Sterling Commerce, Inc.

Gentran Integration Suite v4.2

Security Target

Release Date 1/22/2007

Version 0.7

Prepared By:

Corsec Security Inc.
10340 Democracy Lane
Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050
Fax: (703) 267-6810

Prepared For:

Sterling Commerce, Inc.
Dublin, Ohio

Document History

Release Number	Date	Author	Details
D 0.4	2006/5/16	Elisabeth Sullivan	Third Vendor Review Draft
D 0.5	2006/09/11	Mac Causey	Addressed verdicts from PETR v0.1 and v0.2
D 0.6	2006/12/19	Teresa MacArthur	Addressed informal verdicts from Dec 8, 2006 and verdicts from PETR v0.3.
D 0.7	2007/01/22	Amy Nicewick	Addressed verdicts from PETR REQ_CR_1 received 1/02/2007

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target, 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:	Sterling Commerce Inc. Gentran Integration Suite 4.2[1]
ST Identification:	Sterling Commerce Inc. Gentran Integration Suite 4.2 Security Target[2]
ST Publication Date:	1/22/2007
ST Version:	Draft 0.7
Authors:	Elisabeth C. Sullivan
Keywords:	Business to Business, Trading Partners, Electronic Data Interchange, EDIINT AS1 and AS2

1.2 Conformance Claims

- The TOE is Common Criteria Version 2.3 (ISO/IEC 15408) Part 2 conformant.
- The TOE is Common Criteria Version 2.3 (ISO/IEC 15408) Part 3 conformant.
- The TOE is conformant with Assurance Package EAL2 augmented with ALC_FLR.1
- The TOE is compliant with all International interpretations with effective dates on or before kickoff date[3].
- This TOE is not conformant to any Protection Profiles (PPs).

1.3 Product Overview

Gentran Integration Suite is a transaction engine that runs processes defined and managed according to business needs. The platform supports high volume electronic message exchange, complex routing, translation, and flexible interaction with multiple internal systems and business partners. Gentran Integration Suite allows businesses to:

- tie together applications, processes, data and people, both within and outside the organization.
- offer flexible options for deployment, configuration and customization, including the ability to add capabilities one at a time
- complement rather than disrupts critical existing systems
- provide a robust security infrastructure

[1] Gentran Integration Suite 4.2 will also be referred to as GIS 4.2 or GIS throughout this document.

[2] Gentran Integration Suite 4.2 Security Target will also be referred to as GIS ST, or ST, throughout this document

[3] May 19, 2006.

- include innovative visual management tools for easy configuration and visibility into work flows, system and trading partner activity, translation maps, and business process implementation, and
- work with existing and emerging business and communication standards.

Combined, this functionality enables an enterprise to configure Gentran Integration Suite components to enable secure information exchange between Business to Business trading partners or Business group to Business group within a single company.

The following diagram illustrates the path data takes from the applications of an enterprise to the enterprise's trading partner community. Enterprise Application Integration (EAI) components and B2B services facilitate the transfer of information while the Gentran Integration Suite processing engine, the Integration Broker, manages the processes and formats data appropriately for the final destination.

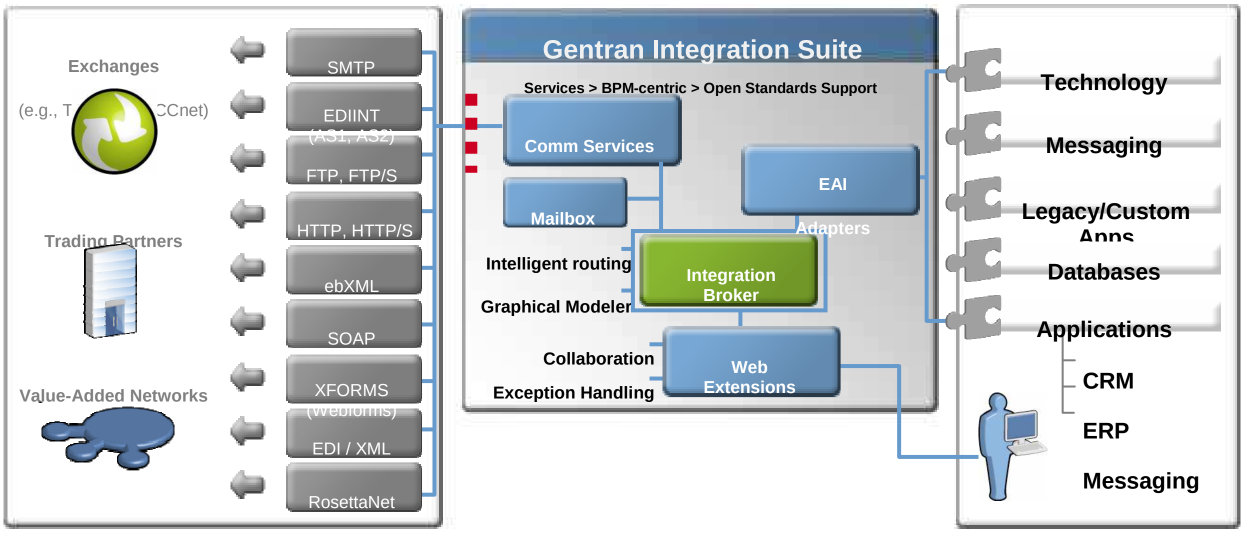

Figure 1-1: GIS Data Exchange Overview

GIS features include the following:

- **Internationalization and Localization Support:** Gentran Integration Suite supports multiple languages (internationalization) and multiple regional data formats (localization) by using encoding and XML resource bundles.
- **Predefined Business Process Models:** Gentran Integration Suite provides a limited number of predefined business process models that can be used when creating models for business processes.
- **Trading Profile Management:** Gentran Integration Suite uses trading profiles to simplify configuration of data related to trading partners. A *trading profile* is a collection of records that describe the technology, business capabilities, and communication capabilities of a trading partner to engage in e-business with other trading partners. Gentran Integration Suite uses the trading profile data to link the trading partner with the business process models created to handle that partner's documents.
- **Advanced File Transfer:** Gentran Integration Suite Advanced File Transfer (AFT) features provide reliable, secure, scalable B2B content distribution and Web services across business boundaries, communication modes, and document formats.
- **Mailbox Service:** Gentran Integration Suite includes a mailbox service that provides store-and-forward capabilities. The mailbox service can be configured to organize, store, monitor, and manage trading partner documents and transactions.

- **Tracking and Searching Capabilities:** Gentran Integration Suite provides several features to help monitor operations, track the state of data in processes, and search for the specific information.
- **Remote administration:** Gentran Integration Suite provides a remote management capability via a browser-based Graphic User Interface (GUI).

GIS also provides the following:

- An administration layer as a single point of access for configuring, monitoring, and managing the system and its integration activities
- Tracking services that trace the flow of information as a business process runs
- Monitoring, which enables viewing business processes as they run
- Logging, which records system events such as GIS user interaction, administration, and the execution of business processes
- Event notifications that provide alerts in response to events or exceptions, using mechanisms such as e-mail or pagers

GIS 4.2 can operate on any of the following hardware/OS platforms

- Windows 2003 /Pentium III 1.3 GHz
- SUN Solaris 10 / SPARC 32 bit
- IBM AIX 5.3
- HPUX 11i
- HPUX 11.23 for IA64 (Itanium)
- Red Hat Enterprise Linux ES Release 3
- SuSE Linux Enterprise Server 9

GIS 4.2 can use any of the following databases:

- MySQL 4.0.18
- SQL Server 2000 SP4 Enterprise & Standard
- Oracle 9i Database Enterprise release 2 (9.2.0.6) and Oracle Database 10g Enterprise Edition Release 1 (10.1.0.4)
- DB2 v8.1 fix pack 5

1.4 ST Organization

- Security Target Introduction (Section 1) – Provides identification of the TOE and ST, conformance claims, an overview of the TOE, this overview of the content of the ST, document conventions, and relevant terminology
- TOE Description (Section 2) – Provides a description of the TOE components and IT security features as well as the physical and logical boundaries for the TOE
- TOE Security Environment (Section 3) – Describes the threats, organizational security policies, and assumptions pertaining to the TOE.
- TOE Security Objectives (Section 4) – Identifies the security objectives for the TOE and its

supporting environment as well as a rationale that objectives are sufficient to counter the threats identified for the TOE

- Functional and Assurance Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) met by the TOE, the Strength of Function claims for the requirements, and the security functional requirements rationale. In addition this section presents Security Assurance Requirements (SARs) met by the TOE as well as the assurance requirements rationale.

- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE that satisfy the security functional requirements, provides the rationale for the security functions, and the rationale for the security function SOF claim. It also describes the security assurance measures for the TOE as well as the rationales for the assurance measures.

- Protection Profile Claims (Section 7) – Presents the rationale concerning compliance of the ST with Protection Profile (PP) conformance

- Rationale (Section 8) – Provides pointers to all rationale sections, to include the rationale for the selection of IT security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability

1.5 Conventions

1.5.1 Convention for Operations

The CC defines four operations on security functional requirements. The conventions below are used in this ST to identify the operations performed.

Assignment	**[bold text in square brackets**]
<u>Selection</u>	<u>[underlined text in square brackets]</u>
Refinement	[*italicized text in square brackets*]
Iteration	indicated with a typical CC requirement naming followed by a lowercase letter enclosed in square brackets e.g. FAU-SEL.1.1[a]

1.5.2 Convention for Interpretations

Security Functional Requirements and Security Assurance Requirements are footnoted in cases where CCIMB interpretations preceding the Evaluation Kickoff Date are used in the statement of the requirements. The footnote identifies the number of the specific interpretation used.

1.6 Terminology

1.6.1 CC Terms

In the Common Criteria, many terms are defined in Section 3 of Part 1. A subset of those definitions is included in the list below. They are listed here to aid the reader of the Security Target.

Assurance Grounds for confidence that an entity meets its security objectives.

Attack potential The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.

Authentication data Information used to verify the claimed identity of a user.

Authorised user A user who may, in accordance with the TSP, perform an operation.

CC Common Criteria

CCIMB Common Criteria Information Management Board

Evaluation Assessment of a PP, a ST or a TOE, against defined criteria

Evaluation Assurance Level (EAL) A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.

External IT entity Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Human user Any person who interacts with the TOE.

Identity A representation (e.g. a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym.

Object An entity within the TSC that contains or receives information and upon which subjects perform operations.

Product A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.

Role A predefined set of rules establishing the allowed interactions between a user and the TOE.

Secret Information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.

Security Assurance Requirement (SAR) Standard way of expressing security requirements of a product.

Security attribute Characteristics of subjects, users, objects, information, and/or resources that are used for the enforcement of the TSP.

Security Function (SF) A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Function Policy (SFP) The security policy enforced by an SF.

Security Functional Requirement (SFR) Standard way of expressing security functions of a product.

Security objective A statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions.

Security Target (ST) A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Strength of Function A qualification of a TOE security function expressing the minimum

(SOF) efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

Subject An entity within the TSC that causes operations to be performed.

Target of Evaluation (TOE) An IT product or system and its associated guidance documentation that is the subject of an evaluation.

TOE Security Functions (TSF) A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP

TOE Security Policy (TSP) A set of rules that regulate how assets are managed, protected, and distributed within a TOE

TSF data Data created by and for the TOE, that might affect the operation of the TOE

Trusted path A means by which a user and a TSF can communicate with necessary confidence to support the TSP.

User Any entity (human user or external IT entity) outside the TOE that interacts with the TOE

User data Data created by and for the user that does not affect the operation of the TSF.

1.6.2 ST Specific Terms and Acronyms

These terms are specific to this ST, or are refinements of CC terminology to clarify specific meanings of the term in this ST.

Adapter Adapters are GIS services that must receive data from outside systems or send data to outside systems. Adapters interact with systems such as applications, middleware or business partners via the Internet.

AFT Advanced File Transfer features provide reliable, secure, scalable B2B content distribution and Web services across business boundaries, communication modes, and document formats.

AS1, AS2 Applicability Statement 1 (AS1) and Applicability Statement 2 (AS2) are specifications for Electronic Data Interchange (EDI) communications between businesses using e-mail protocols. They were created by the EDIINT working group of the IETF.

Audit The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures

Audit Trail In an IT System, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized

Authentication To establish the validity of a claimed user or object

B2B Business to Business

Business Process A combination of linked software services and human activities that accomplishes a business goal.

Confidentiality Assuring information will be kept secret, with access limited to appropriate persons

EAI Enterprise Application Integration is a business computing term for the plans, methods, and tools aimed at modernizing, consolidating, and coordinating the computer applications in an enterprise. Typically, an enterprise has existing legacy applications and databases and wants to continue to use them while adding or migrating to a new set of applications that exploit the Internet, e-commerce, extranet, and other new technologies. EAI may involve developing a new total view of an enterprise's business and its applications, seeing how existing applications fit into the new view, and then devising ways to efficiently reuse what already exists while adding new applications and data.

EDI Electronic Data Interchange (EDI) is the computer-to-computer exchange of structured information, by agreed message standards, from one computer application to another by electronic means and with a minimum of human intervention. In common usage, EDI is understood to mean specific interchange methods agreed upon by national or international standards bodies for the transfer of business transaction data, with one typical application being the automated purchase of goods and services.

EDIINT Electronic Data Interchange-Internet Integration (EDIINT) working group of the Internet Engineering Task Force (IETF), created to promote the use of the Internet for secure, reliable, and nonrepudiable transactions.

The EDIINT working group developed Applicability Statements 1, 2, and 3 (AS1, AS2, and AS3) to use SMTP e-mail, HTTP, and FTP, respectively, to achieve this goal. AS1, AS2, and AS3 all use encryption and digital signatures to ensure secure transmissions and appropriate handshaking to ensure reliability and nonrepudiation.

FIPS 140-2 Federal Information Processing Standards (FIPS) 140-2 is a standard for certification and validation process for cryptographic modules.

FTP File Transport Protocol

GUI Graphical User Interface

HTTP Hyper Text Transport Protocol

IETF Internet Engineering Task Force

Integrity Assuring information will not be accidentally or maliciously altered or destroyed

MIME Multipurpose Internet Mail Extensions, a standard allowing advanced character set and attachment support for email.

RosettaNet Consortium for establishing standard B2B processes.

SAP Systeme, Anwendungen und Produkte in der Datenverarbeitung, or Systems, Applications, and Products in Data Processing. The world’s largest business application and Enterprise Resource Planning vendor.

Service A single step or activity of a workflow or GIS process that accomplishes a specific purpose such as performing data manipulations or execution of a B2B protocol.

SMTP Simple Mail Transfer Protocol

SOAP Simple Object Access Protocol

SVGA Super VGA: a set of graphics standards designed to offer greater resolution than VGA. The SVGA standards are developed by a consortium of monitor and graphics manufacturers called VESA

Threat The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security

Trading partner An individual or representative of a B2B partner who has a trading partner profile on the TOE.

Trading partner data Files, messages, documents, etc. which is sent to the TOE by a trading partner or sent by the TOE to a trading partner.

UCCnet A non-profit subsidiary of the Uniform Code Council, UCCnet is a standards organization that provides an Internet-based supply chain management (SCM) data registry service for e-commerce companies and companies that have an e-commerce component.

VGA Video Graphics Array: a graphics display system for PCs that has become one of the de facto standards for PCs. In text mode, VGA systems provide a resolution of 720 by 400 pixels. In graphics mode, the resolution is either 640 by 480 (with 16 colors) or 320 by 200 (with 256 colors). The total palette of colors is 262,144

Vulnerability Hardware, firmware, or software flow that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing

XML eXtensible Markup Language

2 TOE Description

The Gentran Integration Suite version 4.2 is a business to business communication tool and does not fall directly into any of the categories listed on the Common Criteria Portal.

2.1 TOE Overview

The Gentran Integration Suite (GIS) allows organizations to facilitate business to business (B2B) communication across a wide range of protocols. GIS allows a business to communicate with all its business partners despite the fact that partners may use different communications protocols and heterogeneous document formats. GIS also includes a mailbox service for trading partners that provides store-and-forward capabilities. GIS ensures that this communication is secure by providing robust, independently validated implementations of security protocols and by protecting access to the received information.

The GIS Target of Evaluation (TOE) is a software-only product, which includes the GIS application, a MySQL database, and a Federal Information Processing Standard, (FIPS) 140-2 certified cryptographic module. The TOE is supported by an environment that includes a hardware platform, an operating system, and Java Virtual Machine (JVM), as well as a remote management capability. While the GIS product can be installed on many different operating systems as described in the product overview, section 1.2, the evaluation is performed using the SUN Solaris 10 / SPARC 32 bit hardware/OS platform. Any remote management console(s), and any internal business applications must be installed in a trusted, protected network that contains the GIS server. In addition, the database used for the evaluation is the MySQL database bundled with the GIS product, which is installed on the same platform as the GIS application, JVM, and the cryptographic module.

An example of GIS in its operating environment is shown in Figure 2-1 below. The TOE resides on a host machine that provides the required environment for the TOE to operate: Hardware platform, Operating System, and a Java Virtual Machine (JVM). B2B systems which are installed at trading partner sites connect to the GIS product over an open network to exchange messages and documents. The TOE, its platform, a remote management console and internal business application systems reside in a trusted, private network.

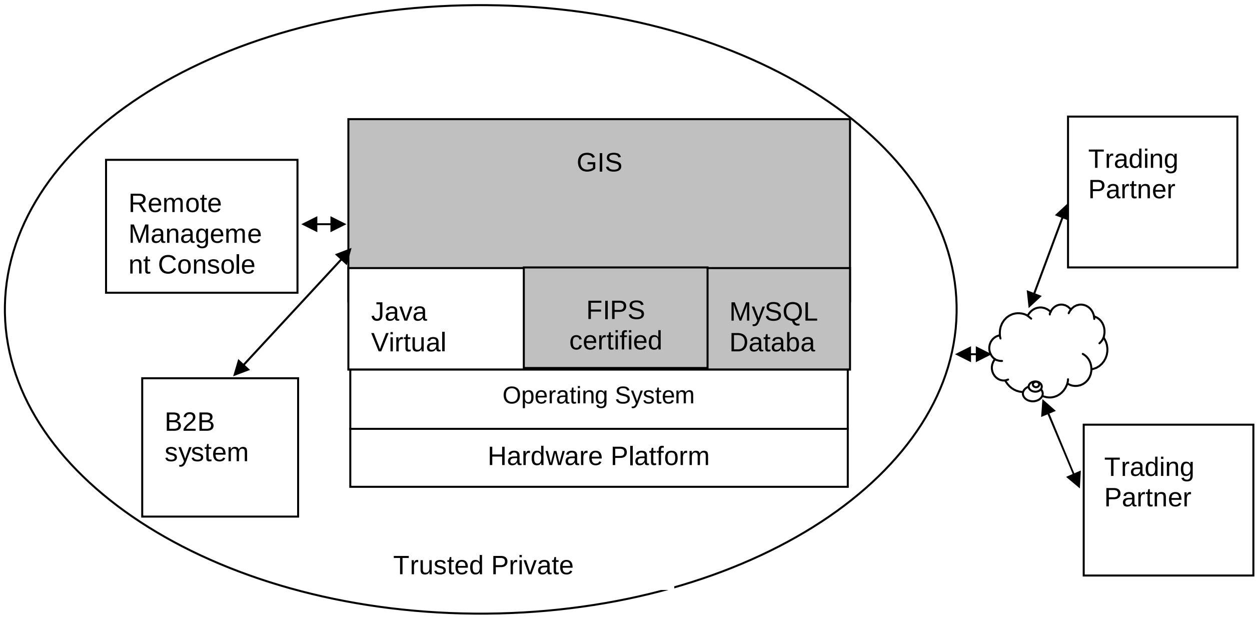

Figure 2-1: The TOE in its Operating Environment

2.2 TOE Components and Subcomponents

The TOE has three major components which are shown as grey boxes in Figure 2-1. They are

- Sterling Commerce's GIS version 4.2 software, referred to as GIS in this document
- MYSQL v 4.0.18, referred to as MYSQL in this document.
- The Certicom Security Builder® FIPS Java Module v 2.0, referred to as SB FIPS Java Module or simply SB FIPS in this document.

2.2.1 GIS

At the core of the GIS product is the Integration Broker component which determines authorization, destination, and services needed for each information exchange. The GIS product includes multiple adapters to enable information exchanges with the Integration Broker. Adapters provide an interface for sending information using GIS-supported communication protocols. The data translation and manipulation services provided by the Integration broker are complex and as such GIS also includes a tool to aid an administrator in defining these services: the Graphical Process Modeler. The following sections describe the GIS software in more detail, including discussion of the following modules of the GIS software component of the TOE.

- Graphic User Interface and Command Line Interface
- Adapters
- Integration Broker
- Graphical Process Modeler.

2.2.1.1 Graphic User Interface and Command Line Interface

GIS provides a web based graphic user interface that is accessible by remote management consoles that are within the trusted network containing the TOE. GIS users who have accounts on the GIS can log into the graphic user interface to manage the TOE user community, audit data, adapters, and other configuration options.

2.2.1.2 Adapters

GIS performs automated services in a business process. Typically the first or last service that is provided will handle the communication with a B2B system. The input and output services are collectively called *adapters*.

Adapters interact with B2B systems such as applications, middleware or business partners via the Internet. Support for major business applications such as SAP, Oracle or PeopleSoft, or for major B2B protocols such as EDI, UCCnet or RosettaNet, include both adapter components and pre-built business process models in the GIS. GIS supports over 200 adapters. However, the ones selected for the TOE are as follows:

- Sterling Commerce's Connect:Direct Server Adapter
- File Transfer Protocol (FTP) Server Adapter
- Hypertext Transport Protocol (HTTP) Server Adapter
- Electronic Data Exchange for the Internet (EDIINT) Message Service
- EDIINT Pipeline Service

Each of these adapters will be explained in more detail in the sections below.

2.2.1.2.1 Connect:Direct Server Adapter

The Gentran Integration Suite Connect:Direct Server adapter implements the functions of the Sterling Commerce proprietary Connect:Direct communications protocol. The Connect:Direct Server is an application that enables secure peer-to-peer file transfer over an insecure network. Connect:Direct installations perform periodic, high-capacity file transfers between specific servers, often for financial services or federal government applications. The adapter appears as a Connect:Direct node within a Connect:Direct network. An external Connect:Direct node can make requests to this adapter and the adapter can make Connect:Direct server level requests to external Connect:Direct nodes. Functions between Connect:Direct nodes include copying files, submitting other processes, running jobs, or running tasks.

The Gentran Integration Suite Connect:Direct Server adapter is compatible with the following versions of Connect:Direct:

- Connect:Direct Windows 4.1 (with patch 26) or later
- Connect:Direct UNIX 3.6 or later
- Connect:Direct OS/390 4.4 or later
- Connect:Direct OS/400 3.5 or later
- Connect:Direct Select
- Connect:Direct HP Non-Stop

2.2.1.2.2 File Transport Protocol (FTP) Server Adapter

The FTP Server adapter receives and processes requests from trading partners that are submitted using the FTP protocol. This adapter is used with a Gentran Integration Suite Perimeter server. A trading partner uses this adapter to put files in to a Gentran Integration Suite mailbox or get files from a Gentran Integration Suite mailbox.

2.2.1.2.3 Hypertext Transport Protocol (HTTP) Server Adapter

The HTTP Server adapter in Gentran Integration Suite processes HTTP requests from trading partners outside the trusted network. The HTTP Server adapter provides two capabilities:

- Triggering of a Gentran Integration Suite business process via an HTTP request
- Host a web application through the HTTP server adapter to support these trading partners.

2.2.1.2.4 The EDIINT Message Service and the EDIINT Pipeline Service

Electronic Data Interchange-Internet Integration (EDIINT) is a protocol developed by the Internet Engineering Task Force (IETF) for securely transporting messages containing business data over the Internet, using MIME packaging types.
There are two types of EDIINT:

- Applicability Standard 1 (AS1), which uses Simple Mail Transfer Protocol (SMTP) as a transport
- Applicability Standard 2 (AS2), which uses HTTP as a transport.

EDIINT is used in conjunction with other the other adapters mentioned above, which perform the session security tasks. EDIINT provides message authentication and message security. Within a business process in Gentran Integration Suite, the EDIINT Message service builds and parses EDIINT AS1 and AS2 messages, including data that is plain text, signed, compressed, encrypted, or a combination of these forms. Communications services then send or receive the messages within the business process. The EDIINT Pipeline Service adapter functions in a similar manner to the Messaging service, but is designed to process messages in a series.

2.2.1.3 The Integration Broker

Based on the incoming protocol and the trading partner profile, the Integration Broker selects the appropriate business process model to run when data enters the system through an input adapter. Adapters are configured to either put data in mailboxes or launch business processes with received messages. The business processes are then executed and managed by the integration broker, which is a workflow engine. When data is placed in a mailbox, business process that is a routing rule can be triggered for the data.

The trading partner profile is a record which describes the parameters of a contract made with a trading partner. The profile contains identity information about the trading partner, to include a unique identifier, name, address, telephone, and other related information. It also contains information about protocols available to the trading partner, including the protocol type and unique identifier for the profile. A trading partner profile may contain other information such as destination information like IP addresses, URLs, port numbers, and the like. For the FTP, HTTP, and Connect:Direct Server adapters, a user name and password are also supplied. The profile also describes the business processes a trading partner is allowed to use. The message or data (payload) may provide other specific instructions as to what should be done with the data

When an input adapter receives data from a B2B system, the Integration Broker locates the appropriate business process or processes to call, and starts the process or delivers the incoming data to the appropriate already-running process. The following example explains how the Integration Broker executes the steps in a business process as a document progresses through Gentran Integration Suite:

- Gentran Integration Suite receives the business message or document through an adapter.
- The Integration Broker determines which service to start next and starts the service, according to the content of the document.
- The adapter places the message or document and other appropriate process state information on a queue for the appropriate service in the selected business process.
- The appropriate service retrieves the initial business process state information from the queue and processes the next step in the business process.

- Each service in the business process updates the business process state information, and records a copy of the related data or pointers to the data for process recoverability.
- An adapter sends the modified business process state information, with the data, to a specific application.

After the adapter has performed the input or before the adapter provides the output of the information the TOE will perform services on the information. Each service is implemented in software and the services can be performed on documents in any specified order. Each service in the business process must complete for the business process to run successfully. Examples of services include:

- Communicating with external applications or middleware
- Performing data manipulations, such as translation, transformation, splitting and joining
- Routing data based on payload
- Publishing data to interested subscribers
- Execution of one or more B2B protocols
- Spawning a pre-defined business process (nested process)
- Performing operations on MySQL database tables

2.2.1.4 Graphical Process Modeler

Business process models define how the Gentran Integration Suite Integration Broker executes the activities in a business process. Creating business process models for the system to follow is the central activity around which operations hinge. The Graphical Process Modeler (GPM) is a Gentran Integration Suite tool that enables creation of business process models using drag-and-drop technology. The GPM depicts the services included in business process models using icons.

2.2.2 MYSQL

MYSQL is an open source database that is bundled with the GIS software. It is also installed on the same platform as the GIS application. While the GIS supports other database management systems, the TOE evaluation is based on the MySQL database only.

2.2.3 SB FIPS Java Module

SB FIPS Java Module is a cryptographic toolkit for Java language users, providing services of various cryptographic algorithms such as hash algorithms, encryption schemes, message authentication, and public key cryptography. It has completed FIPS 140-2 certification at level 1, certificate #578. It is installed on the hardware/software platform used for the GIS application, and is loaded by JVM and used by the GIS application at run-time. For further information about this component of the TOE, please refer to Security Builder® FIPS Java Module Version 2.0 FIPS 140-2 Non-Proprietary Security Policy, Certicom Corp. September 27, 2005.

2.3 Users of the TOE

There are two types of consumers of TOE services: GIS users and trading partners. They are collectively referred to as *users* in this document.

<u>GIS users</u> are administrative individuals who have accounts on the GIS, and access the TOE via the Graphic User Interface (GUI). The GIS users fall into two categories, the GIS administrator and non-root users. The GIS administrator is a root user who is a member of the *admin* group. GIS administrators have all privileges to all GIS data and functions, and have the ability to add other GIS users to the admin group or assign permissions to non-root users for specific tasks. The activities of the GIS users are governed by the GIS Access Control Policy, described below.

Trading partners access the TOE via one of the supported adapters. Trading partners are representatives of B2B partners who may be physically located within the trusted network or may be external to the trusted network. The trading partners who use the FTP Server, HTTP Server, or Connect:Direct Server adapters have user accounts for logging into the adapter. The trading partner activities are limited by the trading partner profile, which describes what business processes the trading partner may use. The trading partner does not have direct access to GIS data, the GUI, or other GUI user processes, and is limited to the activities allowed by the adapter, the trading partner profile, and the Adapter Policy, described below. Processes acting on behalf of trading partners may also be subject to the GIS Access Control Policy if a business process requires use of resources that have associated permissions.

Trading partners who are within the trusted network, and who have user accounts, can access the GIS via the GUI. In this case, the trading partner is viewed as a GIS user, and the access is controlled by the user account role, the Permissions are assigned to the user account, and are governed by the GIS Access Control Policy.

2.4 Hardware and Software for the TOE and its Environment

2.4.1 GIS Software, OS and Hardware Requirements

The application software that must be installed on a single platform to comprise the TOE is as follows:

- GIS 4.2
- MYSQL 4.0.18
- Certicom SB FIPS v2.0

The components that must be installed on the same platform to create the TOE Environment include:

- Sun Microsystems Java Runtime Environment (JRE) 1.4.2 for GIS platforms using a Solaris Operating Systems.
- The GIS TOE is to be tested on the SUN Solaris 10 / SPARC 32 bit hardware/OS platform, and must meet the following System Requirements.
- 2 GB RAM or greater
- 2 GB free disk space or greater
- File descriptor size of 1024 or greater (preferred setting is unlimited)
- File system space requirements will vary depending on the size of documents to be stored and the length of time chosen to keep documents on the file system.

2.4.2 Remote Management Workstation Hardware and Software

The Remote Management workstation is used within the trusted network for administration of the GIS. The hardware and software requirements the workstation must meet are the following minimum requirements:

- CD-ROM drive
- Pentium® or equivalent processor

- 400 MHz processor speed
- Color VGA or SVGA monitor
- Microsoft Internet Explorer 5.x or later
- 256 MB RAM
- 1 GB free disk space
- Adobe Acrobat Reader 6.0 or later

2.5 Scope of the TOE

The following table describes the specific physical entities of the TOE and its environment.

2.5.1 TOE Physical Scope and Boundary

Component	**TOE or Environment**
Certicom SB FIPS Module v. 2.0	TOE
GIS 4.2 Software	TOE
MYSQL 4.0.18	TOE
Sun Microsystems Java Runtime Environment (JRE) V 1.4.2 for Windows, Solaris, and Linux.	TOE Environment
GIS Operating system and Hardware platform	TOE Environment
Remote management Console software, Operating system, and hardware	TOE Environment
trading partner servers	TOE Environment

Table 2-1: Physical Boundary of TOE and TOE Environment

2.5.2 TOE Logical Scope and Boundary

The TOE includes the following security functions.

2.5.3 Audit

GIS provides an audit function that collects information about security-relevant events that occur within the TOE. The audited events include starting or stopping an adapter; creation, deletion, and modification of GIS user accounts; changes to groups, permissions, mailboxes, services or adapter configurations; file transfer and configuration and command information that is transmitted; successful or unsuccessful attempts to access GIS objects and resources; successful or unsuccessful login attempt, SSL client session authentication and authentication using a certificate in a partner profile. For each such event, an *audit record* is created and stored in an *audit trail* of security relevant events.

Each audit log contains a timestamp, a description, an outcome and, as appropriate, the relevant subject, are recorded. A standardized log format is used. The GUI provides a reporting functionality for audit records, allowing authorized users to view and search the audit trail.

2.5.4 Communication

Two adapters, the EDIINT Message Service and the EDIINT Pipeline Service, provide non-repudiation of origin and non-repudiation of receipt. Non-repudiation of origin is accomplished using digital signatures to identify the message creator. Non-repudiation of receipt is accomplished by sending a digitally signed acknowledgement message to the sender when receipt has been accomplished.

2.5.5 Access Control and Information Flow Control

GIS provides access control to GIS resources and information flow control for the activities of trading partners via adapters.

- The access control policy, the GIS Access Control SFP, applies to administrators of the TOE and to Trading partners who use the TOE. It controls access to GIS resources such as mailboxes and configuration files.
- The Adapter SFP, a Security Function Policy that addresses the behavior and access of trading partners using an adapter to send, process, and forward documents and messages as dictated by the Trading Partner Profile and the capabilities of the adapter.

2.5.6 Identification and Authentication

Individuals connecting to the TOE via the GUI and trading partners connecting to the TOE via FTP Server adapter, HTTP Server adapter, and Connect:Direct Server adapter are required to login to the TOE before being allowed to take any actions on the TOE. Trading partners using any of the adapters are also identified by trading partner profiles and authenticated by the adapters via certificate.

2.5.7 Security Management

GIS provides protection of TOE Security functions such as functions for creating and managing trading partner profiles, defining and assigning privileges, creation of GIS user accounts, and the definition of roles. Other management services protect TSF data, which includes identification and authentication data, audit records, and security policy attributes.

2.5.8 Protection of Trading Partner Data in Transit

The TOE provides protection to trading partner data in transit from disclosure and modification by establishing encrypted communication sessions in which trading partner data can be sent or received. The protocols used by the GIS adapters require authentication of the trading partner prior to allowing any communication to take place. The verification of identity at both endpoints of the communication, together with the encryption of the data in transit also provides a trusted path for trading partner data transmissions. Cryptographic services, including encryption, decryption, and digital signatures, are provided by the FIPS 140-2 certified Certicom SB FIPS module.

2.5.9 Protection of TOE Security Functions

The TOE environment provides a secure domain for the TOE's execution, while the TOE ensures that security features of the TOE cannot be bypassed. This is accomplished by a combination of the identification and authentication services which are met by the TOE, and the access control and information flow control policies that govern what resources can be accessed by which GIS users and trading partners, respectively.

2.6 TOE Exclusions

The following item is forbidden in the evaluated configuration by administrator guidance and is excluded from the evaluation:

- The GIS SDK functions and interfaces.

3 TOE Security Environment

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects
- known and presumed threats countered by either the TOE or by the security environment
- organizational security policies with which the TOE must comply

The following table lists the assumptions, threats, and organizational security policies. They are described in detail in the sections below.

Assumptions
A.ADMIN
A.DB
A.GENPUR
A.NOEVIL
A.PHYSICAL
A.PRINET
A.SINGEN
Threats
T.AUDGEN
T.AUDREV
T.B2BCOM
T.DENY
T.MEDIATE
T.NOAUTH
T.SLFPRO
Organizational Security Policies
NONE

Table 3-1: TOE Assumptions, Treats, and Organizational Security policies

3.1 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

A.ADMIN	Administrators of the underlying Operating System are also GIS Administrators.
A.DB	The GIS and the GIS Database are installed on the same physical server and the GIS database is not used for any purpose except that of the GIS.
A.GENPUR	There are no general purpose computing capabilities on the TOE platform (e.g., the ability to execute arbitrary code or applications).
A.NOEVIL	Administrators of the TOE are non-hostile, appropriately trained, and follow all user and administrator guidance.
A.PHYSICAL	The TOE is located within a physical area that protects the TOE from unauthorized physical access.
A.PRINET	The TOE and the remote management console(s) are on a private network that is protected by a Firewall
A.SINGEN	Information cannot flow among the internal and external B2B trading partners unless it passes through the TOE.

3.2 Threats

The following are threats identified for the TOE. The assumed level of expertise of the attacker for all the threats is *unsophisticated*. The threat agents are users authorized to use the TOE as well as unauthorized users (persons or external IT entities) not authorized to use the TOE.

T.AUDGEN	An unauthorized user may perform unauthorized actions that go undetected because of the failure of the system to record actions.
T.AUDREV	Users may not be accountable for the actions they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.B2BCOM	An unauthorized user may be able to view, modify, and/or delete information that is sent between a remotely located trading partner and the TOE.
T.DENY	A user of adapters that do not require login will be able to deny origin or receipt of data.
T.MEDIATE	A user may access files, data, or functions for which he is not authorized because of inadequate access control measures.

T.NOAUTH	An unauthorized user may gain access to system data due to failure of the system to enforce identification and authentication on users.
T.SLFPRO	An unauthorized user may bypass, deactivate, or tamper with TOE security functions.

3.3 Organizational Security Policies

There are no organizational security policies defined for the TOE.

4 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

Objectives
O.ACCTL
O.AUDGEN
O.AUDREV
O.I&A
O.NONREPDN
O.PRODAT
O.ROLES
O.SECFUN
O.SLFPRO
Security Objectives for the IT Environment
OE.TIMSTMP
Security Objectives for the Non-IT Environment
OE.ADMIN
OE.DB
OE.GENPUR
OE.NOEVIL
OE.PHYSICAL
OE.PRINET
OE.SINGEN

Table 4-1 :Objectives for the TOE and the TOE Environment

4.1 Security Objectives for the TOE

O. ACCTL	The TOE must provide the means of controlling and limiting access by GIS users to GIS objects
O.AUDGEN	The TOE must provide the means of recording any security relevant events that contain security relevant information including the time of the event to hold users accountable for any security relevant actions they perform.
O.AUDREV	The TOE must provide a means of viewing audit data.
O.I&A	The TOE must uniquely identify all users of the GIS UI, and will authenticate the claimed identity before granting a user any access
O.NONREPDN	The TOE must provide non-repudiation of origin or receipt for all transmissions processed by adapters not requiring login and password verification. This includes the EDIINT Message Service and the EDIINT Pipeline Service .

O.PASSTHRU	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, from users on a connected network to users on another connected network.
O.PRODAT	The TOE must protect the confidentiality and integrity of User data in transit.
O.ROLES	The TOE shall provide roles for all users of the TOE.
O.SECFUN	The TOE shall provide functionality that enables an authorized administrator to use the TOE security functions and must ensure that only authorized administrators are able to access such functionality.
O.SLFPRO	The TOE must protect itself against attempts by authorized users, unauthorized users, or trading partners to bypass, deactivate, or tamper with TOE security functions.

4.2 Security Objectives for the Environment

The following objectives address non-IT issues that are satisfied by procedural or administrative means, as well as IT objectives addressed by the TOE Environment.

4.2.1 Security Objectives for the IT Environment

OE.TIMSTMP	The IT Environment must provide a mechanism capable of providing reliable source for time.

4.2.2 Security Objectives for the Non-IT Environment

OE.ADMIN	Administrators of the underlying Operating System are also GIS Administrators.
OE.DB	The GIS and the GIS Database are installed on the same physical server and the GIS database is not used for any purpose except that of the GIS.
OE.GENPUR	There are no general purpose computing capabilities on the TOE platform (e.g., the ability to execute arbitrary code or applications).
OE.NOEVIL	Administrators of the TOE are non-hostile, appropriately trained, and follow all user and administrator guidance.
OE.PHYSICAL	The TOE is located within a physical area that protects the TOE from unauthorized physical access.
OE.PRINET	The TOE and the remote management console(s) are on a private network that is protected by a Firewall
OE.SINGEN	Information cannot flow among the internal and external B2B trading partners unless it passes through the TOE.

4.3 Security Objectives Rationale

4.3.1 Tracing for Threats

Table 4-2 demonstrates that all security objectives for the TOE and its supporting environment trace to aspects of the identified threats to be countered and/or aspects of the organizational security policies to be met by the TOE.

	T.AUDGEN	T.AUDREV	T.B2BCOM	T.DENY	T.MEDIATE	T.NOAUTH	T.SLFPRO
O. ACCTL					X		
O.AUDGEN	X						
O.AUDREV		X					
O.I&A						X	
O.NONREPDN				X			
O.PASSTHRU					X		
O.PRODAT			X				
O.ROLES					X		
O.SLFPRO							X
O.SECFUN						X	
OE.TIMSTMP	X						

Table 4-2: TOE Threats Tracing

4.3.2 Security Objectives Rationale: Threats to the TOE

T.AUDGEN An unauthorized user may perform unauthorized actions that go undetected because of the failure of the system to record actions.

The objective O.AUDGEN counters this threat by providing an audit mechanism that collects audit data about security relevant events. The objective for the IT Environment, OE.TIMSTMP, ensures that reliable time stamps are provided for the audit records generated.

T.AUDREV Users may not be accountable for the actions they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.

The Objective O.AUDREV counters this threat by providing a facility to review the audit records to authorized administrators.

T.B2BCOM An unauthorized user may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.

This threat is met by objective O.PRODAT which protects the confidentiality and integrity of user data in transit

T.DENY A user of adapters that do not require login will be able to deny origin or receipt of data.

This threat is countered by O.NONREPDN, which provides non-repudiation of origin or receipt for the communications of trading partners who use the EDIINT Message Service and EDIINT Pipeline Service.

T.MEDIATE A user may access files, data, or functions for which he is not authorized because of inadequate access control measures.

This threat is countered by O.ACCTL, O.PASSTHRU, and O.ROLES. O.ACCTL describes the access controls on TOE objects and O.PASSTHRU describes information flow rules for trading partner data via the adapters. O.ROLES supports the objective O.ACCTL by providing roles which distinguish administrative users from non administrative users.

T.NOAUTH An unauthorized user may gain access to system data due to failure of the system to enforce identification and authentication on users.

This threat is met by O.I&A and O.SECFUN. Identification and authentication for the ESX server is addressed by O.I&A, and identification and authentication to the VirtualCenter is addressed by O.I&A. There are no other ways a user may access the ESX Server or the VirtualCenter. O.SECFUN guarantees that there are adequate security functions to manage the I&A functionality.

T.SLFPRO An unauthorized user may bypass, deactivate, or tamper with TOE security functions.

This threat is met by objectives O.SLFPRO which ensures that users may not bypass, deactivate, or tamper with the TOE security functions.

4.3.3 Security Objectives Rationale: Organizational Security Policies

This ST has no Organizational Policies.

4.3.4 Security Objectives Rationale: Assumptions

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

The following security objectives for the environment are a re-statement of the security assumptions, so those security objectives trace to all aspects of the assumptions.

A.ADMIN and OE.ADMIN

A.DB and OE.DB

A.GENPUR and OE.GENPUR

A.NOEVIL and OE.NOEVIL

A.PHYSICAL and OE.PHYSICAL

A.PRINET and OE.PRINET

A.SINGEN and OE.SINGEN

5 IT Security Requirements

This section provides Security Functional Requirements on the TOE and on the TOE environment, rationales for Security Functional Requirements, Security Assurance Requirements, and the rationale for the Security Assurance requirements in this Security Target (ST).

5.1 Security Functional Requirements

The Security Functional Requirements consist of functional security requirements for this Security Target and includes the following components from Part 2 of the CC.

Security functions on the TOE	
Functional Component	**Summary Description**
FAU_GEN.1	Audit Data Generation
FAU_SAR.1	Audit Review
FCO_NRO.1	Selective Proof of Origin
FCO_NRR.1	Selective Proof of Receipt
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1	Cryptographic Operation
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Simple Security Attributes
FDP_UCT.1	Data Exchange Confidentiality
FDP_UIT.1	Data Exchange Integrity
FIA_UAU.2	User Authentication Before Any Action
FIA_UID.2	User Identification Before Any Action
FMT_MOF.1	Management of Security Functions Behavior
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_MTD.1	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_RVM.1	Non-Bypassability of the TSP

Security functions on the TOE	
Functional Component	**Summary Description**
FTP_TRP.1	Trusted Path
Security functions on the TOE Environment	
Functional Component	**Summary Description**
FPT_SEP.1	TSF Domain Separation
FPT_STM.1	Reliable Time Stamps

5.2 Security Functional Requirements on the TOE

5.2.1 Class FAU: Security Audit

5.2.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1

The TSF shall be able to generate an audit 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 events defined in Table 5-1 below**].

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, 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 other audit relevant information**].

Audit Event:
starting or stopping an adapter
Creation, deletion, and modification of GIS user accounts
Changes to groups, permissions, mailboxes, services or adapter configurations.
file transfer, configuration and command information that is transmitted

successful or unsuccessful attempts to access GIS objects and resources
Successful or unsuccessful login attempt; SSL client session authentication; authentication using a certificate in a partner profile.

Table 5-1: Auditable Events

5.2.1.2 FAU_SAR.1 Audit review

FAU_SAR.1.1

The TSF shall provide [**GIS Administrators, Non-Root Users who have been assigned permissions to audit data**] with the capability to read [**audit information stored in the TOE Environment**] 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.

5.2.2 Class FCO: Communication

5.2.2.1 FCO_NRO.1 Selective proof of origin

FCO_NRO.1.1

The TSF shall be able to generate evidence of origin for transmitted [**messages from the EDIINT Messaging Service or the EDIINT Pipeline service**] at the request of the [**GIS Administrator or any Non-Root user who has permission to the adapter configuration file**].

FCO_NRO.1.2

The TSF shall be able to relate the [**identity**] of the originator of the information, and the [**message**] of the information to which the evidence applies.

FCO_NRO.1.3

The TSF shall provide a capability to verify the evidence of origin of information to [[**the GIS Administrator or any Non-Root User who has permission to the evidence**]] given [**the evidence is still available on the TOE].**

5.2.2.2 FCO_NRR.1 Selective proof of receipt

FCO_NRR.1.1

The TSF shall be able to generate evidence of receipt for received [**messages sent via the EDIINT Messaging Service or the EDIINT Pipeline service**] at the request of the [[**GIS Administrator or any Non-Root user who has permission to the adapter configuration file**]].

FCO_NRR.1.2

The TSF shall be able to relate the [**identity**] of the recipient of the information, and the [**message**] of the information to which the evidence applies.

FCO_NRR.1.3

The TSF shall provide a capability to verify the evidence of receipt of information to [[**the GIS Administrator or any Non-Root User who has permission to the evidence**]] given [**the evidence is still available on the TOE**].

5.2.3 Class FCS: Cryptographic Support

5.2.3.1 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 [**random number generation**] and specified cryptographic key sizes [**256 bit**] that meet the following: [**ANSI X9.62 RNG**].

5.2.3.2 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**].

5.2.3.3 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 [a]

The TSF shall perform [**the operations listed in column 1 of Table 5-2: Cryptographic operations**] in accordance with a specified cryptographic algorithm [**the algorithms in column 2 of Table 5-2: Cryptographic operations**] and cryptographic key sizes [**the key sizes in column 3** of **Table 5-2: Cryptographic operations**] that meet the following: [**list of standards and certificates in column 4 of Table 5-2: Cryptographic operations**].

Cryptographic operation	Cryptographic Algorithm	Cryptographic key sizes	Standards and Certificate number
symmetric block cipher encryption and decryption	DES (transitional phase only, valid until May 19, 2007) (ECB, CBC, CFB64, OFB64)	64	FIPS 46-3 # 298
	TDES (ECB, CBC, CFB64, OFB64)	192	FIPS 46-3 # 318
	AES (ECB, CBC, CFB128, OFB128)	128, 192, 256	FIPS 197 #227
hashing	SHA-1 [FIPS 180-2]	N/A	FIPS 180-2 #307
	SHA-224 [FIPS 180-2]	N/A	FIPS 180-2 #307

	SHA-256 [FIPS 180-2]	N/A	FIPS 180-2 #307
	SHA-384 [FIPS 180-2]	N/A	FIPS 180-2 #307
	SHA-512 [FIPS 180-2]	N/A	FIPS 180-2 #307
message authentication	HMAC-SHA-1 [FIPS 198]	80	FIPS 198 #37
	HMAC-SHA-224 [FIPS 198]	112	FIPS 198 #37
	HMAC-SHA-256 [FIPS 198]	128	FIPS 198 #37
	HMAC-SHA-384 [FIPS 198]	192	FIPS 198 #37
	HMAC-SHA-512 [FIPS 198]	256	FIPS 198 #37
key agreement	DH [ANSI X9.42]	512-15360	ANSI x9.42
	ECDH [ANSI X9.63]	Same as DH	ANSI X9.63
	ECMQV [ANSI X9.63]	512	ANSI X9.63
digital signatures	DSA [FIPS 186-2]	512, 576, 640, 704, 768, 832, 896, 960, 1024	FIPS 186-1, #128
	ECDSA [FIPS 186-2, ANSI X9.62]	[ALL-P], [ALL-K], [ALL-B]	ANSI C9.63, #6
	RSA PKCS1-v1.5 [PKCS #1 v2.1]	1024-15360	PKCS #1 v2.1 #54
key wrapping	RSA PKCS1-v1.5 [PKCS #1 v2.1]	Uses RSA PKCS1 v1.5 and SHA hashing	PKCS #1 v2.1
	RSA OAEP [PKCS #1 v2.1]	Uses RSA PKCS1 v1.5 and SHA hashing	PKCS #1 v2.1
random number generation	ANSI X9.62 RNG [ANSI X9.62]	Uses ECDSA	ANSI X9.62 #68

Table 5-2: Cryptographic operations

5.2.4 Class FDP: User Data Protection

5.2.4.1 FDP_ACC.1 Subset

FDP_ACC.1.1

The TSF shall enforce the [**GIS Access Control SFP**] on
[
Subjects: processes acting on behalf of GIS users or trading partners.

Objects: GUI menu items, Business Processes, mailboxes, messages, keys, certificates, security relevant property files, services, product features.

Operations: All interactions between the subjects and objects identified above]

5.2.4.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1

The TSF shall enforce the [**GIS Access Control SFP**] to objects based on the following:

[Subjects: processes acting on behalf of GIS users or trading partners.

Objects: GUI menu items, Business Processes, mailboxes, messages, keys, certificates, security relevant property files, services, product features.

Subject attributes: Processes acting on behalf of GIS Users: User role, userID, user's groups, users permissions, permissions of groups to which the user belongs. Processes acting on behalf of trading partners: permissions.

Object attributes: **Permissions assigned to objects, or the absence of permissions assigned to objects.]**

FDP_ACF.1.2

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

1 **If the subject is the GIS Administrator, then access is granted.**

2 **If a subject requests access to an object which has no assigned permissions, then access is granted.**

3 **If a subject who is not a GIS Administrator requests access to an object which has assigned permissions, the permissions of the subject are examined to determine if the subject has permission to the object. If a match is found, access is granted.**

4 **If a subject who is not a GIS Administrator requests access to an object with assigned permissions and the subject does not have permission to the object, then the permissions of the groups to which the subject belongs are examined to determine if a group of the subject has permission to the object. If a match is found, access is granted.**

5 **If none of the above rules apply, access is denied.**]

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**None**].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [**none**].

5.2.4.3 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1

The TSF shall enforce the [**Adapter SFP**] on

[**Subjects: trading partners having a valid GIS Trading Partner Profile**

Information: trading partner data

Operations: process transmitted information, pass information].

5.2.4.4 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1

The TSF shall enforce the [**Adapter SFP**] based on the following types of subject and information security attributes:

[**Subject attributes: Trading partner profile including identity, communication protocols, business processes to be used**

Object Attributes: Requested business processes, information destination

FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[**1. Files and messages received by the GIS on behalf of a trading partner will be processed according to the requested business process if the following are true:**

- **If the adapter requires login and password verification, it is successful**
- **For inbound traffic, the trading partner profile must grant the trading partner the ability to perform the business processes requested in the transmitted data.**
- **For inbound traffic via the FTP Server, HTTP Server and Connect:Direct Server adapters, the GIS Access Control SFP grants the logged in user access to all objects that are required for the transaction.**

2. Trading partner data will be delivered to the requested destination if the following are true:

- **Any business processes performed on the data complete successfully.**
- **For data to be stored on GIS, the trading partner profile must allow the trading partner to use the requested mailboxes.**
- **Data transmitted by a GIS adapter on behalf of a trading partner must use the protocols and business processes specified by the trading partner profile, using the encryption packages configured for the adapter.]**

FDP_IFF.1.3

The TSF shall enforce the [**none**].

FDP_IFF.1.4

The TSF shall provide the following [**none**].

FDP_IFF.1.5

The TSF shall explicitly authorise an information flow based on the following rules: [**none**].

FDP_IFF.1.6

The TSF shall explicitly deny an information flow based on the following rules: [**none**].

5.2.4.5 FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1

The TSF shall enforce the [**Adapter SFP**] to be able to [transmit] objects in a manner protected from unauthorised disclosure.

5.2.4.6 FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1

The TSF shall enforce the [**Adapter SFP**] to be able to [receive, transmit] [*trading partner*] data in a manner protected from [modification] errors.

FDP_UIT.1.2

The TSF shall be able to determine on receipt of [*trading partner*] data, whether [modification] has occurred.

5.2.5 Class FIA: Identification and Authentication

5.2.5.1 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1

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

5.2.5.2 FIA_UID.2 User identification before any action

FIA_UID.2.1

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.2.6 Class FMT: Security Management

5.2.6.1 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1

The TSF shall restrict the ability to [<u>determine the behaviour of, disable, enable, modify the behaviour of</u>] the functions [**Functions described in column one of Table 2-1 below**] to [**roles identified in column two of Table 2-1 below**].

Security Management Function	**Roles**
Add, delete, modify user account	**GIS Administrator and any Non-Root User who has permission to access the user account management menus of the GUI.**
Add, delete, modify user group membership	**GIS Administrator and any Non-Root User who has permission to access the user group management menus of the GUI.**
Create or delete a permission	**GIS Administrator and any Non-Root User who has permission to access the permission management menus of the GUI.**
Change own password	**GIS Administrator and Non-Root User**
Add, delete, modify trading profile	**GIS admin and any Non-Root User who has permission to access the trading partner menus of the GUI.**
Modify security relevant property files that are accessible from the GUI	**GIS admin and any Non-Root User who has permission to access the appropriate menus of the GUI.**

Table 5-3: TOE Security Management Functions and roles

5.2.6.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1

The TSF shall enforce the [**GIS Access Control SFP**] to restrict the ability to [change_default, query, modify, delete] the security attributes [**userID, user group membership, user permissions, object permissions, trading partner identities, trading partner profiles**] to [**GIS Administrators and Non-Root Users who have permission to the attribute to be accessed**].

5.2.6.3 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1

The TSF shall enforce the [**GIS Access Control SFP**] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [**GIS Administrator**] to specify alternative initial values to override the default values when an object or information is created.

5.2.6.4 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1

The TSF shall restrict the ability to [selection*:* query, modify, delete, [**create**]] the [**TSF data listed in column 1 of Table 5-4: TSF Data below**] to [**the authorised identified roles in column 3 of Table 5-4: TSF Data**].

TSF data	Operation	Roles
User account	**Create, delete, modify**	**GIS Administrator and any Non-Root User who has permission to access the user account management menus of the GUI.**
User group membership	**Create, delete, modify**	**GIS Administrator and any Non-Root User who has permission to access the user group management menus of the GUI.**
Permission	**Create or delete**	**GIS Administrator and any Non-Root User who has permission to access the permission management menus of the GUI.**
Authentication data: password	**Modify**	**GIS Administrator and Non-Root User**
Authentication data: password	**Create**	**GIS Administrator and Non-Root User who has permission to access the authentication menus of the GUI**
Authentication data: certificates	**Query, create**	**GIS Administrator**

Encryption Keys	**Generate, destroy**	**GIS admin and any Non-Root User who has permission to access the cryptographic module functions**[4]
Trading partner profile	**Create, delete, modify**	**GIS admin and any Non-Root User who has permission to access the trading partner menus of the GUI.**
Property files that are accessible from the GUI	**Modify**	**GIS admin and any Non-Root User who has permission to access the appropriate menus of the GUI.**
Audit logs	**Query, delete**	**GIS Administrator and any Non-Root User who has permission to access the audit files.**

Table 5-4: TSF Data

5.2.6.5 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [

Add, delete, modify user account
Add, delete, modify user group membership
Create or delete a permission
Change own password
Add, delete, modify trading profile
Modify property files

Table 5-5: Security Management Functions

].

5.2.6.6 FMT_SMR.1 Security roles

FMT_SMR.1.1

The TSF shall maintain the roles [**GIS Administrator, Non-Root User**].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

5.2.6.7 FPT_RVM.1 Non-bypassability of the TSP

[4] For a complete list of cryptographic key related operations, refer to Security Builder® FIPS Java Module Version 2.0 FIPS 140-2 Non-Proprietary Security Policy, Certicom Corp. September 27, 2005.

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.

5.2.7 Class FTP: Trusted Path/Channels

5.2.7.1 FTP_TRP.1 Trusted path

FTP_TRP.1.1

The TSF shall provide a communication path between itself and [remote] [*trading partners*] that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2

The TSF shall permit [remote [*trading partners*]] to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [[**sending and receiving data via a TOE adapter**]].

5.3 Security Functional Requirements on the IT Environment

5.3.1.1 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1

The *TOE Environment* shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2

The *TOE Environment* shall enforce separation between the security domains of subjects in the TSC.

5.3.1.2 FPT_STM.1 Reliable time stamps

FPT_STM.1.1

The *TOE Environment* shall be able to provide reliable time stamps for its own use.

5.4 Security Functional Requirements Rationale

5.4.1 Tracing SFR for the TOE and for the Environment to Objectives for the TOE

Table 5-6 : Tracing SFR for the TOE to Objectives for the TOE demonstrates that all security functional requirements for the TOE trace to the objectives for the TOE.

	O.ACCTL	O.AUDGEN	O.AUDREV	O.I&A	O.NONREPDN	O.PASSTHRU	O.PRODAT	O.ROLES	O.SECFUN	O.SELPRO	OE.TIMSTMP

	O.ACCTL	O.AUDGEN	O.AUDREV	O.I&A	O.NONREPDN	O.PASSTHRU	O.PRODAT	O.ROLES	O.SECFUN	O.SELPRO	OE.TIMSTMP
FAU_GEN.1		x									
FAU_SAR.1			x								
FCO_NRO.1					x						
FCO_NRR.1					x						
FCS_CKM.1							x				
FCS_CKM.4							x				
FCS_COP.1							x				
FDP_ACC.1	x										
FDP_ACF.1	x										
FDP_IFC.1						x					
FDP_IFF.1						x					
FDP_UCT.1							x				
FDP_UIT.1							x				
FIA_UAU.2				x							
FIA_UID.2				x							
FMT_MOF.1									x		
FMT_MSA.1	x					x					
FMT_MSA.3	x					x					
FMT_MTD.1									x		
FMT_SMF.1									x		
FMT_SMR.1	x							x			
FPT_RVM.1										x	
FPT_SEP.1 (on env)										x	
FPT_STM.1 (on env)		x									x
FTP_TRP.1						x					

Table 5-6 : Tracing SFR for the TOE to Objectives for the TOE and the TOE environment

5.4.2 Rationale for Security Requirements on the TOE

<table>
<tr><td>O. ACCTL</td><td>The TOE must provide the means of controlling and limiting access by logged in GIS users to GIS objects</td></tr>
<tr><td colspan="2">This objective is met by FMT_SMR.1, FDP_ACC.1 and FDP_ACF.1, which provide role-based access control mechanisms for all logged in users to GIS objects. It is supported by FMT_MSA.1 and FMT_MSA.3, which provide for management of security attributes and static attribute initialisation.</td></tr>
<tr><td>O.AUDGEN</td><td>The TOE must provide the means of recording any security relevant events that contain security relevant information including the time of the event to hold users accountable for any security relevant actions they perform.</td></tr>
<tr><td colspan="2">This objective is met by FAU_GEN.1, which provides for an auditing system that meets these requirements. It is supported from the environment by FPT_STM.1, which requires that the environment provide reliable time stamps to the TOE.</td></tr>
<tr><td>O.AUDREV</td><td>The TOE must provide a means of viewing audit data.</td></tr>
<tr><td colspan="2">This objective is met by FAU_SAR.1 which requires the ability to review the audit records.</td></tr>
<tr><td>O.I&A</td><td>The TOE must uniquely identify all users of the GIS UI, and will authenticate the claimed identity before granting a user any access</td></tr>
<tr><td colspan="2">This Objective is met by FIA_UID.2 and FIA_UAU.2, which require identification and authentication of all GIS UI users.</td></tr>
<tr><td>O.NONREPDN</td><td>The TOE must provide non-repudiation of origin or receipt for all transmissions processed by adapters not requiring login and password verification. This includes the EDIINT Message Service and the EDIINT Pipeline Service.</td></tr>
<tr><td colspan="2">This objective is met by FCO_NRO.1 and FCO_NRR.1, which require that the EDIINT Message Service and the EDIINT Pipeline Service to provide non-repudiation of origin or receipt</td></tr>
<tr><td>O.PASSTHRU</td><td>The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, from users on a connected network to users on another connected network.</td></tr>
<tr><td colspan="2">This objective is met by FDP_IFC.1 and FDP_IFF.1, which specify the rules under which incoming data is accepted and processed, and under which outgoing data is processed and transmitted. It is supported by FMT_MSA.1 and FMT_MSA.3, which provide for management of security attributes and static attribute initialisation. Last, this objective is supported by FTP_TRP.1, which ensures a secure path between the TSF and users.</td></tr>
<tr><td>O.PRODAT</td><td>The TOE must protect the confidentiality and integrity of User data in transit.</td></tr>
<tr><td colspan="2">This objective is met by FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FDP_UCT.1, FDP_UIT.1, FCS_CKM.1 and FCS_CKM.4 describe requirements for securely generating and destroying keys for the cryptographic operations, while FCS_COP.1 describes the operations that the cryptographic module of the TOE provides. FDP_UCT.1 and FDP_UIT.1 provide for protection of data in transit from unauthorized disclosure or modification, which is done using the encryption described by the three FCS family SFR.</td></tr>
<tr><td>O.ROLES</td><td>The TOE shall provide roles for all users of the TOE.</td></tr>
<tr><td colspan="2">This objective is met by FMT_SMR.1, which describes two roles for the TOE—a GIS Administrator and</td></tr>
</table>

all other users of the TOE, who are Non-Root Users.	
O.SECFUN	The TOE shall provide functionality that enables an authorized administrator to use the TOE security functions and must ensure that only authorized administrators are able to access such functionality.
This objective is met by FMT_MOF.1, FMT_MTD.1, and FMT_SMF.1. FMT_SMF.1 identifies the security management functions of the TOE. FMT_MOF.1 identifies what users can modify the behaviour of the TOE security functions, and FMT_MTD.1 descries TSF data and what users can access the TSF data.	
O.SLFPRO	The TOE must protect itself against attempts by authorized users, unauthorized users, or trading partners to bypass, deactivate, or tamper with TOE security functions.
This objective is met by FPT_RVM.1 and contributed to by FPT_SEP.1, on the environment. FPT_RVM.1 requiring that all TOE security policy functions are invoked and succeed before each function in the TOE may proceed. FPT_SEP.1 requires that the TOE environment protect the TOE from interference and tampering of untrusted subjects.	
OE.TIMSTMP	The IT Environment must provide a mechanism capable of providing reliable source for time.
This objective is met by FTP_STM.1, which requires that the TOE Environment provide reliable time stamps to the TOE.	

5.4.3 Rationale For Security Requirement Dependencies

The following table lists all the SFR dependencies with a note as to whether or not the dependency is satisfied.

Functional Component	**Summary Description**	**Dependencies**
FAU_GEN.1	Audit Data Generation	FPT_STM.1
FAU_SAR.1	Audit Review	FAU_GEN.1
FCO_NRO.1	Selective Proof of Origin	FIA_UID.1*
FCO_NRR.1	Selective Proof of Receipt	FIA_UID.1*
FCS_CKM.1	Cryptographic Key Generation	FCS_COP.1 FCS_CKM.4 FMT_MSA.2**
FCS_CKM.4	Cryptographic Key Destruction	FCS_COP.1 FCS_CKM.1 FMT_MSA.2**
FCS_COP.1	Cryptographic Operation	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2**
FDP_ACC.1	Subset Access Control	FDP_ACF.1
FDP_ACF.1	Access Control Functions	FDP_ACC.1

		FMT_MSA.3
FDP_IFC.1	Information Flow Control Policy	FDP_IFF.1
FDP_IFF.1	Information Flow Control Functions	FDP_IFC.1 FMT_MSA.3
FDP_UCT.1	Data Exchange Confidentiality	FDP_ACC.1 FDP_IFC.1 FTP_TRP.1
FDP_UIT.1	Data Exchange Integrity	FDP_ACC.1 FDP_IFC.1 FTP_TRP.1
FIA_UAU.2	User Authentication Before Any Action	FIA_UID.1*
FIA_UID.2	User Identification Before Any Action	none
FMT_MOF.1	Management of Security Functions Behavior	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1	Management of Security Attributes	FDP_ACC.1 FDP_IFC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	Static Attribute Initialisation	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1	Management of TSF Data	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	Specification of Management Functions	none
FMT_SMR.1	Security Roles	FIA_UID.1*
FPT_RVM.1	Non-Bypassability of the TSP	none
FPT_SEP.1 (on env)	TSF Domain Separation	none
FPT_STM.1 (on Env)	Reliable Time Stamps	none
FTP_TRP.1	Trusted Path	none

All dependencies are met except for those marked *, or **. The rationale for not meeting these dependencies is provided below.

* FIA_UID.2 is hierarchal to FIA_UID.1, and is used instead of FIA_UID.1.

** Rationale for not meeting the dependency on FMT_MSA.2: FCS_CKM.1, FCS_CKM.4, and FCS_COP.1 depend on FMT_MSA.2 Secure Security Attributes. Once the TOE has been securely installed, the cryptographic functions are performed automatically, requiring no input by the human User. The cryptographic functions require no Security Attributes outside of the secure values automatically generated by the functions themselves (cryptographic keys), which have been validated by the CMVP FIPS 140-2 evaluation of the Certicom JVM within the GIS TOE.

5.4.4 Strength of Function Claim and Rationale For SOF Claim for Security Functional Requirements

This ST claims a minimum strength of function level of SOF-basic for the TOE security functional requirements.

The rationale for the chosen level of SOF-basic is based on the low attack potential of the threat agents identified. The evaluated TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information. The security objectives imply probabilistic or permutational security mechanism and the metrics defined are the minimal "industry" accepted (for the passwords) metrics that should be good enough for SOF-Basic.

The minimum strength level for the TOE security functions realized by a probabilistic or permutational mechanism is SOF-basic. Specific strength of function metrics are defined for the following requirements:

FIA_UAU.2

5.5 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) as defined by the CC with an augmentation for including ALC_FLR.1. The assurance components are summarized in the following table.

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
ALC Life Cycle Support	ALC_FLR.1	Basic Flaw Remediation
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

Table 5-7 - Assurance Requirements: EAL2

5.6 Assurance Requirements Rationale

EAL2 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.

Sterling has chosen to pursue a Common Criteria evaluation because of the government customer requirements that are mandated by NSTISSC Policy 11. This policy requires a Common Criteria certification for all products to be used within systems used for entering, processing, storing, displaying, or transmitting national security information.

Sterling has specifically chosen an EAL2 evaluation assurance level to meet the requirements mandated by the DoD and Air Force divisions of the government in accordance with the US DoD NSTISSP #11 Interpretation and the USAF CIO Memorandum.

The augmentation of ALC_FLR.1 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

6 TOE Summary Specification

6.1 TOE Security Functions

The TOE Security Functions are identified in chapter 2 of this document. They are as follows:

- Audit
- Communication
- Access Control and Information Flow
- Identification and Authentication
- Security Management
- Protection of Trading Partner Data in Transit
- Protection of the TOE Security Functions

6.1.1 Audit

The TOE auditing function is distributed through the TOE. An overview of the functionality of this distributed auditing function is given below.

Audit Data Generation	Each GIS component generates its own audit records, which are stored in a file unique to that component. This collection of files is called the *audit trail.*
Audit Data Review	Audit trail review is provided by the User Interface for the GIS audit logs

6.1.1.1 Audit Data Generation

FAU_GEN.1.1: Each GIS component generates its own audit records, but the majority of the security relevant audit events are generated by the Graphic User Interface. The events in Table 6-1: Auditable Events, are audited by the TOE. Each GIS subsystem generates its own audit records. Note that, while there may be other events that are captured by the GIS subsystems, the following events are the ones of interest to the claims made by this Security Target.

Audit Events
Starting or stopping an adapter
Creation, deletion, and modification of GIS user accounts
Changes to groups, permissions, mailboxes, services or adapter configurations
File transfer, configuration and command information that is transmitted
Successful or unsuccessful attempts to access

GIS objects and resources
Successful or unsuccessful login attempt; SSL client session authentication; authentication using a certificate in a partner profile.

Table 6-1: Auditable Events

Note that the audit functions are distributed throughout the GIS and cannot be disabled, "started" or "stopped" by the TOE. When the TOE is running, auditing is also running. Since the event of starting or stopping the auditing function does not exist, it is not possible or meaningful to audit starting and stopping the auditing functions.

FAU_GEN.1.2: The GIS subsystem audit records in the audit trail include the date and time of the event recorded, the event type, the relevant subject for the audit event, and the outcome of the event is recorded in terms of success or failure.

6.1.1.2 Security Audit review

FAU_SAR.1: The TOE provides for audit review by allowing appropriately authorized users read access to the audit record files and prohibits unauthorized personnel from having this access. There are audit review facilities within the Graphical User Interface and access to the audit trail is controlled based on user identity and permissions.

6.1.1.3 Reliable Time Stamps

FPT_STM.1: The TOE Environment provides a hardware clock that is made available to the TOE via the underlying operating system interface to the hardware clock. All timestamps applied to audit records are derived from the hardware clock.

6.1.2 Communication

Two of the five adapters in the TOE provide non-repudiation of origin and non-repudiation of receipt. They are the EDIINT Message Service and the EDIINT Pipeline Service.

FCO_NRO.1 : Non-repudiation of origin is the ability to ensure that a party to a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated. Digital signatures are used not only to ensure that a message or document has been electronically signed by the person that purported to sign the document, but also, since a digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature. The EDIINT Messaging service and the EDIINT Pipeline Service meet the AS2 protocol and thus provide non-repudiation of origin. These adapters must be configured to perform non-repudiation of origin. When a message is sent by one of the AS2 protocols, a digital signature is attached to the message using the private key of the sender. The recipient can verify the sender's identity by decrypting the digital signature with the public key of the purported sender.

FCO_NRR.1: The sender of an EDIINT message obtains undeniable proof that the recipient received the message and the message was not altered in transit. Non-repudiation of receipt is implemented via an acknowledgment; the recipient of an EDI message returns this acknowledgment to the sender of the EDI message. This acknowledgment contains a cryptographic hash of a portion of the received message ; also, the acknowledgment is digitally signed by the receiver of the EDI message. The EDIINT Messaging Service and the EDIINT Pipeline Service follow the AS2 protocol and thus provide non-repudiation of receipt. The adapters must be configured to perform non-repudiation of receipt. The protocol implementation at both ends of the transmission stores a receiver's signed acknowledgment, called a Message Disposition Notification (MDN), in the trading partner profile. When a transmission is sent by the

GIS, at the receiving end, the EDI protocol automatically sends the MDN back to the sender, thus verifying the GIS received the document._When a system creates a message to send, it remembers the cryptographic hash of a portion of the message as required by the protocol for the format in use. The sender requests a signed acknowledgement when sending the message. The receiver of the message includes in the signed acknowledgement as part of the information signed an independently computed cryptographic hash of a portion of the message as required by the protocol for the format in use with the same hash algorithm as the sender. The sender can compare the received hash with the one it remembers for the message and know that the receiver got the expected data if they match.

6.1.3 Access Control and Information Flow

There are two policies that control access to GIS data and processes. One is an information flow policy that governs behavior of trading partner requests via the adapters, and the other governs the behavior of GUI users regarding GIS objects.

- The Adapter SFP addresses the behavior and access of trading partner requests. This policy applies to trading partner traffic via all claimed adapters, including those requiring login (FTP Server adapter, the HTTP Server adapter, the Connect:Direct adapter) as well as the EDIINT Messaging Service or the EDIINT Pipeline Service. The policy governs sending, processing, and forwarding documents and messages as dictated by the Trading Partner Profile and the capabilities of the adapter. For trading partners using the FTP, HTP, and Connect:Direct adapters, access is first restricted by the capabilities of the adapter and the trading partner profile. If the access is disallowed by the Adapter Policy, the input is dropped. If the access is allowed by the Adapter Policy, and the subject requests access to a GIS object, then the GIS Access Control SFP is invoked as well.

- The GIS Access Control SFP addresses the behavior and access of users who log into the TOE via the Graphic User Interface. It also addresses the behavior of users who use any one of the three adapters that require user login; the FTP Server adapter, the HTTP Server adapter, and the Connect:Direct adapter. If the requested access is allowed by the Adapter Policy, then the GIS Access Control SFP is used to determine this access.

6.1.3.1 The Adapter Information Flow Policy

Trading partners make requests to process messages and data via one of five different adapters in the GIS. The subjects of this policy are trading partners located on systems that are external to the GIS. When the trading partner joins a community of business partners governed by the GIS, a trading profile for that partner is developed which defines such information as communications protocols, enveloping information, and permitted business processes for that partner. Based on these agreements, trading partner information is processed and passed based on the information in the trading partner profile.

FDP_IFC.1: The TOE implements an information flow control policy called the Adapter SFP that addresses the activities of specific subjects with regard to specific information and specific system operations.

Subjects are trading partners with valid GIS trading partner profiles.[5]

- Identification:
  - Trading partner identifier (required)
  - Optional address, phone number, and other related identity information

[5] A trading partner profile is a record for a trading partner which provides the following types of information.

- Protocol
  - Protocol type and name (required)
  - Destination information such as IP addresses, ports, urls, etc.
- Security
  - For FTP, HTTP, and Connect:Direct, a GIS username and password associated with the trading partner
- MDN [6]

Information relevant to this policy includes files and messages passed to and by trading partners. The information is in the payload of the transmission.

Operations of the policy are to process the transmitted data as requested, and to pass data to the desired location.

FDP_IFF.1: Trading partners using the adapters are subject to the Adapter SPF to process data and pass it forward as described in the trading partner profile. The subjects for these events are the trading partners and the information processed the messages and data that are sent to the TOE by the trading partners via the adapters.

The security attributes of the subject are contained within a trading partner profile, a record which describes the following security relevant information:

- trading partner identity,
- communication protocols allowed,
- business processes to be used

Security attributes of the information include

- trading partner identity and
- the business process(es) requested for the message or document transmitted.
- Information destination--Recipient or storage location for processed data.

When files are received via the FTP Server adapter, the HTTP Server adapter or the Connect:Direct adapter, the trading partner is required to log in. If the login succeeds, then the processing continues. If the login fails, the message is rejected. If the trading partner is using the EDIINT Message Service or EDIINT Pipeline service , no login is required by the EDIINT service, but it is provided by the underlying HTTP, FTP, or Connect:Direct Server adapter.

Generally, processing by an adapter proceeds as follows:

- The adapter receives the business message or document.
- The content of the document indicates what business process is to be applied to the message or document. If the business process requested is allowed for that trading partner according to the trading partner profile, then the information is passed to that business process for processing. If the requested business process is not allowed for that trading partner, the data is dropped.
- When the business process(es) requested are completed, the adapter sends the modified business information to the specified destination.
- When files are transmitted, it is packaged as dictated in the trading partner profile and transmitted using the communication protocols defined in the profile.

[6] Note that administrator guidance requires that an MDN be included in all trading partner profiles that are allowed to use the EDIINT adapter services.

6.1.3.2 The GIS Access Control Policy

FDP_ACC.1. The TOE implements an access control policy called the GIS Access Control SFP that addresses the activities of specific subjects with regard to specific objects of the system and specific system operations.

The subjects of the GIS Access Control SFP are GUI users and logged in users of the FTP Server adapter, HTTP Server adapter, and Connect:Direct [7].

The objects of the GIS Access Control SFP consist of: GUI menu items, web templates, Business Processes, mailboxes, messages, keys, certificates, security relevant property files, services, product features..

The operations governed by the policy are those in which a subject attempts to access one of the objects listed.

FDP_ACF.1: The GIS Access Control SFP functions based on rules for access allowed or disallowed. The rules describe relationships between security attributes of a subject and an object which allow or disallow access.

The subject security attributes for users with GIS accounts are:

- User role (e.g. GIS Administrator or Non-Root User),
- UserID,
- User's groups
- User permissions,
- Permissions of User groups
- Processes acting on behalf of trading partner's permissions

Each authenticated user has a role of GIS Administrator or Non-Root User.

The UserID is a unique identifier assigned to an individual when the individual is granted a user account on the GIS. Permissions are tags that identify the objects a user has permission to access. When a user has permission to an object, the permission is for all actions on that object: a user having permission to an object can view, edit, delete, execute, or save that object.

A user can belong to one or more groups. Groups consist of users and other groups, and permissions are assigned to groups as well as to individuals.

The security attributes for the objects are the permissions associated with an object.

A permission is a string that matches the name of the object to which access is restricted. For example, when a business process named 'TestBusinessProcess' is created, a permission with permission_Id named 'TestBusinessProcess' must be created. If no permission is created for the object, it is considered 'public' and anyone has full access. If a permission does exist for an object, the object is considered 'private' and the user has to have the permission assigned to him (or the user must be assigned a group that has that permission.)

The GIS Access Control SFP is invoked in a consistent manner from each subsystem using a common API to a single access control function that is entirely within the GIS TOE. If there are no permissions to the requested object, then access is granted to the object. If there are permissions associated with the object, the user's permission list is checked for one of the permissions assigned to the object. This includes checking the permissions of groups to which the user belongs. Access is granted or denied if

[7] Technically, the subjects are the processes which act on behalf of the users or trading partners, but for convenience they are referred to as users or trading partners

the user of a group to which the user belongs has permission to the object.

6.1.4 Identification and Authentication

Identification and authentication takes place in several different areas of the TOE. They include the GUI for remote management and several of the adapters. All external interfaces providing login and password verification call a single routine to actually perform the authentication, and all such external interfaces use the same files containing user account information.

FIA_UID.2 and FIA_UAU.2: GIS Users access the TOE via a remote management console and the GUI. These consoles are within the trusted network that hosts the TOE, and cannot be accessed from outside the trusted network. [8]

Users attach to the GIS web server using a browser on a remote management console. Users have user accounts created by GIS administrators or other GIS users who have been given permission to create user accounts. Identification for GIS users is via login ID and authentication is accomplished using password verification conforming to SOF-basic. Administrator guidance forbids using the LDAP authentication option for the evaluated configuration of the TOE.

For trading partners, identification and authentication is performed by certificate authentication when the trading partner session is initiated with an adapter. The FTP Server, HTTP Server, and Connect:Direct Server adapters also require a user account be created for the trading partner, and that the trading partner log into that account after connection but before any other actions are allowed. Note that trading partners are outside the trusted network that hosts the GIS, and as such they cannot access the GIS TOE via the remote management console.

6.1.5 Security Management

The TOE supports traditional roles, as well as management of security functions, TSF data, and security attributes for the two TOE SFP.

FMT_SMR.1: The TOE supports traditional roles for users who log into the system. This includes users who access the system via the GUI, FTP adapter, HTTP adapter, and the Connect:Direct adapter. The roles are as follows:

- GIS Administrator
- Non-root User

GIS Administrators are members of the “administrators” group, and have authorization to perform any activities available to the GIS. All other users are Non-Root Users. The GIS Administrator can assign privileges to other users and their groups, which gives a rich set of user capabilities.

FMT_SMF.1 and FMT_MOF.1: Access to TOE security functions controlled by the GIS Access Control SFP and by role enforcement. These two SFR are implemented by a large selection of security functions that can be manipulated by a GIS Administrator as well as by users who have been given permissions to functions, via having access to GUI menus that control the actions of the security functions. See Table 5-3: TOE Security Management Functions and roles, and Table 5-5: Security Management Functions for details.

FMT_MTD.1: TOE data is protected by the GIS Access Control SFP and by role enforcement. See Table 5-4: TSF Data, for details

[8] Note that there is a local console that can be used to log into the operating system. There are GIS scripts that can be run from the OS that use the TOE, but their use is strictly forbidden by administrator guidance, once the product is properly installed on the OS platform.

FMT_MSA.1 and FMT_MSA.3: Management of security attributes for the GIS Access Control SFP and the Adapter SFP are controlled by the GIS Access Control SFP and role enforcement. This includes both role enforcement and access control to security attributes based on the permissions assigned to the user attempting access. Static attribute initialisation is provided vacuously: there are no defaults for the security attributes.

6.1.6 Protection of Trading Partner Data in Transit

The FIPS 140-2 certified cryptographic module and the adapter protocols together provide the following security functionality to the TOE.

- A trusted path for trading partner data transmission
- Protection of trading partner data in transit from unauthorized modification or disclosure
- Generation and destruction of cryptographic keys as well as encryption, decryption, and digital signatures

FTP_TRP.1, FDP_UCT.1, FDP_UIT.1: The TOE provides protection to trading partner data in transit from disclosure and modification by establishing authenticated, encrypted, and signed communication sessions in which trading partner data can be sent or received. As described above, trading partners are authenticated via certificate verification as a part of establishing a session with the GIS via an adapter. Once a session is established, the trading partner data is encrypted when it is sent by the trading partner to the GIS or vice versa. The verification of identity at both endpoints of the communication, together with the encryption of the data in transit also provides a trusted path for trading partner data transmissions.

FCS_CKM.1, FCS_CKM.4, FCS_COP.1: The cryptographic services discussed above include encryption, decryption, and digital signing and are provided by the FIPS 140-2 certified Certicom SB FIPS module. Details can be found in the FIPS 140-2 Security Policy document[9].

6.1.7 Protection of TOE Security Functions

FTP_SEP.1: The hardware/OS platform provides two-state processing and memory management to separate kernel processing from application processing. Note this is in the TOE Environment.

FPT_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 functions are required to be passed prior to access to any operation: these functions ensure that authorized users only gain access to the functions to which they are authorized.

6.2 Rationale for TOE Security Functions

This section provides a table demonstrating the tracing of the 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 5.1.

[9] See Security Builder® FIPS Java Module Version 2.0 FIPS 140-2 Non-Proprietary Security Policy, Certicom Corp. September 27, 2005.

	Audit	Communication	Access control and Information flow	Identification & authentication	Security management	Protection of Trading Partner Data in transit	Protection of the TSF
FAU_GEN.1	x						
FAU_SAR.1	x						
FCO_NRO.1		x					
FCO_NRR.1		x					
FCS_CKM.1						x	
FCS_CKM.4						x	
FCS_COP.1						x	
FDP_ACC.1			x				
FDP_ACF.1			x				
FDP_IFC.1			x				
FDP_IFF.1			x				
FDP_UCT.1						x	
FDP_UIT.1						x	
FIA_UAU.2				x			
FIA_UID.2				x			
FMT_MOF.1					x		
FMT_MSA.1					x		
FMT_MSA.3					x		
FMT_MTD.1					x		
FMT_SMF.1					x		
FMT_SMR.1					x		
FPT_RVM.1							x
FTP_TRP.1						x	
FPT_SEP.1							x

	Audit	Communication	Access control and Information flow	Identification & authentication	Security management	Protection of Trading Partner Data in transit	Protection of the TSF
FPT_STM.1	x						

Table 6-2: Tracing of TSS Security Functions to SFR

6.3 Security Assurance Measures

Note to Evaluator: The version numbers are likely to change throughout the evaluation.

The TOE Assurance measures are listed below.

[ADMSUP]	Administration Supplement for GIS 4.2
[USRSUP]	User Guidance Supplement for GIS 4.2
[ATR]	GIS 4.2 Actual Test Results
[CM]	Configuration Management Documentation for GIS 4.2
[DEL]	Delivery Procedures for GIS 4.2
[DESIGN]	Functional Specifications, High Level Design, and Correspondence Document for GIS 4.2
[ADM1]	GIS 4.2 System Administration Guide
[ADM 2]	GIS 4.2 Role-based Security
[ADM 3]	GIS 4.2 Graphical Process Modeler Guide
[ADM 4]	GIS 4.2 Resource Management Guide
[ADM5]	GIS 4.2 Archiving and Purging Guide
[ADM 6]	GIS 4.2 Managing Services and Adapters
[ADM 7]	GIS 4.2 Navigation Guide
[ADM 8]	GIS 4.2 Monitoring Business Process Operations
[ADM 9]	GIS 4.2 Dashboard Guide
[ADM 10]	GIS 4.2 Using Document Tracking in Gentran Integration Suite
[ADM 11]	GIS 4.2 Performance and Tuning Guide

[ADM 12]	GIS 4.2 Scheduling guide
[ADM13]	GIS 4.2 Trading Partner and Community Management
[ADM14]	GIS 4.2 Services and Adapters
[ADM15]	GIS 4.2 Implementing SSL
[ADM16]	GIS 4.2 Business Process Modeling Guide
[ADM17]	GIS 4.2 Business Process Modeling Best Practices Guide
[ADM18]	GIS 4.2 Reporting Services
[ADM19]	GIS 4.2 Authentication Report
[ADM20]	GIS 4.2 Authorization Report
[ADM21]	GIS 4.2 Admin Audit Report
[ADM22]	GIS 4.2 Business Process Detail Report
[ADM23]	GIS 4.2 Business Process Definition List Report
[ADM24]	GIS 4.2 EDI Compliance Report
[ADM25]	GIS 4.2 EDI Outbound Acknowledgement Report
[ADM26]	GIS 4.2 EDI Translation Detail Report
[ADM27]	GIS 4.2 System Logs Detail Report
[ADM28]	GIS 4.2 Traffic Report
[ADM29]	GIS 4.2 Traffic Summary Report
[ADM30]	GIS 4.2 Translation Status Report
[ADM31]	GIS 4.2 Translation Service Report
[IGS1]	GIS 4.2 Release Notes
[IGS2]	GIS 4.2 System Requirements
[IGS3]	GIS 4.2 Installation Guide
[IGS4]	GIS 4.2 Overview Guide
[IGS5]	GIS 4.2 Perimeter Server Guide
[IGS6]	GIS 4.2 Property Files
[FLR]	GIS 4.2 Flaw Remediation Procedures
[INS]	Gentran Integration Suite Install Guide Version 4.2
[INSSUP]	GIS 4.2 Installation Supplement
[SOF]	Gentran Integration Suite v 4.2 Strength of Function Analysis
[TOE]	TOE, TOE Test resources
[TPL]	GIS 4.2 Test plan and procedure document

[COV]	GIS 4.2 Functional Tests and Coverage document
[VLA]	Gentran Integration Suite v4.2 Vulnerabilities assessment documentation

The following table identifies assurance measures with assurance requirements.

Table 6-3: TOE Assurance Measures

	ACM_CAP.2	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1[10]	ALC_FLR.1	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVA_VLA.1
CM	x													
DEL		X												
INS, INSSUP			X											
DESIGN				X	X	X								
ADM, ADMSUP							X							
USR1-USR13, USRSUP								X						
FLR									X					
TPL, ATR, TOE, COV										X	X	X		
SOF													X	
VLA														X

6.4 Rationale that Assurance Measures meet the Security Assurance Requirements

Assurance Requirements	Assurance Measures	Rationale
ACM_CAP.2.1D, ACM_CAP.2.2D, ACM_CAP.2.3D	CM	The configuration items that comprise the TOE are specified in the document listed here.
ADO_DEL.1.1D, ADO_DEL.1.2D	DEL	Procedures defining the delivery method of the TOE to the consumer are provided in the document listed here.
ADO_IGS.1.1D	INS INSSUP	The steps necessary for secure installation, generation, and start-up of the TOE are described within the documents listed here.

Assurance Requirements	Assurance Measures	Rationale
ADV_FSP.1.1D, ADV_HLD.1D, ADV_RCR.1D	DESIGN	The Design document includes the functional specification, the high level design, and the correspondence representation. The functional specification describes the TSF and the external interface to the TOE. The high-level design describes the TOE subsystems and identifies their interfaces. The correspondence provides or identifies mappings between all adjacent pairs of available TSF representations, from the TSF summary specification through the high level design.
AGD_ADM.1.1D	ADMSUP ADM USR1-USR13, USRSUP	Administrative guidance provides the TOE administrators with detailed, accurate information of how to administer the TOE in a secure manner. Documents listed here satisfy these requirements.
AGD_USR.1.1D	USR1-USR13, USRSUP	User guidance provides the TOE users with detailed, accurate information of how to administer the TOE in a secure manner. Documents listed here satisfy these requirements.
ALC_FLR.1.1D	FLR	Flaw remediation procedures describe how to update the TOE in a secure manner. Documents listed here satisfy these requirements.
ATE_COV.1.1D	TPL, COV	Testing coverage shows the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. The testing coverage is provided within the testing procedure document as it is listed here.
ATE_FUN.1.1D, ATE_FUN.1.2D	TPL, ATR	Functional testing of the TOE involves providing a test plan, test procedure descriptions, expected test results and actual test results.
ATE_IND.2.1D	TOE	Independent testing requires Sterling Commerce to provide the TOE suitable for testing and Sterling Commerce has fulfilled this requirement.

Assurance Requirements	Assurance Measures	Rationale
AVA_SOF.1.1D	SOF	Strength of function analysis requires the developer to provide an analysis of the strength of function claimed in this ST. The TOE makes a claim of SOF-basic.
AVA_VLA.1.1D, AVA_VLA.1.2D	VLA	A vulnerability analysis of the TOE involves describing the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP as to ensure that all obvious vulnerabilities have been addressed. The document listed here satisfies these requirements.

Table 6-4; Security Assurance Measures

7 Protection Profile Claims

This ST does not conform to a PP.

8 Rationale

8.1 Rationale for Security Objectives

The rational for the security objectives is found in section 4.3 .

8.2 Rationale for Security Functional Requirements

The rationale for the security functional requirements is found in section 5.4 and 5.6.

8.3 Rationale for Security Assurance Requirements

The security assurance rationale is found in section 5.6.

8.4 TOE Security Functions Rationale

The TOE Summary specification rationale is found in section 6.2.

8.5 TOE Assurance Measures Rationale

The TOE assurance measures rationale is found in section 6.4

8.6 Protection Profile Rationale

The Protection Profile rationale is found in section 7.

8.7 Rationale for Strength of Function

The Strength of Functions rationale is found in section 5.4.4.