify which categories of resources may be accessed by a range of authorized Administrators. For the Common Criteria Evaluated Configuration, the TOE supports two user roles: Administrator and Client XML user. A third role, the FE agent, exists. However, these access control mechanisms do not apply in the same manner. Once a FE user is successfully authenticated, their certificate is used to determine the cryptographic key and key metadata that are passed to the FE agent.	None
Security Management	Security Management is managed by authorized Administrators utilizing the Ingrian Management Console subsystem through the Web Management Console machine GUI or through the CLI interface. In all cases, Administrators must be properly identified and authenticated by the TOE prior to granting access to Security Management functions and TSF resources.	None
Secure Communications	Secure Communication practices are utilized in the TOE for administrator access via SSL/TLS for access to the appliance GUI via a Web Console machine browser. CLI access to TOE resources requires SSHv2 to be utilized.	None
Protection of TOE	Physical and logical protection of the TOE ensures that TOE related security	None

	functions are not bypassed or altered. This is provided by the TOE and Operating System Environment and through the secure communication methods described in the Ingrian OS Users Guide.	

6. DOCUMENTATION

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Ingrian DataSecure Appliance. Note that not all evidence is available to customers.

The TOE is physically delivered to the end User. The guidance is part of the TOE components and is delivered with the TOE on CD labeled "Documentation CD" (bold document titles refer to documentation that is provided to the end user).

6.1. Design documentation

Document	Revision	Date
Ingrian Network DataSecure Appliance i416, i426, and i116 Release 4.6.2 High Level Design	5.0	3/3/2008
Ingrian Networks DataSecure Appliance i416, i426, and i116 Release 4.6.2 Functional Specification	7.0	4/23/2008
Ingrian Networks DataSecure Appliance i416, i426, i116 Release 4.6.2 Correspondence Representation	3.0	2/25/2008

6.2. Guidance documentation

Document	Revision	Date
IngrianOS User Guide	20080226	2/26/08
Ingrian File System Connector User Guide	4.5	5/2007
NAE Developer Guide for the XML Interface	1.4	12/2006
Quick Start Guide Ingrian DataSecure 400 Series, i416, i426	ING-QSG-i416/i426-10-2007	10/2007
Quick Start Guide Ingrian i116 DataSecure Platform	ING-QS-i116-2007-07	07/2007

6.3. Configuration Management and Lifecycle

cument	Revision	Date
Ingrian Networks DataSecure Appliance i416, i426, and i116 Release 4.6.2 Configuration Management	4.0	3/3/08

6.4. Delivery and Operation documentation

Document	Revision	Date
Ingrian Networks DataSecure Appliance i416, i426, and i116 Release 4.6.2 Secure Delivery	2.0	9/11/2007

6.5. Test documentation

Document	Revision	Date
Ingrian Networks DataSecure Appliance i416, i426, and i116 Release 4.6.2 EAL Independent Test Plan (ATE_IND.2)	1.1	3/3/2008
Ingrian Networks DataSecure Appliancei416, i426, and i116 Release 4.6.2 Test Plan	4.0	9/20/07

6.6. Vulnerability Assessment documentation

Document	Revision	Date
Ingrian Networks Data Secure Appliance i416, i426, and i116 Release 4.6.2 Vulnerability Assessment	3.0	10/1/07

6.7. Security Target

Document	Revision	Date
Ingrian Networks DataSecure Appliance i416, i426, and i116 Release 4.6.2 Security Target	1.8	5/7/08

7. IT PRODUCT TESTING

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

7.1. Developer testing

The test procedures were written by the Developer and designed to be conducted using manual interaction with the TOE interfaces. During the evaluation of the ATE_FUN.1, the evaluation team identified inconsistencies in the test cases and worked with the Developer to create accurate test cases.

The Developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The Developer's approach to testing is defined in the TOE Test Plan. The expected and actual test results (ATRs) are also included in the TOE Test Plan. 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 2. The evaluation team determined that the Developer's actual test results matched the Developer's expected test results.

7.2. Evaluation Team Independent Testing

The evaluation team conducted independent testing at the CCTL. The evaluation team installed the TOE according to vendor installation instructions and established the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE while performing work unit ATE_IND.2-2. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Developer's Test Plan as a basis for creating the Independent Test Plan. The evaluation team analyzed the Developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions that implement critical security features
- Security functions critical to the TOE's security objectives
- Security functions that gave rise to suspicion regarding the behavior of the security features during the documentation evidence evaluation
- Security functions not tested adequately in the vendor's test plan and procedures

The following TOE Security Functions were added to the Security Target to better enumerate the security functions provided by the TOE after the FVOR. Because the TOE is being evaluated at the EAL2 level of assurance, completing testing of all TOE SFRs is not required. As such, the following SFRs have not been tested by the Developer OR the Evaluation Team.

- FIA_AFL.1 Authentication Failure
- FCS_CER.EXP.1 Certificate Generation
- FCS_CER.EXP.2 Certificate Import
- FCS_CER.EXP.3 Certificate Export
- FCS_CER.EXP.4 Certificate Request Generation
- FCS_CKM.EXP.2a Cryptographic key export – XML Users
- FCS_CKM.EXP.2b Cryptographic key export – FE Agent
- FCS_CKM.EXP.5 Cryptographic key import – Administrator
- FCS_INF.EXP.1 Cryptographic Key Information Query
- FCS_POL.EXP.1 Cryptographic Authorization Policy
- FDP_MEM.EXP.1 XML user group membership query
- FDP_BAU.EXP.1 Backup File Import

The evaluation team reran 100% of the Sponsor's test cases and specified additional tests. The additional test coverage was determined based on the analysis of the Developer test coverage and the ST.

Each TOE Security Function was exercised at least once (except for the SFRs listed above) and the evaluation team verified that each test passed.

Table 9: Vendor Test List

Test ID	Security Function	Test Description	Applicable SFR	Applicable TSFI
Vendor Tests				
TC-1	Identification and Authentication	The goal of this test is to test the Identification and Authentication, Cryptographic Services and Protection of the TOE security functions to ensure	FIA_SOS.1.1 FMT_SMF.1.1	Management Console Interface

Test ID	Security Function	Test Description	Applicable SFR	Applicable TSFI
		that they behave as designed and implemented.		
TC-2	Identification and Authentication	The goal of this test is to test the Identification and Authentication security function to ensure that it behaves as designed and implemented.	FIA_UID.1 FIA_UAU.1	Management Console Interface
TC-3	Cryptography, Identification and Authentication	The goal of this test is to test the Cryptographic Services ensure that they behave as designed and implemented.	FMT_SMF.1.1 FMT_MTD.1.1a FCS_CKM.EXP.5	Management Console Interface
TC-4	Secure Communication	The goal of this test is to verify the secure communication function over the CLI interface.	FCS_COP.1	Command Line Interface
TC-5	Access Control, Security Management	The goal of this test is to test the Access Control security function to ensure that they behave as designed and implemented.	FDP_ACC.1b	Management Console Interface
TC-6	Identification and Authentication	The goal of this test is to test the Identification and Authentication security function to ensure that it behaves as designed and implemented.	FIA_UID.1 FIA_UAU.1	Command Line Interface

Test ID	Security Function	Test Description	Applicable SFR	Applicable TSFI
TC-7	Secure Communication	The goal of this test is to test the Secure Communication security function to ensure that it behaves as designed and implemented.		XML Interface
TC-8	Security Management	To verify the administrator access control functions over the Management Console Interface.	FDP_ACC.1b FDP_ACF.1b	Management Console Interface
TC-9	Security Management	To verify the Security Management functions over the Command Line Interface.	FMT_SMF.1.1 FMT_SMR.1	Command Line Interface
TC-10	Security Management	To verify the Cryptographic Services functions over the File Encryption Interface.	FAU_GEN.2.1 FAU_SAR.1.1 FAU_SAR.1.2 FAU_GEN.EXP.1	Management Console Interface, File Encryption Interface
TC-11	Secure Communication	To verify the Identification and Authentication and secure communication functions over the File Encryption Interface.	FSC_COP.1	Management Console Interface, File Encryption Interface

Table 10: Lab Independent Test List

Independent Functional Testing				
IGL_FAU-101	Audit	This test will verify that every type of audit data can be traced back to the "owner" of the event.	FAU_GEN.2.1	Management Console Interface
IGL_FAU-102	Audit	This test will verify that the TOE does not allow audit record deletion and that the TOE will overwrite the oldest stored audit records and forward an email notification to the TOE Administrator if the audit trail is full.	FAU_STG.1.1, FAU_STG.4.1	Management Console Interface
IGL_FAU-103	Audit	This test will verify that the TOE audits the modification or deletion of Client XML key data.	FAU_GEN.EXP.1.2, FMT_MTD.1a, FMT_SMF.1	Management Console Interface
IGL_FAU-104	Audit	This test will verify that the TOE audits the modification or deletion of SSL/TLS certificate data.	FAU_GEN.EXP.1.2, FMT_MTD.1a, FMT_SMF.1	Management Console Interface
IGL_FAU-105	Audit	This test will verify that the TOE audits the modification or deletion of Client XML user password.	FAU_GEN.EXP.1.2, FMT_MSA.1 FMT_SMF.1	Management Console Interface
IGL_FAU-106	Audit	This test will verify that the TOE audits the creation, modification or deletion of Administrator roles.	FAU_GEN.EXP.1.2, FMT_MTD.1a, FMT_SMF.1,	Management Console Interface

			FMT_SMR.1	
IGL_FAU-107	Audit	This test will verify that the TOE audits the export of cryptographic keys.	FAU_GEN.EXP.1.2, FCS_CKM.EXP.2.1a, FCS_CKM.EXP.2.1b, FMT_SMF.1	Management Console Interface
IGL_FAU-108	Audit	This test will verify that the TOE audits the failure of identification and authentication through the Management Console Interface.	FAU_GEN.EXP.1.2, FIA_UAU.1, FIA_UID.1	Management Console Interface
IGL_FAU-109	Audit	This test will verify that the TOE audits the failure of identification and authentication through the Command Line Interface.	FAU_GEN.EXP.1.2, FIA_UAU.1, FIA_UID.1	Management Console Interface
IGL_FAU-110	Audit	This test will verify that the TOE audits the failure of identification and authentication through the XML Interface.	FAU_GEN.EXP.1.2, FIA_UAU.1, FIA_UID.1	Command Line Interface
IGL_FCS-101	Secure Communication	This test will verify that the TOE will not be able to support https connections via SSL 2.0 and SSL 3.0.		Management Console Interface
IGL_FCS-102	Cryptography	This test will verify that the TOE is able to perform Encrypt/Decrypt operations through	FCS_COP.1.1	XML Interface

		the XML Interface with TDES.		
IGL_FCS-103	Cryptography	This test will verify that the TOE is able to perform Encrypt/Decrypt operations through the XML Interface with AES.	FCS_COP.1.1	XML Interface
IGL_FCS-104	Cryptography	This test will verify that the TOE is able to perform Encrypt/Decrypt operations through the XML Interface with RC4.	FCS_COP.1.1	XML Interface
IGL_FCS-105	Cryptography	This test will verify that the TOE is able to perform Encrypt/Decrypt operations through the XML Interface with SEED.	FCS_COP.1.1	XML Interface
IGL_FCS-106	Cryptography	This test will verify that the TOE is able to perform Encrypt/Decrypt operations through the XML Interface with RSA.	FCS_COP.1.1	XML Interface
IGL_FCS-107	Cryptography	This test will verify that the TOE is able to perform hash operations through the XML Interface with HMAC-SHA1.	FCS_COP.1.1	XML Interface
IGL_FCS-108	Cryptography	This test will verify that the TOE is able to perform Sign/Verify operations through	FCS_COP.1.1	XML Interface

		the XML Interface with RSA.		
IGL_FIA-101	Identification and Authentication	This test will verify that the operator can only poll the system status, initiate SSH sessions, initiate SSL/TLS, and negotiate XML versions with the TOE before authenticating.	FIA_UAU.1.1 FIA_UID.1.1	Management Console Interface, Command Line Interface, XML Interface, File Encryption Interface
IGL_FIA-102	Identification and Authentication	This test will verify that the Client XML user must be identified and authenticated before it can request from the TOE.	FIA_UAU.1.1 FIA_UID.1.1	XML Interface
IGL_FIA-103	Identification and Authentication	This test will verify that the TOE Administrator must be identified and authenticated in order to access the TOE management functions via Web Console and Command line interface.	FIA_UAU.1.1 FIA_UID.1.1	Command Line Interface Management Console Interface
IGL_FMT-101	Security Management	This test will verify that the TOE administrator can manage the TOE users.	FMT_SMR.1.1 FMT_SMF.1.1	Management Console Interface
IGL_FMT-102	Security Management	This test will verify that the TOE administrator can create keys, certificates, and manage usage	FMT_SMF.1.1	Management Console Interface

		through the Management Console Interface.		
IGL_FMT-103	Security Management	This test will verify that the TOE administrator can create keys, certificates, and manage usage through the Command Line Interface.	FMT_SMF.1.1	Command Line Interface
IGL_FMT-104	Security Management	This test will verify that the TOE administrator can change and set permissions between Administrators/Client XML users, groups, and keys.	FMT_SMF.1.1	Management Console Interface
IGL_FMT-105	Security Management	This test will verify that the TOE administrator can modify the TOE Appliance's internal clock.	FMT_SMF.1.1	Management Console Interface

Table 11: Lab Penetration Test List

Independent Penetration Testing				
IGL_PEN-101		This test will attempt to inject various length passwords and observe if the TOE handles each correctly through the Management Console Interface.		Management Console Interface
IGL_PEN-102		This test will attempt to change the TOE's date and time to the maximum values (12/31/2020 23:59:59) and observe the result.		Management Console Interface

7.3. Vulnerability Analysis

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 evaluation team's Vulnerability Analysis, and the evaluation team's performance of penetration tests.

The Developer performed a Vulnerability Analysis of the TOE to identify any obvious vulnerabilities in the product and to show that they are not exploitable in the intended environment for the TOE operation. In addition, the evaluation team conducted a sampling of the vulnerability sites claimed by the Sponsor to determine the thoroughness of the analysis.

Based on the results of the Developer's Vulnerability Analysis, the evaluation team devised penetration testing to confirm that the TOE was resistant to penetration attacks performed by an attacker with an expertise level of unsophisticated. The evaluation team conducted testing using the same test configuration that was used for the independent team testing. In addition to the documentation review used in the independent testing, the team used the knowledge gained during independent testing to devise the penetration testing. This resulted in a set of three penetration tests.

8. EVALUATED CONFIGURATION

The evaluated configuration of the Ingrian DataSecure Appliance, as defined in the Security Target, consists of the several components. Please refer to Tables 1 and 2 for the TOE's hardware and software components.

The Ingrian DataSecure Appliance must be configured in accordance with the following Guidance Documents:

- IngrianOS User Guide, Version 20080226

.

9. 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.

The InfoGard Laboratories, Inc. Common Criteria Testing Laboratory has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 2 augmented with ALC_FLR.1. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished in November 2007. A final passing Validation Oversight Review (VOR) was completed on April 4, 2008.

10. VALIDATOR COMMENTS

The validation team's observations support the evaluation team's conclusion that the DataSecure Appliance Release 4.6.2 product meets the claims stated in the Security Target. The validation team also wishes to add the following notations about the use of the product.

The TOE makes use of cryptographic modules in order to fulfill some security functions. Cryptographic modules are evaluated under the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2, a separate standard from the Common Criteria. The cryptographic functions were not evaluated further during this evaluation. Users should ensure that they select a product that meets their needs, including FIPS 140-2 compliance, if appropriate.

The following cryptographic algorithms used by the TOE have not been FIPS 140-2 validated, however the vendor asserts that they operate correctly. Users of the product should consider this lack of FIPS certification for these algorithms when using this product.

Algorithm
SEED
RC4

The Command Line Interface (CLI) is used only during the installation, initial configuration of the TOE and troubleshooting problems. Exchanges with the TOE over the CLI are not encrypted or protected, therefore the TOE and CLI terminal should only be used in a protected environment in accordance with the A.LOCATE assumption.

11. ANNEXES

None

12. SECURITY TARGET

The security target for this product's evaluation is *Ingrian Networks© DataSecure Appliance i416, i426, and i116 Release 4.6.2 Security Target*, Version 1.8, May 7, 2008.

13. GLOSSARY

Client XML users	Used to denote the non-human client users of the TOE within the network, i.e. Network Server & Database clients accessing the TOE for cryptographic services. Throughout the TOE documentation this user is also referred to as NAE Client and NAE Client Connector.
Administrative Users	Used to denote (the sole) human users of the TOE which are limited to Appliance Administrators.
Server certificates	These certificates allow an Ingrian device to authenticate itself to a client application (Client XML users and FE agents) during an SSL handshake.
Client certificates	These certificates allow client applications (Client XML users and FE agents) to authenticate themselves to the Ingrian device during an SSL handshake.
FE Agents	Used to denote the non-human client users of the TOE within the network, i.e. FE agent software running on a workstation accessing the TOE for cryptographic keys and key metadata. Throughout the TOE documentation, the FE agent is also referred to as the file system connector.

14. BIBLIOGRAPHY

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

1. *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model*, dated August 2005, Version 2.3.
2. *Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements*, dated August 2005, Version 2.3.
3. *Common Criteria for Information Technology Security Evaluation – Part 2: Annexes*, dated August 1999, Version 2.1.
4. *Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements*, dated August 2005, Version 2.3.
5. *Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model*, dated 1 November 1998, version 0.6.
6. *Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology*, dated August 2005, version 2.3.
7. *Evaluation Technical Report Ingrian Networks DataSecure Appliance i416, i426, and i116 Release 4.6.2, Document ID: 07-1212-R-0106* Version 1.2, April 29, 2008
8. *Ingrian Networks DataSecure Appliance i416, i426, and i116 Release 4.6.2 Security Target*, Version 1.8, May 7, 2008.
9. *Ingrian Networks DataSecure Appliance i416, i426, and i116 Release 4.6.2 Functional Specification*, Version 7.0, April 23, 2008.
10. *Ingrian Networks DataSecure Appliance i416, i426, and i116 Release 4.6.2 EAL 2 Independent Test Plan (ATE_IND.2)*, Version 1.1, March 3, 2008.
11. Ingrian FVOR II Report, VID100282-FVOR-0005, April 22, 2008.
12. *NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories*, Version 1.0, March 20, 2001