Ingrian Networks DataSecure Appliance i416, i426, and i116 Release 4.6.2

Security Target

May 7, 2008

Version: 1.8

Prepared by:

Ingrian Networks

350 Convention Way

Redwood City, CA 94063-1405

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), conformance claims, ST organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 Identification

TOE Identification:	Ingrian Networks DataSecure Appliance i416, i426, and i116 Release 4.6.2[1]
ST Identification:	Ingrian Networks© DataSecure Appliance i416, i426, and i116 Release 4.6.2 Security Target EAL 2 + ALC_FLR.1
ST Version:	1.8
ST Publish Date:	05/07/08
ST Authors:	Shawn Fitzgerald (Ingrian Networks)
PP Identification:	N/A

1.2 CC Conformance Claim

The TOE is Common Criteria (CC) Version 2.3[2] Part 2 extended.

The TOE is Common Criteria (CC) Version 2.3 Part 3 conformant at EAL2 augmented ALC_FLR.1

The TOE is also compliant with all International interpretations with effective dates on or before 01/11/07.

The TOE is compliant with selected NIAP Interpretations. The selected NIAP Interpretations are identified as they are applied to the security requirements in Section 5.

This TOE is not conformant to any Protection Profiles (PPs).

1.3 Overview

The Ingrian DataSecure Appliance i416, i426, and i116 Release 4.6.2 is a scalable network security appliance that provides a centralized approach to cryptographic processing, key

[1] Throughout this document, the Ingrian Networks DataSecure Appliance i416, i426, and i116 version 4.6.2 will be referred to collectively as “the DataSecure”, unless discussing differences between specific versions. In this case, the product being discussed will be called “DataSecure Appliance i416”, “DataSecure Appliance i426”, or ”DataSecure Appliance i116”, whichever is appropriate. The TOE will be referred to as “the DataSecure TOE” or simply, “the TOE”. The ST may also be referred to as the “DataSecure ST”, or simply “the ST”.

[2] Common Criteria (CC) for Information Technology Security Evaluation – CC v2.3/CEM v1.3 (August 2005),.

management and security management/policy deployment. When cryptographic processing services are required by web servers or databases served by the DataSecure appliance, they submit XML based requests to the Appliance. The cryptographic operation is completed following authentication within the DataSecure appliance and the encryption or decryption results are returned to the server. This allows the DataSecure Appliance to offload backend application servers from processor intensive cryptographic operations by providing intelligently applied cryptographic services. The DataSecure Appliance delivers this functionality through a dedicated hardware appliance, containing a resident Network Attached Encryption (NAE) Server which communicates with Network Server and Databases exclusively over an SSL/TLS [3] secured XML interface.

1.4 Organization

Section	Title	Description
1	Introduction	Provides an overview of the security target.
2	TOE Description	Defines the hardware and software that make up the TOE, and the physical and logical boundaries of the TOE.
3	TOE Security Environment	Contains the threats, assumptions and organizational security policies that affect the TOE.
4	Security Objectives	Contains the security objectives the TOE is attempting to meet.
5	IT Security Requirements	Contains the functional and assurance requirements for this TOE.
6	TOE Summary Specification	A description of the security functions and assurances that this TOE provides.
7	PP Claims	Protection Profile Conformance Claims
8	Rationale	Contains pointers to the rationales contained throughout the document.

Table 1: ST Organization and Description

[3] Throughout this document SSL and TLS are used interchangeable. The evaluated configuration of the TOE only allows SSL v3.1 and/or TLS v1.0. These are in fact the same protocols.

1.5 Document Conventions

The CC defines four operations on security functional requirements. The conventions below define the conventions used in this ST to identify these operations. When NIAP interpretations are included in requirements, the additions from the interpretations are displayed as refinements.

Assignment: **indicated with bold text**

Selection: indicated with underlined text

Refinement: ***additions indicated with bold text and italics***

deletions indicated with strike-through ~~bold text and italics~~

Iteration: indicated with typical CC requirement naming followed by a lower case letter for each iteration (e.g., FMT_MSA.1a)

The explicitly stated requirements claimed in this ST are denoted by the ".EXP" extension in the unique short name for the explicit security requirement.

1.6 Document Terminology

Please refer to CC Part 1 Section 2.3 for definitions of commonly used CC terms.

1.6.1 ST Specific Terminology

Client XML users	Used to denote the non-human client users of the TOE within the network (i.e. Network Server & Database clients access 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 file system connector.

1.6.2 Acronyms

ICS	Ingrian Cryptographic Services
IKM	Ingrian Key Manager
OS	Operating System
SSL	Secure Socket Layer
TLS	Transport Layer Security
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol (Secure)
NAE	Network Attached Encryption
PRNG	Pseudo Random Number Generator
DSA	Digital Signature Algorithm
FE	File Encryption
SCP	Secure Copy Protocol

1.7 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.

2 TOE Description

2.1 Overview

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. 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 the TOE can also provide cryptographic keys and key meta data to FE Agents.

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 an DataSecure.

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. 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. 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. Features a dual processor architecture and dual hard drives in a RAID-1 mirroring configuration. These drives are hot swappable. This appliance can process more than 45000 secure cryptographic operations per second.

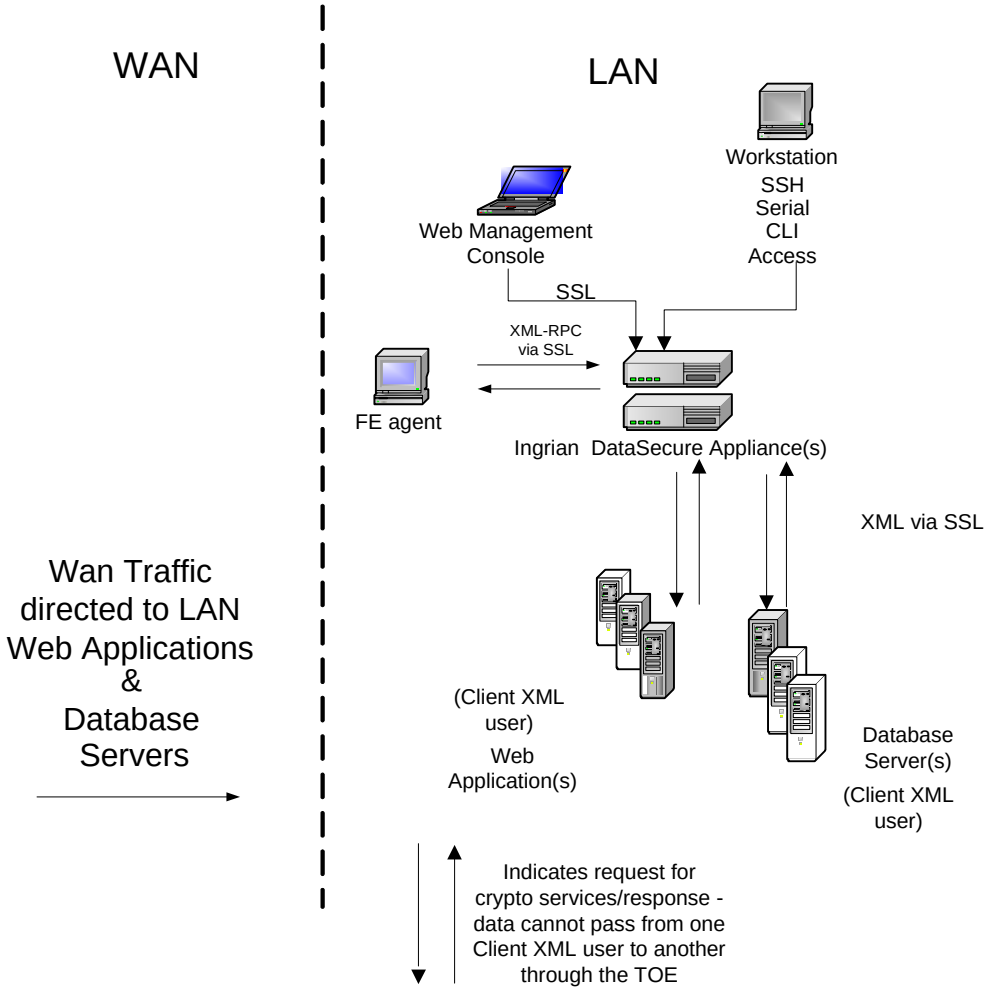


Figure 1: TOE Architecture – network deployment

*note: the TOE does not process network traffic between the WAN & LAN but rather processes cryptographic processing requests from entities within the protected network.

2.2 Architecture Description

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

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

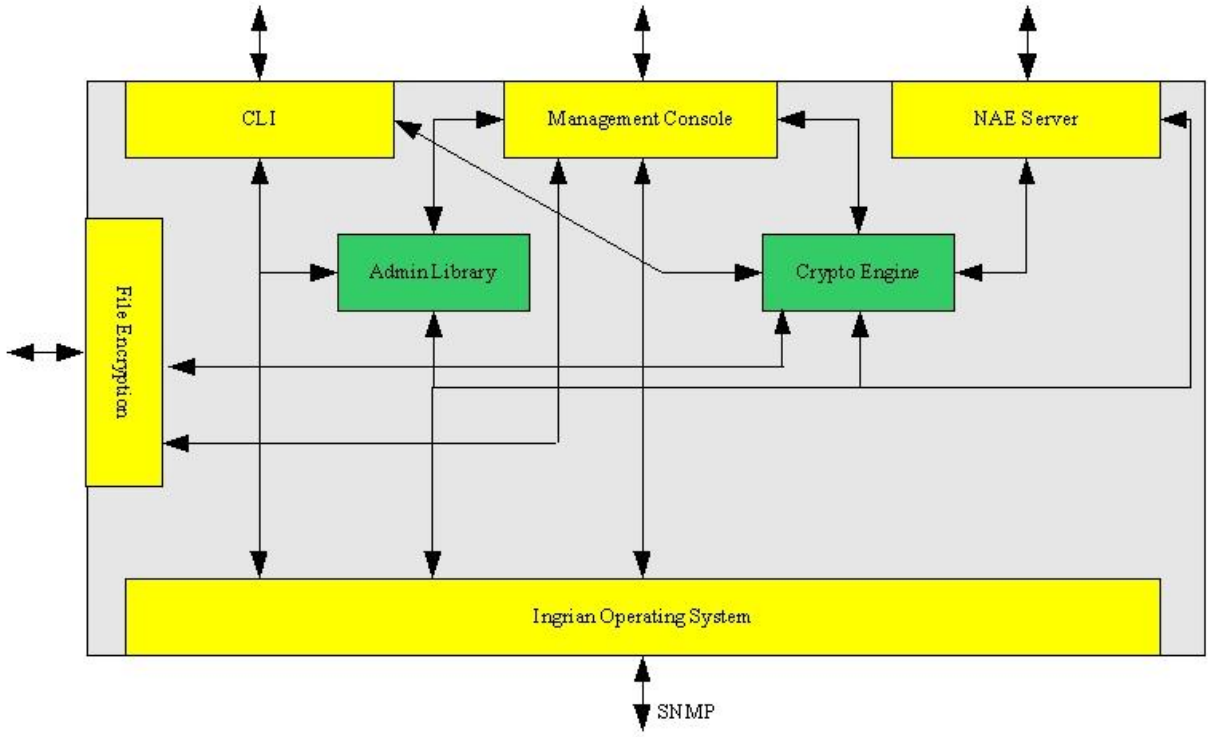


Figure 2: TOE Internal Architecture

2.2.1 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 for administrators to access the appliance through a web console machine in the IT Environment using only a standard browser component. Management sessions through the management console are secured using SSL/TLS.

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

2.2.2 Command Line Interface (CLI)

The command line interface mirrors the functionality provided by the management console through CLI commands versus GUI menus. Administrators must establish an SSH encrypted tunnel and be authenticated by the Management Console in order to gain access to the TOE. The CLI is also used local (i.e. administrators must have physical access to the TOE) to the appliance through the serial connector. Note that the serial connector is not encrypted and therefore should only be used during installation, initial configuration activities and trouble shooting activities.

2.2.3 Admin Library

The Admin Library interfaces with the Pluggable Authentication Module (PAM) within the Ingrian Operating System to authenticate TOE Administrators.

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. Additional information relating to logging is contained in Section 2.4.3.

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.

2.2.4 Crypto Engine

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

2.2.5 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.

2.2.6 File Encryption

The File Encryption Subsystem provides the external interface for providing keys and key metadata for file encryption (FE) client agents. It presents an XML RPC interface in which certificate based authenticated client FE client agents can get 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. Note that keys generated by the TOE Administrator for FE Agents can't be accessed before the authentication process and setup of the SSL tunnel has been established.

2.2.7 Ingrian Operating System

The underlying operating system for the appliance is based on Linux CentOS version 4.3, and supports the operation of 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.

2.2.8 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 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.

2.3 Physical 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.

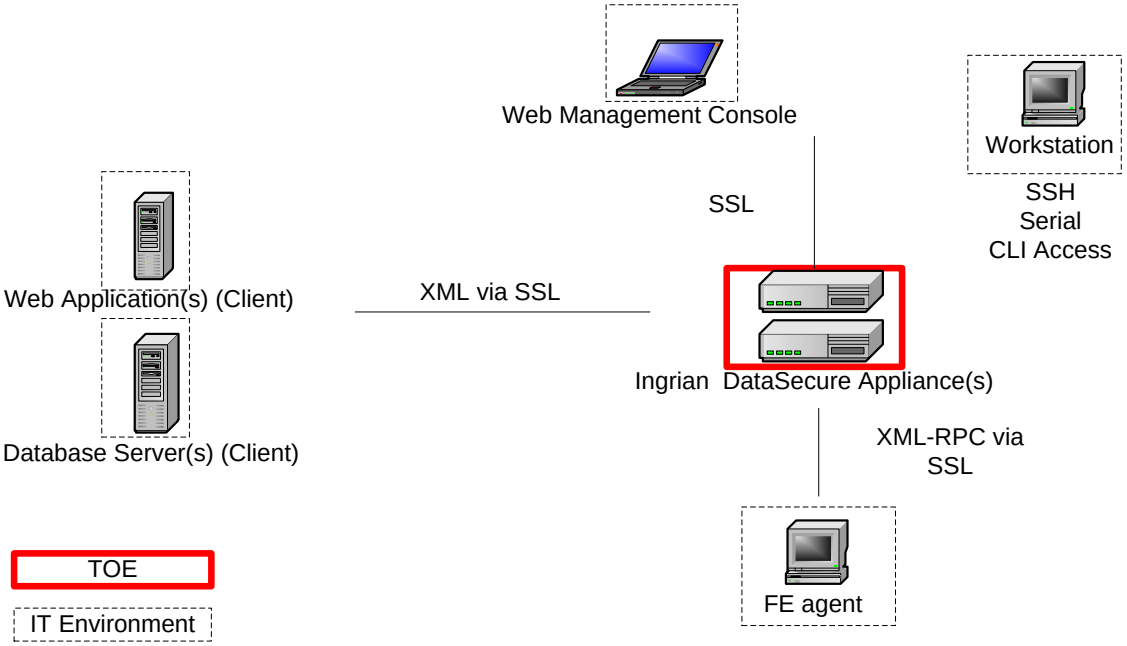


Figure 3: TOE Physical Boundaries

2.3.1 Hardware Components

This table identifies hardware components and indicates whether or not each component is in the TOE.

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

Table 2: Hardware Components

2.3.2 Software Components

This table identifies software components and indicates whether or not each component is in the TOE.

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)

Table 3: Software Components

2.3.3 Guidance Documents

The following guidance documents are provided with the TOE upon delivery in accordance with EAL 2 requirements:

- AGD_USR – User Guidance – NAE Developer Guide for the XML Interface, v4.6.2;
- AGD_ADM – Administrator Guidance – IngrianOS User Guide, v4.6.2;
- ADO_IGS – Installation Guidance – IngrianOS User Guide, v4.6.2.

Note that Users of the TOE should specifically read Chapter 9 Advance Security of IngrianOS User Guide, v4.6.2 which details installing and configuring the TOE in the evaluated configuration. All documentation delivered with the product is germane to and within the scope of the TOE.

2.3.4 FIPS Validation

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

2.4 Logical Boundaries

This section contains the product features and denotes which are in the TOE.

2.4.1 Identification 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 except 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.

Administrators accessing the TOE through the Web Server GUI interface are identified and authenticated through the Management Console subsystem by the Admin Library which calls the

pluggable authentication module (PAM) to verify the username and password against hashed credentials stored on the appliance. Password policies are configured by the TOE administrator and enforced by the Admin Library to assure that minimum password length and complexity guidelines are adhered to by Administrators. The TOE must be configured such that administrators authenticate to the Web Server GUI interface (i.e. the Management Console interface) in one of the following ways:

- Server certificate authentication and client username/password authentication
- Server certificate authentication, client cert authentication, and username/password client authentication.

Administrators accessing the appliance through the CLI interface (typically only for installation purposes) are authenticated by PAM in the same manner as noted above.

The TOE also supports certificate based authentication using either certificates issued by a Certifying Authority (CA) or through self signed certificates that may be created on the Ingrian TOE appliance. This must be configured by an authorized administrator of the TOE. The TOE must be configured such that XML users authenticate to the XML interface (i.e. the NAE Server interface) in one of the following ways:

- Server certificate authentication and client username/password authentication.
- Server certificate authentication and client cert authentication (no client username/password is sent).
- Server certificate authentication, client cert authentication, and username/password client authentication.

The differences in identification and authentication techniques used by the TOE Administrators and Client XML users are based on design differences. Administrators are identified and authenticated through the PAM module functionality within the underlying operating system (as noted above) whereas Client XML Users are identified and authenticated through the NAE Server component which includes verification of whether a given Client XML user is allowed to use a specific cryptographic key. (This is further discussed in Section 6.1.1). FE agents are always authenticated to the File Encryption Subsystem via Server certificate authentication and client cert authentication (no client username/password is sent) and must successfully authenticate and have established an SSL encrypted tunnel before any keys or key meta data are export to the FE agent.

2.4.2 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.

Client XML user profiles are established by the TOE administrator during initial configuration to

establish the identity, configuration and key usage permissions associated with that entity.

The Ingrian TOE appliance provides cryptographic services for Client XML users which consist of Application Servers, Web Server and/or Databases in the IT Environment. Through the TOE XML interface, the Client XML user requests cryptographic operations. This request is authenticated through by the NAE Server to assure that the particular Client XML user is authorized to perform the requested operation (e.g. to utilize a requested key). Upon successful authentication, the cryptographic operation is performed within the appliance and the data (encrypted or decrypted) is passed between the TOE appliance and Client XML over SSL/TLS. Note that using SSL/TLS over the XML interface must be configured in the evaluated configuration of the TOE.

The Ingrian TOE appliance generates keys internal to the appliance for use in encryption/decryption of Client XML user data. Only authorized administrators may generate keys within the appliance and Client XML users must be explicitly authorized by administrators to access keys prior to usage. Authorized administrators can also import cryptographic keys. The primary user to which a key is assigned with full rights is considered to be the key owner. Additionally, authorized XML users can export cryptographic keys.

The TOE also supports the export of cryptographic keys and key metadata to FE agents over an SSL/TLS encrypted channel.

The TOE supports the creation of Client XML user groups to make cryptographic keys available to users other than the key owner. Authorized administrators can establish these groups and then assign limited key privileges to the group. This allows any authenticated group member to use the key for specified operations. Groups can be assigned rights to use the key for any of the following operations: Encryption, Decryption, Signing and Sign Verify.

The Ingrian TOE support key destruction utilizing zeroization of plaintext keys and all critical security parameter in accordance with the requirements of FIPS 140-2.

2.4.3 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 be identified and authenticated by the Management Console or CLI subsystem prior to access.

The TOE maintains various log files that log events such as system events, service usage, identification and authentication failures, NAE server requests and actions. Audit logs include time stamps which identify the time of the event and each event is associated with the Client XML user or Administrator that was associated with the event.

There are two logging levels that may be configured on the Ingrian appliance:

- Log Normal: All messages including system errors are recorded. This is the default and

recommended level.

- Log Low: Successful configuration changes and Administrator input errors are recorded.

The Common Criteria Evaluated Configuration requires the use the "Log Normal" setting to assure all events are available for administrator review.

2.4.4 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.

The TOE appliance also provides Access Control measures to control access and usage of cryptographic keys and certificates that are used for encryption and decryption services. Access Control configuration settings, which are consulted by the TOE to assure proper authentication is provided for cryptographic key usage and is enforced by the NAE Server.

2.4.5 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.

Security Management functions for configuration and maintenance of the Ingrian TOE include:

- Appliance Network Configuration
- Appliance System Configuration
- Password Management
- Certificate Management
- SSL/TLS Management
- Appliance Logging Configuration

Also included in the Security Management security function are password management functions that enforce the Ingrian appliance password policy. By default, Administrators and Client XML

user passwords must include at least 8 characters. Additional settings are provided for requiring upper/lowercase, numbers and special characters within the password. Password reuse is constrained by the password history setting which remembers from 1 to 25 passwords to prevent administrators from reusing a previous password. Passwords can be set to expire within 1 to 365 days to support regular changing of administrator passwords. When new Administrators are created, the defaults enable broad access to TOE functions. The logical step in configuring a new Administrator is creating the user and then configuring the permissions, however, the default values are permissive in that they begin as all inclusive.

It should be noted that in the evaluated configuration of the TOE "allow key and policy configuration operations" must not be enabled. Therefore no management operations are allowed via the XML interface.

2.4.6 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[4] to be utilized.

Communication between Client XML users and the TOE is only allowed through XML transfer over SSL/TLS secured sessions. Client XML users are required by the TOE to be identified by presentation of a valid certificate and then secondarily, identified and authenticated by username and password prior to establishing a session and gaining access to TOE services.

All communications to the TOE must be either secured via SSL/TLS or SSH.

2.4.7 Protection of TOE Functions

Physical and logical protection of the TOE ensures that TOE related security functions are not bypassed or altered. This is provided by the TOE and Operating System Environment and through the secure communication methods described in Ingrian OS Users Guide.

[4] Note that the TOE only allows Version 2 of the SSH Protocol. All references the SSH refer to SSH Protocol Version 2.

2.5 Items and Functionality Excluded from the TOE

The following provides an overview of the TOE functionality that cannot 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

3 TOE Security Environment

The TOE is intended to be used either in environments in which, at most, sensitive but unclassified information is processed, or the sensitivity level of information in both the internal and external networks is equivalent.

This section contains assumptions regarding the security environment and the intended usage of the TOE and threats on the TOE and the IT environment.

3.1 Assumptions

The assumptions are ordered into three categories: personnel assumptions, physical environment assumptions, and operational assumptions.

3.1.1 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.

3.1.2 Physical Environment 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.

.

3.1.3 Operational Assumptions

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

3.2 Threats

The TOE or IT environment addresses the threats identified in this section. The threat agents are authorized persons/processes, unauthorized persons/processes, or external IT entities not authorized to use the TOE itself. The threats identified assume that the threat agent is a person with a low attack potential who possesses an average expertise, few resources, and low to moderate motivation.

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.CRYPTO	Sensitive data utilized by Client XML and FE agent user IT resources in the IT Environment may be compromised or disclosed during transit.
T.TSF_COMP	An attacking user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.UNSEC_DATA	Data Transfer between the Ingrian Appliance and the Administrator workstation, Client XML or FE agent users may be modified or disclosed in transit.

3.3 Organizational Security Policies

There are no Organizational Security Policies for this TOE.

4 Security Objectives

This chapter describes the security objectives for the TOE and the TOE's Operating environment. The security objectives are divided between TOE Security Objectives (for example, security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (for example, security objectives addressed by the IT domain or by non-technical or procedural means).

4.1 Security Objectives For The TOE

This section defines the IT security objectives that are to be addressed by the TOE.

Security Objective	Description	Reference:
O.AUDIT_GEN	The TOE will provide the capability to generate and review audit records and protect those records from unauthorized access.	FAU_GEN.EXP.1 FAU_SAR.1 FAU_STG.1
O.CRYPTO	The TOE will provide encryption and decryption of Client User data when requested by authenticated Client XML users to prevent disclosure and provide Certificate Authority Services.	FCS_COP.1 FCS_CKM.1 FCS_CKM.4 FMT_MSA.2 FCS_CKM.EXP.2a FCS_CKM.EXP.2b FCS_CKM.EXP.5 FCS_CER.EXP.1 FCS_CER.EXP.2 FCS_CER.EXP.3 FCS_CER.EXP.4 FCS_INF.EXP.1 FCS_POL.EXP.1
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FMT_MSA.1 FMT_MSA.2 FMT_MSA.3a FMT_MSA.3b FMT_MSA.3c FMT_MTD.1a FMT_MTD.1b FMT_MTD.1c FMT_SMF.1 FDP_BAU.EXP.1
O.ACCESS	The TOE will provide access control functions to specific SFP objects and operations based on selected security attributes.	FDP_ACC.1a FDP_ACC.1b FDP_ACC.1c FDP_ACF.1a FDP_ACF.1b FDP_ACF.1c FMT_MSA.1 FMT_MSA.2 FMT_MSA.3a FMT_MSA.3b

		FMT_MSA.3c FMT_SMR.1 FDP_MEM.EXP.1
O.SELF_PROT	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure.	FPT_RVM.1 FPT_SEP.1
O.TIME_STAMPS	The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.	FPT_STM.1
O.ROBUST_TOE	The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	FIA_UID.1 FIA_UAU.1 FIA_AFL.1
O.SECURE_DATA	The TOE will establish SFPs to ensure secure data transfer within the TOE and between the TOE and trusted IT products using cryptography.	FCS_COP.1 FCS_CKM.1 FCS_CKM.4 FMT_MSA.2 FCS_CKM.EXP.2a FCS_CKM.EXP.2b FCS_CKM.EXP.5

Table 4: TOE Security Objectives

4.2 Security Objectives for the Environment

The following non-IT security objectives for the environment listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or Administrative measures.

OE.ADMIN — Sites using the TOE will ensure that the authorized administrators are appropriately trained, not careless, not willfully negligent, non-hostile and follow all instructions within administrative guidance.

OE.USE — Administrators will assure that the Ingrian Appliance is dedicated to its primary function and does not provide any general purpose computing or storage capabilities.

OE.PHYSICAL — The TOE is physically secure and physical access is controlled to assure only authorized Administrators have access.

4.3 Mapping of Security Environment to Security Objectives

The following table represents a mapping of the threats, assumptions, and OSPs to the security objectives defined in this ST.

	A.ADMIN	A.LOCATE	A.USE	T.SEC_FUNC	T.MASK	T.CRYPTO	T.TSF_COMP	T.UNSEC_DATA
O.AUDIT_GEN				X				
O.CRYPTO						X		
O.MANAGE							X	
O.ACCESS					X		X	
O.SELF_PROT							X	
O.TIME_STAMPS				X				
O.ROBUST_TOE					X			
O.SECURE_DATA								X
OE.ADMIN	X							
OE.USE			X					
OE.PHYSICAL		X						

Table 5: Threats & IT Security Objectives Mappings

4.4 Rationale For Threat Coverage

This section provides a justification that for each threat, the security objectives counter the threat.

T.SEC_FUNC — O.AUDIT_GEN mitigates this threat by logging all security function related events within the TOE and making these logs available for review. O.TIME_STAMPS supports the audit function by assuring that accurate time stamps are provided for audit records generated.

T. MASK	O.ROBUST_TOE helps mitigate this threat by providing mechanisms that control access to the TOE and to explicitly deny access when appropriate. O.ACCESS provides access control mechanisms to specify operations and objects that may be accessed by specific Users of the TOE.
T.CRYPTO	O.CRYPTO mitigates this threat by providing cryptographic mechanisms and services that secure Client XML user IT resource data provided to the TOE for cryptographic processing.
T. TSF_COMP	O.MANAGE mitigates this threat by assuring all the functions and facilities necessary to support management of security functions and prevent unauthorized use are available to Administrators. O.SELF_PROT helps to mitigate this threat by requiring the TOE to maintain a domain for its' own execution that protects itself from interference, tampering or disclosure. O.ACCESS supports mitigation of this threat by managing access control functions to SFP operations and attributes.
T.UNSEC_DATA	O.SECURE_DATA mitigates this threat by the implementation of secure communication methods (SSL/TLS/SSH) for all communications between the TOE and Administrator Workstation.

4.5 Rationale For Organizational Policy Coverage

There are no Organizational Policies for this TOE.

4.6 Rationale For Assumption Coverage

This section provides a justification that for each assumption, the security objectives for the environment cover that assumption.

- A.ADMIN:

  This assumption is restated in the form of OE. ADMIN addressing this assumption in the form of provided documentation and assurance of Administrator suitability and non malicious activity.

- A.LOCATE

  This assumption is restated in the form of OE.PHYSICAL assuring that facilities housing the TOE and TOE environment provide a protective environment with restricted access.

- A.USE

This assumption is restated in the form of OE.USE which requires that the TOE Environment is dedicated to the specified use and will not house additional applications or functions unrelated to the TOE.

5 IT Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST. These security requirements are defined in Sections 5.1 – 5.4.

TOE Security Functional Requirements (from CC Part 2)	
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP_ACC.1a	Subset Access Control – Cryptographic Operations
FDP_ACC.1b	Subset Access Control – Appliance Administration
FDP_ACC.1c	Subset Access Control – FE Agent Key export operations
FDP_ACF.1a	Security attribute based access control– Cryptographic Operations
FDP_ACF.1b	Security attribute based access control– Appliance Administration
FDP_ACF.1c	Security attribute based access control– FE Agent Key export operations
FIA_AFL.1	Authentication Failure
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of Identification
FIA_SOS.1	Verification of Secrets
FIA_SOS.2	TSF Generation of Secrets
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3a	Static attribute initialization - Client XML Users and Cryptographic Attributes
FMT_MSA.3b	Static attribute initialization-Administrator Attributes
FMT_MSA.3c	Static attribute initialization- FE Agents
FMT_SMF.1	Specification of mgmt functions

FMT_SMR.1	Security Roles
FMT_MTD.1a	Management of TSF data – Query, Modify, Delete
FMT_MTD.1b	Management of TSF data - Query
FMT_MTD.1c	Management of TSF data - Modify
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
FPT_STM.1	Reliable Time Stamps
FAU_GEN.EXP.1	Audit data generation (explicit)
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

Table 6: Functional Requirements

5.1 TOE Security Functional Requirements

The SFRs defined in this section are taken from Part 2 of the CC.

5.1.1 Class FAU: Security Audit

FAU_GEN.2 User identity association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **Administrator** with the capability to read **audit information in Table 9** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_STG.1 **Protected audit trail storage**

FAU_STG.1.1 The TSF shall protect the stored audit records from ***~~unauthorised~~*** deletion.

FAU_STG.1.2 The TSF shall be able to prevent ***~~unauthorized~~*** modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall "overwrite the oldest stored audit records" **and "which the administrator must configure to be backed up automatically through the secure copy protocol to an external log file"** if the audit trail is full.

5.1.2 Class FCS: Cryptographic key management

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **as noted in Table 7, column #1** and specified cryptographic key sizes **(per table 7, column #2)** that meet the following: **as listed in table 7, column #3**.

Key Gen Algorithm	Key Sizes	Standards Met	Key Type
X9.31 for AES	128, 192, 256 bit	ANSI X9.31	Symmetric
X9.31 for 3DES	112, 168 bit	ANSI X9.31	Symmetric

X9.31 for RC4	128 bit	ANSI X9.31	Symmetric
X9.31 for SEED	128 bit	ANSI X9.31	Symmetric
X9.31 for HMAC-SHA1	128 bit	ANSI X9.31	HMAC hash
RSA	1024, 2048 bit	ANSI X9.31	Asymmetric
DSA	1024 bit	ANSI X9.31	Asymmetric

Table 7: Key Generation attributes

FCS_CKM.4 **Cryptographic key destruction**

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **Zeroization** that meets the following**: FIPS 140-2.**

FCS_COP.1 **Cryptographic operation**

FCS_COP.1.1 The TSF shall perform **Operations in Column #1 in table 8** in accordance with a specified cryptographic algorithm **algorithms listed in Column #2 in table 8** and cryptographic key sizes **as listed in Column #3 in table 8** that meet the following: **standard listed in Column #4 in table 8.**

Crypto Operations	Cryptographic algorithm	Key Sizes	Standards
Encrypt/Decrypt	3DES	112, 168 bit	FIPS 46.3
Encrypt/Decrypt	AES	128, 192, 256 bit	FIPS 197
Encrypt/Decrypt	RC4	128 bit	RFC 4345
Encrypt/Decrypt	SEED	128 bit	RFC 4269
Encrypt/Decrypt	RSA	1024, 2048 bit	PKCS#1
Hash functions	HMAC-SHA1	160 bit	FIPS 198
Sign/Verify	RSA	1024, 2048 bit	PKCS#1
Sign/Verify	DSA	1024 bit	FIPS PUB 186-2

Table 8: Cryptographic Operation attributes

5.1.3 Class FDP: User Data Protection

FDP_ACC.1a **Subset access control – *Cryptographic Operations***

FDP_ACC.1.1a The TSF shall enforce the **Ingrian Access Control SFP** on

Subjects: Client XML **users**
Objects: Cryptographic Keys
Operations: Encrypt/Decrypt/Key Export.

FDP_ACC.1b **Subset access control – *Appliance Administration***

FDP_ACC.1.1b The TSF shall enforce the **Ingrian Access Control SFP** on

Subjects: Administrators
Objects: Appliance configuration objects
Operations: Modify appliance configuration.

FDP_ACC.1c **Subset access control – *FE Agent Key export operations***

FDP_ACC.1.1c The TSF shall enforce the **Ingrian Access Control SFP** on

Subjects: FE Agents
Objects: Cryptographic Keys and Key metadata
Operations: Export.

FDP_ACF.1a **Security attribute based access control – *Cryptographic Operations***

FDP_ACF.1.1a The TSF shall enforce the **Ingrian Access Control SFP** to objects based on the following:

The following access control attributes associated with a subject: Client XML

- **Server certificate authentication and client username/password authentication or;**
- **Server certificate authentication and client cert authentication (no client username/password is sent) or;**
- **Server certificate authentication, client cert authentication, and username/password client authentication.**

The following access control attributes associated with an object: cryptographic key assignments/permissions based on Client XML **user profile**

FDP_ACF.1.2a The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a Client XML **user may access cryptographic services based on assigned** Client XML **user profile, successful certificate based authentication, successful username/password verification and configured permissions to access specified keys and associated cryptographic processes.**

FDP_ACF.1.3a The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **no additional rules.**

FDP_ACF.1.4 a The TSF shall explicitly deny access of subjects to objects based on the: **no additional rules.**

FDP_ACF.1b **Security attribute based access control - *Appliance Administration***

FDP_ACF.1.1b The TSF shall enforce the **Ingrian Access Control SFP** to objects based

on the following:

The following access control attributes associated with a subject: Administrator authenticated role

The following access control attributes associated with an object: Role based permissions to access specific TOE configuration objects based on authenticated Administrator role

FDP_ACF.1.2b The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

An Administrator may access specific Appliance Configuration Objects if they are authenticated in the Administrator user role with a successful username/password and the required permissions.

FDP_ACF.1.3b The TSF shall explicitly authorise access of subjects to objects based on the following additional rules**: no additional rules.**

FDP_ACF.1.4b The TSF shall explicitly deny access of subjects to objects based on the **no additional rules.**

FDP_ACF.1c **Security attribute based access control – *FE Agent Key Export Operations***

FDP_ACF.1.1c The TSF shall enforce the **Ingrian Access Control SFP** to objects based on the following:

The following access control attributes associated with a subject: FE Agent **user authentication profile (certificate)**

The following access control attributes associated with an object: cryptographic key and key metadata assignments based on authenticated FE agent user

FDP_ACF.1.2c The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a FE Agent **user may export cryptographic key and key metadata based on successful certificate based authentication.**

FDP_ACF.1.3c The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **no additional rules.**

FDP_ACF.1.4 c The TSF shall explicitly deny access of subjects to objects based on the: **no additional rules.**

5.1.4 Class FIA: Identification and authentication

FIA_AFL.1 **Authentication Failure**

FIA_AFL.1.1 The TSF shall detect when **six** unsuccessful authentication attempts occur related to **XML user and Administrator authentication**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall **lock the account for a period of 60 seconds**.

FIA_UAU.1 **Timing of authentication**

FIA_UAU.1.1 The TSF shall allow

- **System status information to be polled from the TOE.**
- **Unauthenticated remote administrators to initiate SSH sessions via CLI.**
- **Initiate SSL/TLS handshake via the XML, Management, and File Encryption Interfaces.**
- **Client XML users to negotiate version information with the TOE via the XML interface.**

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.1 **Timing of identification**

FIA_UID.1.1 The TSF shall allow

- **System status information to be polled from the TOE.**
- **Unauthenticated administrators to initiate SSH sessions via CLI.**
- **Initiate SSL/TLS handshake via the XML, Management, and File Encryption Interfaces.**
- **Client XML users to negotiate version information with the TOE via the XML interface**

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_SOS.1 **Verification of secrets**

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **Administrator configured Password Management settings – 8 characters minimum, at least five different characters, must not contain only whitespace, resemble a phone number, dictionary word, or reversed dictionary word, or be based on the username associated with the password, no more than 4 sequential characters.**

FIA_SOS.2 **TSF Generation of secrets**

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet **1024 bit (min) Client XML user and FE agent certificates**.

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for **Server SSL establishment and Client XML user and FE agent cryptographic service (key) access.**

5.1.5 Class FMT: Security Management

FMT_MSA.1 **Management of security attributes**

FMT_MSA.1.1 The TSF shall enforce the **Ingrian Access Control SFP** to restrict the ability to query, modify, delete the security attributes **Key Type (algorithm), Key Length, FE Agent cryptographic key and key metadata assignments, Client XML user Key Assignments and Client XML user Access Control attributes (role, password assignments, group memberships)** to the **Administrator role**.

FMT_MSA.2 **Secure security attributes**

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MSA.3a **Static attribute initialization – *Client XML Users and Cryptographic Attributes***

FMT_MSA.3.1a The TSF shall enforce the **Ingrian Access Control SFP** to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2a The TSF shall allow the **Administrator** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3b **Static attribute initialization – *Administrator Attributes***

FMT_MSA.3.1b The TSF shall enforce the **Ingrian Access Control SFP** to provide permissive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2b The TSF shall allow the **Administrator** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3c **Static attribute initialization – *FE Agents***

FMT_MSA.3.1c The TSF shall enforce the **Ingrian Access Control SFP** to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2c The TSF shall allow the **Administrator** to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1a **Management of TSF data – *Query, Modify, Delete***

FMT_MTD.1.1a The TSF shall restrict the ability to query, modify, delete **Administrators, Administrator Roles,** Administrator/Client XML **user Passwords, Client XML user Key data, Client XML User Key Assignment/Permissions data, SSL/TLS certificate data** to **the Administrator Role.**

FMT_MTD.1b **Management of TSF data - *Query***

FMT_MTD.1.1b The TSF shall restrict the ability to query **Audit/logging data** to **the Administrator Role.**

FMT_MTD.1c **Management of TSF data - *Modify***

FMT_MTD.1.1c The TSF shall restrict the ability to modify **Appliance time/date** to **the Administrator Role.**

FMT_SMF.1 **Specification of Management Functions**

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

a. Creating & Managing Administrator/Client XML user attributes (roles, passwords)
b. Creating & Managing Groups
c. Creating Keys, Certificates and managing usage
d. Setting and Changing permissions between Administrators/Client XML users, groups and keys
e. Initial setting and subsequent modification of the time and date maintained by the TOE Appliance's internal clock
f. Exporting cryptographic keys and key metadata to FE agents.

FMT_SMR.1 **Security roles**

FMT_SMR.1.1 The TSF shall maintain the roles **Administrator**, **Client XML user and FE agent**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.6 Class FPT: Protection of the TSF

FPT_RVM.1 **Non-bypassability of the TSP**

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1 **TSF domain separation**

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.2 Explicitly Stated TOE Security Functional Requirements

The SFRs defined in this section are explicitly stated and are derived from similar requirements in Part 2 of the CC.

5.2.1 Audit Data Generation

5.2.1.1 FAU_GEN.EXP.1 Audit data generation

FAU_GEN.EXP.1.1 The TSF shall be able to generate a log record of the following auditable events:

a) Start-up ~~*and shutdown*~~ of the audit functions;

b) All auditable events for the not specified level of audit; and

c) **the auditable events listed in Table 9.**

FAU_GEN.EXP.1.2 The TSF shall record within each log record at least the following information:

a) Date and time of the event (for all logs except the audit log), type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **No additional audit relevant information.**

Functional Component	Auditable Event
FIA_UAU.1	Administrator authentication failure
FIA_UID.1	Administrator identification failure
FIA_AFL.1	Account lockout due to multiple authentication failure.
FMT_MSA.1,	Modification or deletion of security attributes (per

FMT_SMF.1	FMT_MSA.1.1) – key attribute changes: key type, key length
FMT_MSA.1, FMT_SMR.1, FMT_SMF.1	Modification or deletion of security attributes (per FMT_MSA.1.1) Client XML user role changes
FMT_MSA.1, FMT_SMF.1	Modification or deletion of security attributes (per FMT_MSA.1.1) Client XML user password changes
FMT_MSA.1, FMT_SMF.1	Modification or deletion of security attributes (per FMT_MSA.1.1) Client XML user group membership changes
FMT_MTD.1a, FMT_SMF.1	Modification or deletion of TSF values (per FMT_MTD.1.1a**): Administrators**
FMT_MTD.1a, FMT_SMR.1, FMT_SMF.1	Modification or deletion of TSF values (per FMT_MTD.1.1a**): Administrator/Client XML user roles**
FMT_MTD.1a, FMT_SMF.1	Modification or deletion of TSF values (per FMT_MTD.1.1a**): Client XML key data**
FMT_MTD.1a, FMT_SMF.1	Modification or deletion of TSF values (per FMT_MTD.1.1a**): Client XML key assignments/group membership data**
FMT_MTD.1a, FMT_SMF.1	Modification or deletion of TSF values (per FMT_MTD.1.1a**): SSL/TLS certificate data**
FMT_SMF.1 FMT_MTD.1c	Modification of Appliance time/date
FCS_CKM.EXP.2.1a FCS_CKM.EXP.2.1b FMT_SMF.1	Export of cryptographic keys

Table 9: FAU_GEN.EXP.1 Auditable Events

5.2.1.2 FCS_CER.EXP.1 Certificate Generation

FCS_CER.EXP.1.1 The TSF shall generate certificates in the following formats: X509.

5.2.1.3 FCS_CER.EXP.2 Certificate Import

FCS_CER.EXP.2.1 The TSF shall be able to import certificates which are formatted in the following manner: PEM Encoded PKCS #7, PEM Encoded PKCS #12, PEM Encoded X509.

5.2.1.4 FCS_CER.EXP.3 Certificate Export

FCS_CER.EXP.3.1 Administrators shall be able to download certificates formatted in the following manner: X509.

5.2.1.5 FCS_CER.EXP.4 Certificate Request Generation

5.2.1.6 FCS_CER.EXP.4.1 The TSF shall be able to generate a certificate request in the following format: X.509 certificate request message format.FCS_CKM.EXP.2a Cryptographic key export – XML Users

FCS_CKM.EXP.2.1a The TSF shall export **AES, SEED, DES, DES-EDE, RC4, HMACSHA1, RSA as per Table 7** cryptographic keys encrypted with one of the following cryptographic algorithms: **3DES, AES, or RC4** that meet the following: **standard listed in Column #4 in table 8**.

5.2.1.7 FCS_CKM.EXP.2b Cryptographic key export – FE Agent

FCS_CKM.EXP.2.1b The TSF shall export 256 bit AES cryptographic keys as listed in Table 7 encrypted with one of the following cryptographic algorithms: **3DES, AES, or RC4** that meet the following: **standard listed in Column #4 in table 8**.

5.2.1.8 FCS_CKM.EXP.5 Cryptographic key import – Administrator

FCS_CKM.EXP.5.1 The TSF shall allow Administrators to import **AES, SEED, DES, DES-EDE, RC4, HMACSHA1, RSA as per Table 7** cryptographic keys encrypted with one of the following cryptographic algorithms: **3DES, AES, or RC4** that meet the following: **standard listed in Column #4 in table 8**.

5.2.1.9 FCS_INF.EXP.1 Cryptographic Key Information Query

FCS_INF.EXP.1.1 XML users can get the following key information on keys which they are

authorized to use: Key Name, Key Size, if the key is exportable, cryptographic operation(s) allowed, key fingerprint[5]

5.2.1.10 FCS_POL.EXP.1 Cryptographic Authorization Policy

FCS_POL.EXP.1.1 Authorized administrators can set authorization policies on cryptographic keys to limit the rate cryptographic operations are performed and the time cryptographic operations are performed.

5.2.1.11 FDP_MEM.EXP.1 XML user group membership query

FDP_MEM.EXP.1.1 Authorized XML users can query the TOE to determine their group membership.

5.2.1.12 FDP_BAU.EXP.1 Backup File Import

FDP_BAU.EXP.1.1 The TSF shall be able to import backup files.

5.3 TOE Strength of Function Claim

The only probabilistic or permutational mechanisms in the product are the password mechanism used to authenticate users and the cryptographic mechanisms. Strength of cryptographic algorithms is outside the scope of the Common Criteria.

The claimed minimum strength of function is SOF-basic. FIA_UAU.1 is the only non-cryptographic TOE security functional requirements that contain a permutational function.

5.4 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2 Augmented ALC_FLR.1) as defined by the CC. The assurance components are summarized in the following table.

[5] If the request is for information about the public key from a certificate, then the TOE omits the fingerprint information in the response.

Assurance Class	Assurance Components	
ACM: Configuration management	ACM_CAP.2	Configuration items
ADO: Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis
ALC: Life Cycle Support	ALC_FLR.1	Basic Flaw Remediation

Table 10: Assurance Requirements: EAL2 Augmented ALC_FLR.1

5.4.1 ACM_CAP.2 Configuration items

Developer action elements:

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labelled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.2.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.6C The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.

ACM_CAP.2.7C The CM system shall uniquely identify all configuration items that comprise the TOE.

Evaluator action elements:

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.2 ADO_DEL.1 Delivery procedures

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.3 ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.4.4 ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions, and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.4.5 ADV_HLD.1 Descriptive high-level design

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.4.6 ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.7 AGD_ADM.1 Administrator guidance

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.8 AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.9 ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.10 ATE_FUN.1 Functional testing

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.11 ATE_IND.2 Independent testing - sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.4.12 AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.4.13 AVA_VLA.1 Developer vulnerability analysis

Developer action elements:

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements:

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.4.14 ALC_FLR.1 Basic flaw remediation

Developer action elements

ALC_FLR.1.1D The developer shall provide flaw remediation procedures addressed to TOE developers.

Content and presentation of evidence elements

ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

Evaluator action elements

ALC_FLR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.5 Rationale For TOE Security Requirements

5.5.1 TOE Security Functional Requirements

	O.AUDIT_GEN	O.CRYPTO	O.MANAGE	O.ACCESS	O.SELF_PROT	O.TIME_STAMPS	O.ROBUST_TOE	O.SECURE_DATA
FAU_GEN.2	X							
FAU_SAR.1	X							
FAU_STG.1	X							
FAU_STG.4	X							
FCS_CKM.1		X						X
FCS_CKM.4		X						X
FCS_COP.1		X						X
FIA_AFL.1							X	
FDP_ACC.1a				X				
FDP_ACC.1b				X				
FDP_ACC.1c				X				
FDP_ACF.1a				X				
FDP_ACF.1b				**X**				
FDP_ACF.1c				**X**				
FIA_UAU.1							**X**	
FIA_UID.1							**X**	
FIA_SOS.1							**X**	
FIA_SOS.2							**X**	
FMT_MSA.1			**X**	**X**				
FMT_MSA.2		**X**	**X**	**X**				**X**
FMT_MSA.3a			**X**	**X**				

	O.AUDIT_GEN	O.CRYPTO	O.MANAGE	O.ACCESS	O.SELF_PROT	O.TIME_STAMPS	O.ROBUST_TOE	O.SECURE_DATA
FMT_MSA.3b			X	X				
FMT_MSA.3c			X	X				
FMT_MTD.1a			X					
FMT_MTD.1b			X					
FMT_MTD.1c			X					
FMT_SMF.1			X					
FMT_SMR.1			X	X				
FPT_RVM.1					X			
FPT_SEP.1					X			
FPT_STM.1						X		
FAU_GEN.EXP.1	X							
FCS_CKM.EXP.2a		X						X
FCS_CKM.EXP.2b		X						X
FCS_CKM.EXP.5		X						X
FCS_CER.EXP.1		X						
FCS_CER.EXP.2		X						
FCS_CER.EXP.3		X						
FCS_CER.EXP.4		X						
FCS_INF.EXP.1		X						
FCS_POL.EXP.1		X						
FDP_MEM.EXP.1				X				
FDP_BAU.EXP.1			X					

Table 11: SFR and Security Objectives Mapping

Security Objective	Mapping Rationale
O.AUDIT_GEN	FAU_GEN.EXP.1 specifies the security related items that the TOE must log in the course of TOE operation to assure accountability for security function alterations and visibility to security related events. FAU_GEN.2 specifies that audit logs are associated by the user that caused the event. FAU_SAR.1 specifies that the TOE provides for the review of audit records by specified users (Administrators) and in an appropriate form for those users to interpret audit information. FAU_STG.1 specifies that the TOE has mechanisms to protect audit records from unauthorized access and prevent modification of audit records. FAU_STG.4 specifies that the TOE overwrites audit records when the audit log is full and are exported automatically through scp to an external log file.
O.CRYPTO	FCS_COP.1 specifies the use in the TOE of cryptographic operations and specifies the algorithms and key sizes supported for encryption/decryption operations. FCS_CKM.1 specifies the key generation mechanisms used by the TOE by applicable algorithm, key size and applicable standard. FCS_CKM.EXP.2 specifies encrypted key export mechanism used by the TOE to securely export cryptographic keys. FCS_CKM.EXP.5 specifies encrypted key import mechanism used by the TOE to security import cryptographic keys by an authorized administrator. FCS_CKM.4 specifies the methods used by the TOE for the destruction of keys and the applicable standard of the method in use. FMT_MSA.2 specifies the TOE mechanisms which assure that only secure values are accepted by the TOE for security attributes. FCS_CER.EXP.1 specifies the certificate generation method used by the TOE to generate certificates. FCS_CER.EXP.2 Specifies certificate import methods used by the TOE to import certificates. FCS_CER.EXP.3 Specifies certificate Export mechanisms used by the TOE. FCS_CER.EXP.4 Specifies certificate request generation specifies the mechanisms to generate certificate requests.. FCS_INF.EXP.1 Specifies Cryptographic Key Information Query mechanisms used by XML users to query the TOE for key information.

	FCS_POL.EXP.1 Specifies Cryptographic Authorization Policy which provides limits on key usage by XML users.
O.MANAGE	FMT_MSA.1 specifies the management of security attributes by authorized users/user roles. This assures that sufficient control and visibility is present within the TOE to effectively manage security functions. FMT_MSA.2 specifies that only secure values will be accepted by the TOE for security attributes. FMT_MSA.3a, FMT_MSA.3b, FMT_MSA.3c specifies restrictive default values for security attributes and specifies that only the Administrator can change initial values. FMT_MTD.1a, FMT_MTD.1b, FMT_MTD.1c places restrictions on which users/roles may manipulate TSF data thereby affecting security functionality within the TOE. FMT_SMR.1 specifies the role that the TOE provides for appliance administrator users. FMT_SMF.1 specifies the management functions that the TOE uses to define parameters under which the TOE manages security related aspects of operation. The TOE provides detailed administrator guidance to ensure correction configuration and management of security functions FDP_BAU.EXP.1 Backup File Import allows authorized administrators to import back up files.
O.ACCESS	FDP_ACC.1a, FDP_ACC.1b, FDP_ACC.1c specifies the subjects, objects and operations which the TOE applies the Ingrian access control security policy. FDP_ACF.1a, FDP_ACF.1b, FDP_ACF.1c specifies the access rules which are enforced by the TOE in implanting the Ingrian access control policy. FMT_MSA.1 specifies the management of security attributes by authorized users/user roles. This assures that sufficient control and visibility is present within the TOE to effectively manage security functions. FMT_MSA.2 specifies that only secure values will be accepted by the TOE for security attributes. FMT_MSA.3a, FMT_MSA.3b, FMT_MSA.3c specifies restrictive default values for security attributes and specifies that only the Administrator can change initial values. FMT_SMR.1 specifies the role that the TOE provides for appliance Administrators. FDP_MEM.EXP.1 Specifies XML user group

	membership functionality
O.SELF_PROT	FPT_SEP.1 specifies that the TOE will provide a secure domain for its execution and will enforce separation between subjects in the TSC. FPT_RVM.1 specifies that the TOE may not be able to be bypassed to avoid this protective domain.
O.TIME_STAMPS	FPT_STM.1 provides for the capability to annotate audit logs with a time stamp produced during TOE operation for accurate time related rendition of TOE auditable activities.
O.ROBUST_TOE	FIA_UID.1 and FIA_UAU.1 specify that Users must be positively identified and authenticated prior to accessing TSF resources except for limited access items specified. FIA_SOS.1 specifies that the TSF enforces the use of passwords having a minimum of 8 characters. FIA_SOS.2 specifies that the TSF provides mechanisms to create certificates of at least 1024 bits for use in Server SSL session negotiation and Client XML user authentication enforcement.FIA_AFL.1 specifies that on the sixth unsuccessful authentication attempt XML users and Administrator accounts are locked for 60 seconds.
O.SECURE_DATA	FCS_COP.1 specifies the use in the TOE of cryptographic operations and specifies the algorithms and key sizes supported for encryption/decryption operations. FCS_CKM.1 specifies the key generation mechanisms used by the TOE by applicable algorithm, key size and applicable standard. FCS_CKM.EXP.2 specifies encrypted key export mechanism used by the TOE to securely export cryptographic keys. FCS_CKM.4 specifies the methods used by the TOE for the destruction of keys and the applicable standard of the method in use. FCS_CKM.EXP.5 specifies encrypted key import mechanism used by the TOE to security import cryptographic keys. FMT_MSA.2 specifies the TOE mechanisms which assure that only secure values are accepted by the TOE for security attributes.

5.5.2 TOE Security Assurance Requirements

EAL2 (Augmented ALC_FLR.1) was chosen to provide a low to moderate level of independently assured security. The chosen assurance level is consistent with the threat

environment. Specifically, that the threat of malicious attacks is not greater than moderate and the product will have undergone a search for obvious flaws.

The ALC_FLR.1 augmentation was chosen to demonstrate Ingrian's internal processes and procedures that are used to track all reported security flaws in each release of the TOE. This assurance measure assure that these processes are thorough and consistent in identifying and correcting security flaws and communicating these changes to TOE Administrators.

5.6 Rationale for Explicitly Stated Security Requirements

Table 12 presents the rationale for the inclusion of the explicit requirements found in this Security Target.

Explicit Requirement	Identifier	Rationale
FAU_GEN.EXP.1	Audit data generation	This requirement is explicitly stated because the TOE does not include logging of audit function de-activation within the TOE's auditing capability.
FCS_CKM.EXP.2	Export of encrypted cryptographic keys	This requirement is explicitly stated because no SFR captures the concept of exporting encrypted keys. FCS_CKM.2 in particular deals with algorithmic key distribution methods.
FCS_CKM.EXP.5	Import of encrypted cryptographic keys	This requirement is explicitly stated because not SFR captures the concept of importing encrypted keys.
FCS_CKM.EXP.1	Certificate Generation	This requirement is explicitly stated because no SFR captures the concept of Certificate Generation.
FCS_CKM.EXP.2	Certificate Import	This requirement is explicitly stated because no SFR captures the concept of Certificate Import.
FCS_CKM.EXP.3	Certificate Export	This requirement is explicitly stated because no SFR captures the concept of Certificate Export.
FCS_CKM.EXP.4	Certificate Request Generation	This requirement is explicitly stated because no SFR captures the concept of Certificate Request Generation.
FCS_INF.EXP.1	Cryptographic Key Information Query	This requirement is explicitly stated because no SFR captures the concept of Cryptographic Key Information Query.

Explicit Requirement	Identifier	Rationale
FCS_POL.EXP.1	Cryptographic Authorization Policy	This requirement is explicitly stated because no SFR captures the concept of Cryptographic Authorization Policy.
FDP_MEM.EXP.1	XML user group membership query	This requirement is explicitly stated because no SFR captures the concept of XML user group membership query.
FDP_BAU.EXP.1	Backup File Import	This requirement is explicitly stated because no SFR captures the concept of Backup File Import.

Table 12: Explicitly Stated SFR Rationale

5.7 Rationale For IT Security Requirement Dependencies

This section includes a table of all the security functional requirements and their dependencies and a rationale for any dependencies that are not satisfied.

Functional Component	Dependency	Included/Rationale
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.1	Yes
FCS_CKM.1	FCS_COP.1, FCS_CKM.4, FMT_MSA.2	Yes
FCS_CKM.4	FCS_CKM.1, FMT_MSA.2	Yes
FCS_COP.1	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	Yes
FDP_ACC.1a	FDP_ACF.1	Yes
FDP_ACC.1b	FDP_ACF.1	Yes
FDP_ACF.1a	FDP_ACC.1, FMT_MSA.3	Yes
FDP_ACF.1b	FDP_ACC.1, FMT_MSA.3	Yes
FDP_ACF.1.c	FDP_ACC.1, FMT_MSA.3	Yes
FDP_AFL.1	FIA_UAU.1	Yes
FIA_UAU.1	FIA_UID.1	Yes
FIA_UID.1	None	None
FIA_SOS.1	None	None

Functional Component	Dependency	Included/Rationale
FIA_SOS.2	None	None
FMT_MSA.1	FMT_SMR.1, FMT_SMF.1, FDP_IFC.1	Yes
FMT_MSA.2	FDP_ACC.1, FMT_MSA.1, FMT_SMR.1	Yes
FMT_MSA.3	FMT_SMR.1, FMT_SMF.1, FDP_IFC.1, FMT_MSA.1	Yes
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	Yes
FMT_MTD.1a, b, c	FMT_SMR.1, FMT_SMF.1	Yes
FPT_RVM.1	None	Yes
FPT_SEP.1	None	Yes
FPT_STM.1	None	Yes
FAU_GEN.EXP.1	FPT_STM.1	Yes
FCS_CER.EXP.1	None	None
FCS_CER.EXP.2	None	None
FCS_CER.EXP.3	None	None
FCS_CER.EXP.4	None	None
FCS_CKM.EXP.2	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	Yes
FCS_CKM.EXP.5	FCS_CKM.4, FMT_MSA.2	Yes
FCS_INF.EXP.1	FCS_CKM.1	Yes
FCS_POL.EXP.1	None	None
FDP_MEM.EXP.1	None	None
FDP_BAU.EXP.1	None	None

Table 13: SFR Dependencies

5.8 Rationale For Internal Consistency and Mutually Supportive

The selected requirements are internally consistent. The ST includes all the SFRs provided by the TOE. All operations performed on the security requirements comply with the rules and intent required by the operation in the CC. The requirements defined in the ST are not contradictory.

The selected requirements together form a mutually supportive whole by:

- satisfying all dependencies as demonstrated in **Table 13: SFR Dependencies**
- tracing security functional requirements to security objectives and justifying that tracing as demonstrated in Section 5.5
- including the SFRs FPT_RVM.1 and FPT_SEP.1 to protect the TSF
- including audit requirements to detect security-related actions and potential attacks
- including security management requirements to ensure that the TOE is managed and configured securely.

5.9 Rationale For Strength of Function Claim

The rationale for choosing SOF-basic is based on the low to moderate attack potential of the threats identified in this ST. The security objectives provide probabilistic security mechanisms and the strength of function claim is satisfied by the password management features provided by the TOE.

6 TOE Summary Specification

6.1 TOE Security Functions

The TOE consists of the following Security Functions:

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

6.1.1 Identification and Authentication

Administrator GUI & CLI Access - FIA_UID.1, FIA_UAU.1, FIA_SOS.1 FIA_AFL.1

Administrators gain GUI access to the TOE appliance by opening a secure browser session using HTTPS on the Web Management Console Computer. Upon entering the IP address of the TOE appliance, the administrator receives a logon dialog. The Administrator enters the applicable username and password, the password is hashed and compared with hashed password values within the TOE appliance database resource. If the hashed values match, then the administrator is authenticated. The TSF verifies that the Administrator password meets all criteria established by the TOE Administrator through the password management function available on the TOE. The password mechanism utilized satisfies the Strength of Function claim of SOF-Basic. It should be noted that on the 6th unsuccessful authentication attempt, accounts are locked for 60 seconds. Communication between the Administrator Management Computer and TOE Appliance is secured via SSL/TLS. Identification and Authentication for Administrators is managed by the PAM module within the underlying Operating System. It should be noted that the TOE can be configured to require client certificate authentication for the GUI (i.e. management console). If this is required it is in addition to username/password authentication, and the username must match the common field on the client certificate.

Alternatively, access to the TOE by the Administrator may be made through a serial connection via Command Line Interface (CLI) over an SSH connection. The identification and authentication process works in a similar manner as for the GUI specified above.

The password authentication mechanism is realized by a probabilistic or permutational security mechanism.

Client XML User Identification and Authentication process - FIA_UID.1, FIA_UAU.1, FIA_SOS.1 FIA_AFL.1

Client XML users are positively identified and authenticated to the TOE appliance via a certificate exchange and a username/password. Client XML users are required to present a client certificate, a valid username/password pair, or both a client certificate and a valid username/password pair to the TOE for identification and authentication (note that this is configured by an authorized administrator). If certificate based authentication is used this will take place prior to the establishment of an SSL/TLS encrypted tunnel. If the TOE is configured such that it requires username/password based authentication, this will take place after the establishment of a SSL/TLS encrypted tunnel. Successfully authentication using one of these mechanisms is always required to gain access to the TOE Appliance and TSF resources. The NAE server component of the TOE manages Identification and Authentication for Client XML users.

File Encryption Agent Identification and Authentication process – FIA_UAU.1, FIA_UID.1

FE agents are positively identified and authenticated to the TOE appliance via mutual certificate exchange. The FE agent must present a certificate to the TOE for identification prior to establishing an SSL/TLS encrypted tunnel. Once mutual authentication has been successfully performed encrypted cryptographic keys and key metadata are passed to the FE agent.

Note that when File Encryption is activated the TOE generates a self signed root CA that is only used for authentication over the File Encryption Interface. This process is transparent to all administrators and the certificate cannot be viewed. When a new FE agent is initialized the FE agent sends a certificate signing request (CSR) to the TOE. The TOE signs the CSR and sends the signed certificate and the known CA certificate back to the FE Agent. Once this process is complete the FE agent can authenticate to the TOE and receive keys and key metadata.

TOE Implementation of the Identification and Authentication Security Function

Aside from the following limited operations, the TOE requires all Client XML users and Administrators to successfully authenticate prior to allowing any other TSF mediated actions:

- 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/TLS respectively and Client XML users may negotiate version information with the TOE via the XML interface, prior to identification and authentication.

Client XML users must present a user name/password pair and/or valid certificate in order to authenticate to the TOE.

For Administrator authentication over the Management Console or CLI, the username/password pair is passed to the Administrative Library which then calls PAM (Pluggable authentication module) to perform the authentication. This authentication uses standard Unix mechanisms (i.e. comparing the username and cryptographic hash of the password, with what is stored on the in a file on the underlying Operating System). Once the Administrator is authenticated, the Administration Library then determines the Administrator's permissions by examining a configuration file. The Administrator user permissions are then passed back to the management console (or the CLI process in the case of the CLI interface) which builds the Administrator web pages or available commands based on the Administrator's permissions.

Client XML user authentication does not use the mechanisms provided by the Operating system. When a user name and password or client certificate is passed to the NAE server via the XML interface, the NAE server compares these values with those within a configuration file on the underling file system. Once the Client XML user is authenticated, this username is used to determine the Client XML user's permissions for the requested operation.

If, for example, the Client XML user has requested to perform an encryption with a specific key, the NAE server examines the configuration file in order to determine if the user has permission to use the requested key.

FE agent authentication does not use the mechanisms provided by the Operating system. The FE agent's certificate is associated with cryptographic key and key metadata information. Once the FE agent is authenticated values within the certificate are used to determine the keys and key metadata to pass to the FE agent.

Password and Certificate Management - FIA_SOS.1, FIA_SOS.2

The TOE maintains a password management function that allows the TOE Administrators to specify parameters that establish the password policy for Administrators and Client XML users. The default password requirements within the appliance require:

All passwords on the Ingrian device are subject to the same basic constraints. Passwords must contain at least five different characters.

Passwords must not:

- contain only whitespace.
- resemble a phone number, dictionary word, or reversed dictionary word.
- be based on the username associated with the password.
- contain more than 4 sequential characters.

In addition, the TOE Administrators can configure the following additional options:

- Password Expiration - specify a duration for password usage, the TSF will require a new password after reaching expiration.
- Password History – maintain a list of previously used passwords to avoid reuse

- Minimum Password Length - (default 8 characters)
- Special Characters –specify that at least one, lowercase, uppercase, number or special character be used in the password

Certificates must be used for the Common Criteria Evaluated Configuration for SSL session establishment with the NAE server as well as for Client XML users to authenticate to the TOE for cryptographic services. Additionally both client and server certificates are required to authenticate FE agents to the TOE.

Server certificates are used by the TOE to identify itself to Client XML user applications and Client XML user certificates are used to authenticate to the TOE as a prerequisite to obtain TOE cryptographic services. Certificates may be produced by the TOE and may be signed by a Certificate Authority (CA) or self signed within the TOE during setup. Certificates produced by the TOE for Common Criteria include keys with a minimum length of 1024 bits and maximum length of 2048 bits.

6.1.2 Cryptographic Services

The TOE provides encryption, decryption and key management services for Client XML users within the appliance. Client XML users request Cryptographic Services over the XML interface by requesting the operation along with specifying the key to be used for the operation. The TOE verifies that the specific Client XML user may access this key (through successful authentication) and then completes the operation and forwards the result over the XML interface back to the requesting Client XML user.

The TOE also uses cryptography to secure communications between Client XML users and the TOE and Administrators and the TOE via secure SSL/TLS or SSH sessions as described in the Secure Communications security function in Section 6.1.6.

Keys are created by authorized administrators for Client XML users by the ICS library which in turn calls libcrypto for key generation. Once a key is created it is stored along with associated information (e.g. key owner, algorithm, iv) in a directory on the operating system's underlying file system. It should be noted that the key and its associated information are stored on separate files within the underlying Linux file system.

When an authenticated Client XML user requests an operation with a specific key, the NAE server (within the appliance) first verifies that the Client XML user has access rights to that key. As stated above this information is stored within a file in the same directory as the key is stored. Once the Client XML user is authorized to use the cryptographic key, the request is passed to the ICS library which opens the key file and calls libcrypto to perform the cryptographic operation. This information is then passed back to the NAE Server. When keys are deleted by an authorized Administrator, the ICS library is called to zeroize and delete the key file, associated information and directory the key resides in.

The confidentiality and integrity of keys is maintained through a layered approach. Direct access

to any keys (and the underlying files system for that matter) is not possible through any of the TOE interface. Only indirect access to keys is provided (i.e. via the management, CLI and XML interface), and only in a controlled manner. Additionally only specific processes have access to individual keys, which is enforced by the access control mechanisms of the underlying operating system. Finally all keys are obfuscated with an obfuscation key.

Client XML user key access is limited to the Key owner or membership in an Administrator established group that has been granted explicit access by the TOE Administrator to specific key operations by group membership.

Cryptographic Key Generation - FCS_CKM.1

All cryptographic keys on the TOE are generated with the FIPS 140-2 approved PRNG ANSI X9.31 seeded with entropy generated from /dev/random. The output from X9.31 is directly used as keys for AES, TDES, HMAC-SHA-1, RC4 and SEED. For RSA and DSA key generation, the output of X9.31 is used to generate values, which are then tested for primality. If the value tests prime, RSA key generation follows as per PKCS#1.

Cryptographic Key Export – FCS_CKM.EXP.2

After mutual certificated based authentication is successful FE agents request and are sent encrypted cryptographic keys and key metadata. Keys are encrypted via the SSL/TLS cryptographic channel that is established which uses the following cryptographic algorithms for encryption: 3DES, AES, or RC4. These keys are always 256-bit AES keys. The user of the FE Agent does not have access to the keys directly. The FE Agent encrypts/decrypts on be half of the user. Keys created for FE Agents by the TOE are only used for the purpose.

If permission is granted by an authorized administrator Client XML users can also export cryptographic keys encrypted via the SSL/TLS cryptographic channel that is established which uses the following cryptographic algorithms for encryption: 3DES, AES, or RC4. The keys that can be export are the following: AES, SEED, DES, DES-EDE, RC4, HMACSHA1, RSA as per Table 7**.** It should be noted that the keys that can be exported are no different from the keys that are used by the TOE to internally perform cryptographic operations on data.

Cryptographic Key Destruction within the TOE - FCS_CKM.4

When a key is deleted on the TOE it is actively zerorized to ensure that the value does not inadvertently remain in memory. This is true for all secret and private key material used on the TOE and is performed by cryptographic services by overwriting the key.

Cryptographic Key Import – FCS_CKM.5

Authorized administrators can import the following encrypted cryptographic keys AES, SEED, DES, DES-EDE, RC4, HMACSHA1, RSA as per Table 15 via an SSL/TLS cryptographic channel that is established which uses the following cryptographic algorithms for encryption: 3DES, AES, or RC4. This is performed through the management console when creating a new key.

TOE usage of Cryptography Operations - FCS_COP.1

The TOE utilizes cryptography for the purpose of encryption and decryption sensitive data on behalf of Client XML users via the XML interface.

All cryptographic functionality on the TOE is performed using established and peer reviewed cryptographic algorithms. The following table presents an overview of cryptographic algorithms, key sizes and associated standards:

Cryptographic Algorithm	Key sizes	Standard
AES	128, 192 and 256-bit	FIPS PUB 197
TDES	112, 168-bit	FIPS PUB 46-3
HMAC-SHA-1	160-bit	FIPS PUB 198
RC4	128-bit	RFC 4345
SEED	128-bit	RFC 4269
RSA – Encrypt/Decrypt	1024, 2048-bit	PKCS#1
RSA – Sign/Verify	1024, 2048-bit	PKCS#1
DSA	1024-bit	FIPS PUB 186-2

Table 14: Cryptographic Algorithms & Key usage

Certificate Authority Operations – FCS_CER.EXP.1, FCS_CER.EXP.2, FCS_CER.EXP.3, FCS_CER.EXP.4

Certificates can be imported encrypted with SSL/TLS via the management console interface or through SCP. In the Common Criteria evaluated configuration the IngrianOS guide specifies that certificates should not be imported through FTP.

Cryptographic Authorization Policies – FCS_POL.EXP.1

Authorized administrators can set cryptographic authorization policies on cryptographic keys. Policies can be set to limit the number of cryptographic operations per hour from between 1-500,000,000. Authorized time periods of usage of the cryptographic key can also be set. These policies are not enabled by default and therefore do not limit the authorized usage of a key unless configured.

Use of Secure Values for Security Attributes - FMT_MSA.2

The TOE assures that only secure security attributes are allowed in the TOE for Cryptographic operations. The TOE by design and by selected configuration items allows only the algorithms listed in Table 14 are used for Cryptographic Encryption/Decryption Operations and for securing Client XML users, TOE Administrators and FE agent communication with the DataSecure appliance. In addition, options which may allow communications over unsecured protocols (http) or unapproved cryptographic methods are disabled through Administrator configuration of the appliance for the CC Evaluated Configuration.

Transfer of Key Information to Client XML users – FCS_INF.EXP.1

Client XML users can request that the server return information about a specified key or about all of the keys available to the client. The client can request information about a specific key by using the <KeyInfoRequest> element.

Client XML users can request the server to return information about all keys available to the client by using the <KeyQueryRequest> element. For authenticated clients, this request will query keys owned by the client, and keys for which the client has some defined permissions.

For both individual and multiple key queries, the Appliance returns information such as the algorithms that can be used with the key, the size of the key, whether the key is exportable and/or deletable, and the permissions that the client has for the specified key (encrypt, decrypt). In addition, the Appliance returns the fingerprint of the key. If the request is for information about the public key from a certificate, then the server omits the fingerprint information in the response.

6.1.3 Audit

The TOE provides a comprehensive audit logging capability to identify TSF access, modification of TSF settings and service requests received by the appliance from Client XML users for cryptographic processing.

Audit Record Generation and TOE Logging Types - FAU_GEN.EXP.1

The generation of audit records represents a key functionality of the TOE and as such cannot be

turned off, which ensures that the audit functionality can never be bypassed.

Audit records generated by the TOE are grouped into three distinct types. These are the Audit Log, the NAE Log and the System Log. The Audit Log records administrative access to the TOE via both the management console and the CLI. This includes both successful and unsuccessful authentication attempts and all configuration changes made to the TOE as well as all requests by the Administrator. The NAE Log records Client XML user access to the TOE via the XML interface. This includes both successful and unsuccessful authentication attempts and all Client XML user requests including the name of the key being used (if relevant). The System Log records information regarding system services (e.g. starting and stopping of SNMP and network configuration changes). TOE actions related to the FE agent are recorded in both the audit log and the file system tools log file. The latter store audit data such as key and meta data key push and export, the former stores administrator initiated actions related to file encryption (e.g. initiate a key push to a specific FE agent).

Audit logs generated by the FE Agent and uploaded to the TOE are not considered TSF data. These audit logs include information to uniquely identify the originator as well as timestamp information that is generated by the FE agent.

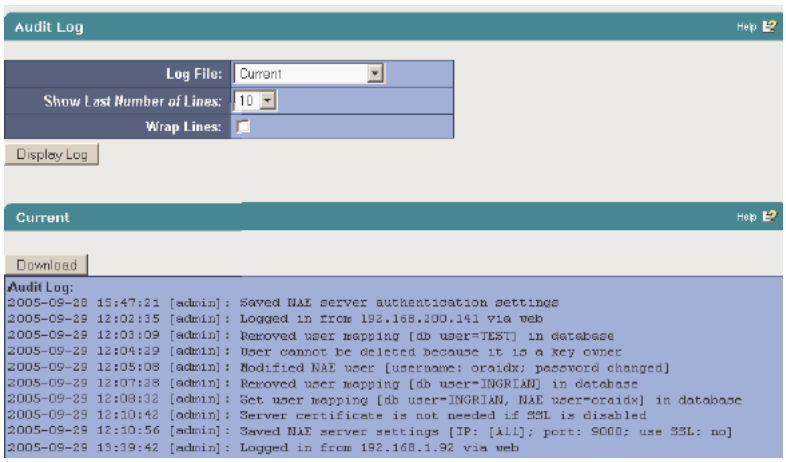
There are two logging levels that may be configured on the Ingrian appliance:

- Log Normal: All messages including system errors are recorded. This is the default and recommended level.
- Log Low: Successful configuration changes and Administrator user input errors are recorded.

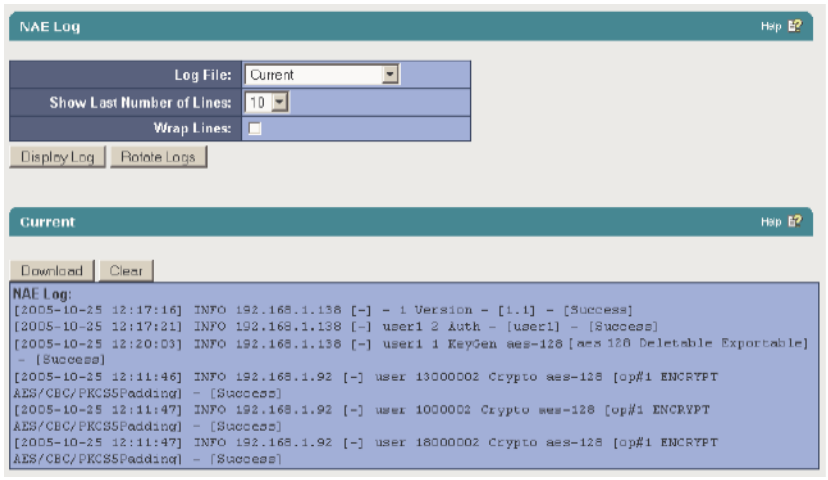
The Common Criteria Evaluated Configuration requires the use the “Log Normal” setting to assure all events are available for administrator review. Furthermore these settings do not affect what is audited by the TOE (which is not configurable), only what audit information is displayed.

Within each audit record, at least the following information is recorded: date and time of event, user or process identity, class or type of event and a description of the event (which includes the outcome of the event). Audit records are accessed by the Administrator through the Web Console.

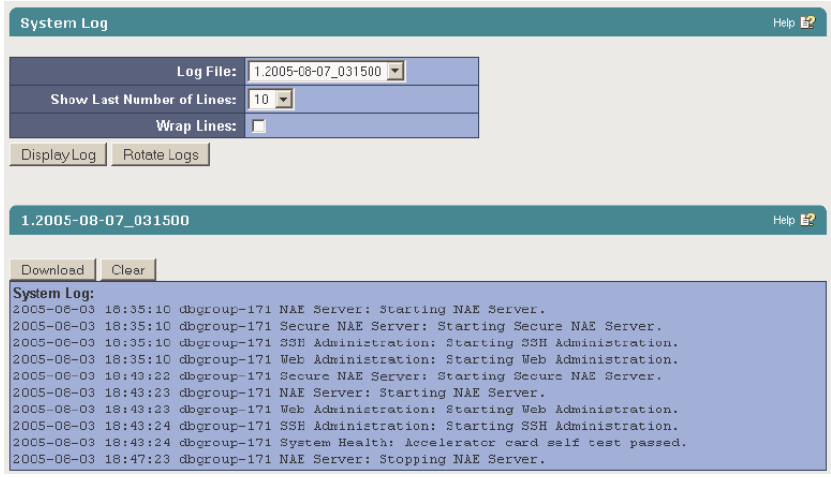
Audit records define the entity that generated each audited event. Administrators are identified in audit records by Username and Client XML users are identified by IP address and User ID which is an identification number assigned to the User when established by the TOE Administrator. FE agents are identified by name and IP address.



Administrator Log example



NAE Log example



System Log Example

Timestamps use in Audit Records - FPT_STM.1

The TOE generates timestamps based on the hardware clock on the motherboard. When a process generates an audit event, this time is gathered from the operating system and written to the audit log along with the auditable event.

Audit Records associated by Users - FAU_GEN.2, FAU_SAR.1

Audit records generated by the TOE are associated with the user identity that caused the event. For the Audit and NAE logs the Administrator or Client XML user who generated the event is included. In the case of the System log the process (e.g. SNMP) represents the user identity associated with each event.

All TOE Administrators have the capability to read all audit information generated by the TOE.

TOE Implementation of the Audit Security Function

All audit records are stored in files within a central location on the underlying Linux Operating System. Processes responsible for generating audit logs write audit events to these files in a syslog like format. The following represents an example audit event:

```
2006-09-25 11:32:32 [Administrator] [Login] [Login]: Logged in from 192.168.1.179 via web
```

The audit functionality is hard coded into these processes and cannot be configured or turned off. The primary processes that record audit events are the administration Libraries which audit all interaction through the management console and CLI and the NAE Server which records all Client XML user access via XML, including all access to cryptographic keys. The system log represents system level events generated by processes running on the TOE (for example the starting and stopping of NAE Server or rebooting of the TOE). A separate process called logmanager is responsible for rotating log files.

When an authorized administrator requests to view an audit log, the administration library reads the required files from the central location on the operating system and passes them to the CLI or Management Console for display.

The TOE does not provide the functionality to directly access the audit files (i.e. there is no shell access to the underlying Linux OS), and all access to the audit logs must be through the CLI or Management Console.

TOE Protection of Audit Records and Prevention of Loss - FAU_STG.1, FAU STG.4

The TOE ensures that Audit Log records cannot be manipulated or individually deleted. Once full, the TOE will begin to overwrite the oldest records first to maintain the most recent records within the audit log repository. The TOE must be configured to transfer log files via SCP before the log file is rotated.

6.1.4 Access Control

Access Control - FDP_ACC.1a, FDP_ACC.1b, FMT_SMR.1, FDP_MEM.EXP.1

The TOE provides access control mechanisms that assure only properly identified and authenticated (Administrator/Client XML) users can access TSF resources. In addition, the TOE maintains (Administrator/Client XML) user attributes by assigned role to facilitate different access levels to different classes of (Administrator/Client XML) users. Administrators can access all security management and appliance configuration screens of the TOE appliance whereas Client XML users are limited to communicating exclusively through XML and can only poll appliance status and participate in cryptographic operation exchanges (requests etc).

The access control mechanisms of the TOE are based around three classes of users, Client XML users, FE agents and Administrators.

In the case of Administrators, after an administrator is successfully authenticated, the administrator's permissions are determined by examining a configuration file on the underlying file system in conjunction with the programmable authentication module (PAM) functionality. This information is then used to build the set of commands or WebPages provided to that administrator.

Client XML users are authenticated by examining a configuration file on the underlying file system, the Client XML user's group membership is also determined at that time (if that Client XML user is a member of any groups). This information is then used to determine the Client XML users access rights to specific keys on the TOE. When a Client XML user requests an operation with a specific key, a configuration file associated with that key is examined to determine if the Client XML user is the owner of the key (in which case all cryptographic operations with that key are allowed) or if the users groups have access rights to that key. If any of the Client XML users groups have access rights to the key, the allowed operations of that group are checked against the Client XML users requested operation (e.g. decrypt). Only if the operation is allowed will it then proceed.

Access Control Client XML users – group memberships

The TOE has provisions for groups to be created to use specified key resources based on a policy established by the Administrator. If an owner is listed for the key, then that owner is the only Client XML user who can access the key (unless additional group permissions have been granted for the key). When the Client XML user contacts the TOE appliance to request a key operation, the User ID is verified first to determine if they are the key's owner, then if they are not the keys owner, the group permissions are queried to determine if the requester is a member of a group that has key usage permissions.

Group permissions can be assigned to a key. For example, you might give members of Group1 permission to encrypt and members of Group2 permission to decrypt. Using authorization policies, you can set usage limitations for keys.

Take for example a scenario where the following permissions are assigned for key1:

Group	Encrypt	Decrypt	Sign	Sign Verify
group1	always	never	policy1	policy2

In this example members of group1 have permission to use key1 to encrypt always, decrypt never, sign according to policy1, and sign verify according to policy2. The owner of the key implicitly has permissions to perform all applicable operations using the key, even if that user belongs to a group for which permission to use the key is explicitly restricted.

If a Client XML user is listed in two groups that contain different permissions for a given key, the user will have the most permissive access of the groups' permissions. If a user is not the owner and is not a member of any group with permissions to use the key, that user cannot access the key for any operation.

Key access policies are determined by key assignment, therefore, a Client XML user must either be the key owner or be a member of a group with an explicit permitted operation. All other access to any operation related to that key is prohibited.

Authorized XML users can query the TOE to determine their group membership. Note that the TOE must be configured so that users do not have NAE user administrator permissions or change password permissions.

Access Control Rules - FDP_ACF.1a, FDP_ACF.1b

The TOE enforces the Ingrian Access Control SFP based on Key access (by Client XML Users) and TOE access to configuration items by Administrators. These Access Control Roles are established, in part, by the configuration of security attributes which support the enforcement of the Ingrian Access Control SFP. A detailed description of these security attributes, their management and related access restrictions are contained under Security Management (Section 6.15)

Client XML users interact with the TOE through the XML interface based on the following rule: A Client XML user may access Cryptographic Services based on their assigned Client XML user profile, successful certificate based authentication, and configured permissions to access specified keys and associated cryptographic processes.

Once Client XML users are created on the TOE cryptographic keys can be created and key ownership assigned to specific Client XML users. The key owner can perform all cryptographic operations with that key. Keys can also be associated with groups of Client XML users and specific cryptographic operations can be assigned to that group (e.g. encrypt but not decrypt).

Administrators interact with the TOE through the management interface (i.e. web interface) and the CLI (over SSH or Serial connection) based on the following rule: An Administrator may access specific appliance configuration objects if they are authenticated in the Administrator role with the required permissions.

Administrators can be created with access to a variety of administrative functions and access to appliance configuration objects (essentially all administrative functionality can be granted or denied). While the appliance supports the creation of multiple Administrator type users with various levels of local access on the appliance, at least one administrator must have at least the ability to create other administrators (i.e. Administrator Configuration access control). It should be noted that after installation the initial administrator account can be deleted as long as at least one other administrator account has been created with create administrator permissions.

6.1.5 Security Management

The TOE appliance provides a comprehensive set of management functions that allow TOE administrators to establish and manage Client XML users and Administrators, configure cryptographic functionality and usage rules, establish and manage the access control polices and permissions among Administrator/Client XML users. Access to the Security Management function requires that the Administrator is identified and authenticated to the TOE as noted in Section 6.1.1. Client XML Users do not access the TOE for the purposes of security management as they access the TOE solely for the purposes of receiving cryptographic services, exclusively via the XML interface.

In the evaluated configuration of the TOE, "Allow Key and Policy Configuration Operations" must not be enabled. Therefore no management operations are allowed via the XML interface.

Management Functions provided by the TOE - FMT_SMF.1, FDP_BAU.EXP.1

The specific security management functions provided by the TOE include:

Administrator Management functions which allow administrators to create and manage TOE Users (Administrators/Client XML users), including setting roles and password guidelines

Group Management functions which allow administrators to create and manage groups for the purpose of allocating cryptographic services to groups of Client XML users

Key Management and Certificate management functions which allow Administrators to create Key Pairs and Certificates for Client XML users and configure permissions for specific Client XML users (groups) to utilize specific keys for encryption and decryption

Access control attributes which specify permissions for access to the TOE and the TOE's cryptographic resources.

The TOE provides the ability for the TOE Administrator to initially configure the time & date on the appliance and make subsequent modifications to these values as necessary.

Authorized administrators can import backup files in order to restore backup configuration settings.

Exporting cryptographic keys and key metadata to FE agents.

Management of the TSF Data and Restrictions – FMT_MTD.1a, FMT_MTD.1b, FMT_MTD.1c

The TOE utilizes the appliance access control mechanisms to restrict access to TSF data and limit which (Administrator) users may access or manipulate this data. All access to TSF data requires that the (Administrator) user be authenticated in the Administrator role. Through this mechanism, the TSF restricts the ability to query, modify or delete:

- Client XML user and Administrator data including role assignment and passwords.
- Cryptographic TSF data including Key Assignments, Key attributes and SSL/TLS certificates

The TOE restricts the ability to query audit and logging records through these mechanisms to Administrators. Audit/Log records cannot be modified or deleted by design in the TOE, therefore, no Administrator, regardless of privileges can modify or delete audit records.

The TOE restricts the ability to modify the time & date maintained by the TOE (and reflect in audit records) to the Administrator.

Management of TOE Security Attributes – FMT_MSA.1, FMT_MSA.2

The TOE provides mechanisms for the management of security attributes through the Security Management security function. Through configuration of these attributes, the Administrator establishes the basis for the enforcement of the Ingrian Access Control SFP and access to these security attributes are restricted based on authenticated role.

The TOE enforces the Ingrian Access Control SFP to restrict the ability to query, modify or delete the following security attributes:

- Cryptographic key characteristics including Key Type (Algorithm, Key Length) and Client XML user usage permissions
- Administrator related security attributes including Access Control attributes such as role assignments, password policy and configured key usage permissions by Client XML users.

Mechanisms within the TOE enforce that only secure values are allowed for security attributes within the TOE. The TOE enforces that only secure connections to the TOE are allowed by both Administrator and Client XML users (see 6.1.6 Secure Communications) using secure cryptographic keys and usage attributes. Authentication is enforced prior to granting access to these secure attributes by either Administrator or Client XML users.

Client XML user and Cryptographic Security Attribute Initialization –FMT_MSA.3a

The TOE maintains restrictive default values (values that deny access) for most security attributes within the appliance and all security attributes which relate to Client XML users and Cryptographic functionality to include the following examples:

- When a key is created, only a key name and algorithm must be specified and all other values must be added by an authorized administrator. This creates restrictive default

values.

- When a Client XML user is created, only a username and password must be specified. All other values must be actively selected by the appliance Administrator. This creates restrictive default values.
- When Client groups are created only a group name must be specified. All other values must be actively selected by and authorized Administrator. This creates restrictive default values.
- Key usage by Client XML users is established by the appliance Administrator and without granting of explicit permission, access and use of the key is prohibited. This creates restrictive default values.

Administrator Security Attribute Initialization –FMT_MSA.3b

While the TOE uses restrictive default values for most security attributes by default, when new Administrators are created, the defaults enable broad access to TOE functions. The logical step in configuring a new Administrator is creating the user and then configuring the permissions, however, the default values are permissive in that they begin as all inclusive.

- For example, when Administrators are created a username and password must be selected. By default all possible administrator functions are enabled. This creates permissive default values.

6.1.6 Secure Communications

FCS_COP.1

All communications to the TOE are secured via fully authenticated SSL/TLS sessions using an algorithm listed in Table 14. For Administrative sessions, communication is established either through a browser based HTTPS session for GUI access or through a SSH based CLI session using a workstation in the IT Environment. Identification and Authentication to the TOE must be completed before access is allowed as described in Section 6.1.1.

Communications between the TOE and Client XML users in the network environment is executed exclusively through the XML interface using SSL/TLS. Communication over this interface using unencrypted sessions is not allowed except during initial session initiation and certificate exchanges processes. Identification and Authentication to the TOE must be completed for Client XML users before cryptographic service requests can be processed as described in Section 6.1.1.

Additionally all communication between the TOE and FE agents is encrypted with SSL/TLS. It should be noted that the default session time out period for SSL/TLS is 7200 seconds, however this can be configured by an authorized administrator.

Use of cryptography for secure communications utilizes the same key usage procedures as described in 6.1.2 under Cryptographic Services.

6.1.7 Protection of the TOE

Domain Separation & Non-bypassibility of the TSP

Protection of the TOE from physical and logical tampering is ensured by the physical security assumptions and by the domain separation requirements on the TOE. A secure session is required to be established prior to allowing TSF access and operating system based access controls restrict TSF access to Administrators only.

Non-Bypassibility - FMT_RVM.1

The TSP enforcement functions that must be invoked and succeed before the functions within the TSC are allowed to proceed include the following:

- Identification and authentication: these functions ensure that no unauthorized users can gain access to the TOE.
- Access Control prior to access to any TOE operation: these functions ensure that authorized users only gain access to the functions and objects to which they are authorized.

Domain Separation - FMT_SEP.1

The TOE maintains domain separation by providing a restricted domain in which all users of the TOE interact. This domain, which is effectively a sandbox, represents the environment provided by the management console, CLI, FE Interface and XML interface. There are no mechanisms which allow any user access directly with the underlying operating system.

6.2 Security Assurance Measures

The following table maps assurance requirements to assurance components.

Assurance Requirement	Assurance Components
ACM_CAP.2	The configuration management documentation.
ADO_DEL.1	The delivery documentation.
ADO_IGS.1	The installation, generation, and start-up procedures.
ADV_FSP.1	The informal functional specification.
ADV_HLD.1	The descriptive high-level design.
ADV_RCR.1	The informal correspondence demonstration is provided in <title>.
AGD_ADM.1	The administrator guidance documentation.
AGD_USR.1	The user guidance documentation

Assurance Requirement	Assurance Components
ATE_COV.1	The evidence of coverage.
ATE_FUN.1	The functional testing description.
ATE_IND.2	The TOE and testing documentation were made available to the CC testing laboratory for independent testing.
AVA_SOF.1	The strength of function analysis.
AVA_VLA.1	The vulnerability analysis.
ALC_FLR.1	The Flaw Remediation documentation.

Table 15: Assurance Requirements: EAL2 Augmented ALC_FLR.1

6.3 Rationale for TOE Security Functions

This section provides a table demonstrating the tracing of TOE security functions back to aspects of the security functional requirements (SFRs).

A justification that the security functions are suitable to cover the SFRs can be found in Section 6.1.

	ID and Authentication	Cryptographic Services	Audit	Access Control	Security Management	Secure Communications	Protection of the TOE
FAU_GEN.2			X				
FAU_SAR.1			X				
FAU_STG.1			X				
FAU_STG.4			X				
FCS_CKM.1		X					
FCS_CKM.4		X					
FCS_COP.1		X				X	
FDP_ACC.1a				X			
FDP_ACC.1b				X			
FDP_ACC.1c				X			
FDP_ACF.1a				X			

	ID and Authentication	Cryptographic Services	Audit	Access Control	Security Management	Secure Communications	Protection of the TOE
FDP_ACF.1b				X			
FDP_ACF.1c				X			
FIA_AFL.1	X						
FIA_UAU.1	X						
FIA_UID.1	X						
FIA_SOS.1	X						
FIA_SOS.2	X						
FMT_MSA.1					X		
FMT_MSA.2		X			X		
FMT_MSA.3a					X		
FMT_MSA.3b					X		
FMT_MSA.3c					X		
FMT_SMF.1					X		
FMT_SMR.1				X			
FMT_MTD.1a					X		
FMT_MTD.1b					X		
FMT_MTD.1c					X		
FPT_RVM.1							X
FPT_SEP.1							X
FPT_STM.1			X				
FAU_GEN.EXP.1			X				
FCS_CER.EXP.1		X					
FCS_CER.EXP.2		X					

	ID and Authentication	Cryptographic Services	Audit	Access Control	Security Management	Secure Communications	Protection of the TOE
FCS_CER.EXP.3		X					
FCS_CER.EXP.4		X					
FCS_CKM.EXP.2a		X					
FCS_CKM.EXP.2b		X					
FCS_CKM.EXP.5		X					
FCS_INF.EXP.1		X					
FCS_POL.EXP.1		X					
FDP_MEM.EXP.1				X			
FDP_BAU.EXP.1					X		

Table 16: TOE Security Function to SFR Mapping

6.4 Appropriate Strength of Function Claim

The claim of SOF-basic for the Identification and Authentication security function is consistent with the claim of SOF-basic for the FIA_UAU.1 SFR that maps to that security function.

6.5 Rationale for Security Assurance Measures

The assurance documents listed below were developed to meet the developer action and content and presentation of evidence elements for each assurance required defined in the CC.

The documentation titles in the table below will be updated with new titles and version numbers during the course of the evaluation.

Assurance Requirement	Assurance Rationale
ACM_CAP.2	The configuration management documents defines the configuration items and contains the necessary information to demonstrate that a CM system is used and that there is a unique reference for the TOE.

Assurance Requirement	Assurance Rationale
ADO_DEL.1	The delivery document describes the steps performed to deliver the TOE. It describes the process used to create distribution copies of the TOE software and the steps taken to ensure consistent, dependable delivery of the TOE to the customer.
ADO_IGS.1	The installation, documents describe the steps necessary for secure installation, generation and start-up of the TOE.
ADV_FSP.1	The informal functional specification document identifies the external interfaces that completely represent the TSF and describes the purpose and method of use of all external TSF interfaces. It also describes the effects, exceptions, and error messages for each of the external TSF interfaces.
ADV_HLD.1	The descriptive high-level design describes the complete TSF in terms of subsystems. The security functions for each subsystem are described. The subsystem interfaces are defined and the externally visible interfaces are identified.
ADV_RCR.1	The informal correspondence document maps the security functionality as described in the FSP and ST and as described in the FSP and HLD.
ALC_FLR.1	Flaw Remediation outlines the sponsor's process to address security related product issues
AGD_ADM.1	The administrator guidance documents provide complete administrative guidance for the TOE, including all security features and configuration items.
AGD_USR.1	The User guidance documents provide complete User guidance for the TOE.
ATE_COV.1	The test coverage document provides a mapping of the test cases performed against the TSF.
ATE_FUN.1	The functional testing document includes the test plans, test procedures, and associated test cases of the TOE functional testing effort.
ATE_IND.2	The TOE hardware, software, guidance, and testing documentation were made available to the CC testing laboratory for independent testing.

Assurance Requirement	Assurance Rationale
AVA_SOF.1	The strength of function analysis document provides the SOF argument for the password mechanism.
AVA_VLA.1	The vulnerability analysis document identifies and describes the process used to discover obvious vulnerabilities, the results of the vulnerability analysis, and the mitigation of each identified obvious vulnerability.

Table 17: Rationale for Security Assurance Measures

7 Protection Profile Claims

This Security Target does not claim conformance to any Protection Profiles.

8 Rationale

This Security Target does not claim conformance to any Protection Profiles.

8.1 Security Objectives Rationale

Sections 4.3 - 4.6 provide the security objectives rationale.

8.2 Security Requirements Rationale

Sections 5.5 - 5.9 provide the security requirements rationale.

8.3 TOE Summary Specification Rationale

Sections 6.3 - 6.5 provide the TOE summary specification rationale.

8.4 Protection Profile Claims Rationale

This Security Target does not claim conformance to any Protection Profiles.