Layer 7 SecureSpan Product Suite 4.1
Security Target

Version 1.0
13 August 2010

Prepared for:
Layer 7 Technologies, Inc.
Suite 405 – 1100 Melville Street
Vancouver, BC
V6E 4A6

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive
Columbia, MD 21046

1. SECURITY TARGET INTRODUCTION 4

1.1 SECURITY TARGET, TOE AND CC IDENTIFICATION 4
1.2 CONFORMANCE CLAIMS 4
1.3 CONVENTIONS, ACRONYMS, AND TERMINOLOGY 5
1.3.1 Acronyms and Abbreviations 5
1.3.2 Terminology 7

2. TOE DESCRIPTION 9

2.1 TOE OVERVIEW 9
2.2 TOE ARCHITECTURE 9
2.2.1 Physical Boundaries 10
2.2.2 Logical Boundaries 11
2.3 TOE DOCUMENTATION 13

3. SECURITY ENVIRONMENT 14

3.1 THREATS 14
3.2 ASSUMPTIONS 14

4. SECURITY OBJECTIVES 15

4.1 SECURITY OBJECTIVES FOR THE TOE 15
4.2 SECURITY OBJECTIVES FOR THE IT ENVIRONMENT 15
4.3 SECURITY OBJECTIVES FOR THE NON-IT ENVIRONMENT 15

5. IT SECURITY REQUIREMENTS 16

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 16
5.1.1 Security audit (FAU) 16
5.1.2 Cryptographic support (FCS) 17
5.1.3 User data protection (FDP) 18
5.1.4 Identification and authentication (FIA) 19
5.1.5 Security management (FMT) 19
5.1.6 Protection of the TSF (FPT) 20
5.1.7 TOE access (FTA) 21
5.2 IT ENVIRONMENT SECURITY FUNCTIONAL REQUIREMENTS 21
5.2.1 Protection of the TSF (FPT) 21
5.3 TOE SECURITY ASSURANCE REQUIREMENTS 21
5.3.1 Configuration management (ACM) 22
5.3.2 Delivery and operation (ADO) 23
5.3.3 Development (ADV) 23
5.3.4 Guidance documents (AGD) 25
5.3.5 Life cycle support (ALC) 26
5.3.6 Tests (ATE) 27
5.3.7 Vulnerability assessment (AVA) 28

6. TOE SUMMARY SPECIFICATION 30

6.1 TOE SECURITY FUNCTIONS 30
6.1.1 Security audit 30
6.1.2 Cryptographic support 31
6.1.3 User data protection 31
6.1.4 Identification and authentication 32
6.1.5 Security management 32
6.1.6 Protection of the TSF 35
6.1.7 TOE access 35
6.2 TOE SECURITY ASSURANCE MEASURES 35
6.2.1 Configuration management 35

6.2.2 Delivery and operation *36*
6.2.3 Development *36*
6.2.4 Guidance documents *36*
6.2.5 Life cycle support *37*
6.2.6 Tests *37*
6.2.7 Vulnerability assessment *37*

7. PROTECTION PROFILE CLAIMS 39

8. RATIONALE 40

8.1 SECURITY OBJECTIVES RATIONALE 40
8.1.1 Security Objectives Rationale for the TOE and Environment *40*
8.2 SECURITY REQUIREMENTS RATIONALE 42
8.2.1 Security Functional Requirements Rationale *42*
8.3 SECURITY ASSURANCE REQUIREMENTS RATIONALE 45
8.4 STRENGTH OF FUNCTIONS RATIONALE 45
8.5 REQUIREMENT DEPENDENCY RATIONALE 46
8.6 EXPLICITLY STATED REQUIREMENTS RATIONALE 46
8.7 TOE SUMMARY SPECIFICATION RATIONALE 47
8.8 PP CLAIMS RATIONALE 47

LIST OF TABLES

Table 1 TOE Security Functional Components 16
Table 2 EAL4 augmented with ALC_FLR.2 Assurance Components 22
Table 3 TOE Security Management roles 33
Table 4 TOE Non-Security Management roles 34
Table 5 Environment to Objective Correspondence 40
Table 6 Objective to Requirement Correspondence 43
Table 7 Security Functions vs. Requirements Mapping 47

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Layer 7 SecureSpan Product Suite v4.1 provided by Layer 7 Inc. The TOE consists of two components; the SecureSpan™ SecureSpan Gateway and the SecureSpan™ SecureSpan Manager that act together to protect applications exposed as Web services, connect applications across security and identity domains, and validate policy compliance end-to-end across a transaction.

The Security Target contains the following additional sections:

- TOE Description (Section 2) - This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Security Environment (Section 3) - This section details the expectations (assumptions) of the environment and the threats that are countered by the TOE and IT environment.
- Security Objectives (Section 4) - This section details the security objectives of the TOE and its environment.

  IT Security Requirements (Section 5) - The section presents the Security Functional Requirements (SFRs) for TOE and IT Environment that supports the TOE, and details the Security Assurance Requirements (SARs) for EAL4 augmented with ALC_FLR.2.
- TOE Summary Specification (Section 6) - The section describes the security functions represented in the TOE that satisfies the security requirements.
- Protection Profile Claims (Section 7) - This section presents any protection profile claims.
- Rationale (Section 8) - This section closes the ST with the justifications of the security objectives, requirements, and TOE summary specifications as to their consistency, completeness and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – Layer 7 SecureSpan Product Suite v4.1 Security Target

ST Version – Version 1.0

ST Date – 13 August 2010

TOE Identification – SecureSpan Product Suite v4.1, comprising SecureSpan Gateway 4.1-6 and SecureSpan Manager Version 4.1 Build 3826

TOE Developer – Layer 7 Inc.

Evaluation Sponsor – Layer 7 Inc.

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- No Protection Profile compliance is claimed
- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.
    - Part 2 Conformant

- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.
    - Part 3 Conformant
    - Assurance Level: EAL4 augmented with ALC_FLR.2
    - Strength of Function Claim: SOF-Medium

1.3 Conventions, Acronyms, and Terminology

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.1 Acronyms and Abbreviations

Acronym / Abbreviation	Definition
ACM	CM (SAR class)
ADO	Delivery and Operation (SAR class)
ADV	Development/Design (SAR class)
AFL	Authentication Failure family of FIA
AGD	Guidance documents (SAR class)
ALC	Life-cycle Support (SAR class)
ASE	ST (SAR class)
ATD	User Attribute Definition family of FIA
ATE	Tests (SAR class)
AVA	Vulnerability Assessment (SAR class)
CC	Common Criteria
CCTL	CC Testing Laboratory
CEM	Common Evaluation Methodology
CCEVS	CC Evaluation and Validation Scheme
CI	Configuration Item
CM	Configuration Management
CMP	CM Plan
DMZ	DeMilitarized Zone
EAL	Evaluation Assurance Level
FAU	Security Audit (SFR class)

Acronym / Abbreviation	Definition
FIA	Identification and Authentication (SFR class)
FMT	Security Management (SFR class)
FPT	Protection of the TOE Security Functions (SFR class)
FSP	Functional Specification
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
GEN	Security Audit Data Generation family of FAU
GUI	Graphical User Interface
HLD	High-level Design
HTTP	Hyper-text Transfer Protocol
HTTPS	Secure HTTP
ID	Identity/Identification
IP	Internet Protocol
IT	Information Technology
ITT	Internal TOE TSF Data Transfer family of FPT
LDAP	Lightweight Directory Access Protocol
MOF	Management of Functions family of FMT
MTD	Management of TSF Data family of FMT
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OS	Operating System
PP	Protection Profile
SAIC	Science Applications International Corporation
SAR	Security Assurance Requirement
SEL	Security Audit Event Selection family of FAU
SFR	Security Functional Requirement
SSL	Secure Socket Layer
SMF	Specification of Management Functions family of FMT
SMR	Security Management Roles family of FMT
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOF	Strength of Function
ST	Security Target
STG	Security Audit Event Storage family of FAU
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TOE scope of control
TSF	TOE Security Functions
TSS	TOE Summary Specification
UAU	User Authentication family of FIA
UID	User Identification family of FIA
US	United States
WSDL	**W**eb **S**ervices **D**escription **L**anguage
XML	Extensible Markup Language
XSL	e**X**tensible **S**tylesheet **L**anguage
XSLT	e**X**tensible **S**tylesheet **L**anguage **T**ransformations

1.3.2 Terminology

Term	Definition
Consumer	A client that connects to the SecureSpan Gateway in an attempt to gain access to its protected services. Consumers (subjects) do not log into the TOE. Consumers can be a human user or an external IT entity.
Credentialing	A set of credentials that are used to process service requests; normally a user name and password.
Extensible Stylesheet Language Transformations (XSLT)	XSLT is a language for transforming XML documents into other XML documents.
Identity Bridging	A mechanism for merging identities from different security domains.
Identity Domains	Bridging of identities that reside in disparate security or identity domains. These domains can be associated with two departments or divisions of the same company or two entirely separate business partners.
Identity federation	An arrangement that can be made among multiple enterprises that lets subscribers use the same identification data to obtain access.
Message Routing	Message Routing assertions define where service messages are sent and what access credentials are required by the back-end service.
Message Transformation	Transformation assertion allows the user to define or specify an XSL stylesheet using the XSL Transformation (XSLT) language. A stylesheet can be embedded within the policy or can fetch a URL from within a message. A stylesheet is used to transform the structure of an XML request or a response message (e.g. to convert data between different XML schemas or to convert XML data into web pages or PDFs).
Schema Validation	The Validate XML Schema assertion allows the administrator to specify a schema for validating Web service or XML application requests or response messages. The assertion is used to protect backend web services against XML parameter tampering (XML parameters in the request are validated to ensure conformance with XML schema specifications) and XDoS attacks (The message structure and content are examined to ensure they are correct).

Term	Definition
Service-level Authentication	The authorized administrator can configure the TOE to use one of the following Service-level authentication methods for the consumers (end-users) of the TOE: • None (Anonymous) - Select this option for anonymous services. No credentials are required • Specify HTTP Credentials - Select this option for basic HTTP authentication. You are prompted to enter your User Name, Password, NTLM Domain, and NTLM Host • Use HTTP Credentials from Request - Select this option to use the HTTP basic or NTLM authentication headers in the request • Attach SAML Sender-Vouches - Select this option to attach a SAML sender-vouches ticket to each outgoing back-end request that was authenticated by the SecureSpan Gateway. This ticket contains the user name of the authenticated user along with an expiration time, and is signed by the SecureSpan Gateway using the SSL certificate. Optionally enter a Ticket expiry time, in minutes (whole number only). Note: This option is enabled only for SOAP web service policies. It differs from the SAML Assertion as follows: o The Attach SAML Sender-Vouches option is being added to the outgoing message from the SecureSpan Gateway to the protected service o The SAML Assertion requires that SAML security already be present in an incoming message from a client application to the SecureSpan Gateway • Send TAI Header - Select this option to require a Trust Association Interceptor (TAI) third-party authentication pass. TAI credential chaining can be used with or without a static user name and password. With TAI, if the SecureSpan Gateway authenticated a user, then the user name of that authenticated user will be included in the IV_USER HTTP header in the outgoing request
SOAP	SOAP is the core communications protocol for the Web, and most Web services use this protocol to talk to each other. SOAP defines the message format in the Web services request.
Threat Protection	The Threat Protection assertions help protect against common web service and XML threats. The TOE includes built-in protection against TCP/IP based attacks, coercive parsing, XML bomb and external entity attacks, schema poisoning, WSDL scanning, and XML routing detours. This built-in protection cannot be disabled.
Transports	The SecureSpan Gateway provides the following transports for both incoming and outgoing messages: • HTTP • HTTPS • FTP • FTPS The transports can be mixed within an assertion (policy). For example, a message can be received (inbound) via FTP and be routed (outbound) using HTTP. In addition, both the HTTP and FTP assertions can be configured to use SSL, and to use any key pair and certificate under management of the SecureSpan Gateway.

2. TOE Description

The Target of Evaluation (TOE) is Layer 7 SecureSpan Product Suite v4.1. The TOE consists of two components; the SecureSpan™ Gateway and the SecureSpan™ Manager that act together to protect applications exposed as Web services, connect applications across security and identity domains, and validate policy compliance end-to-end across a transaction.

2.1 TOE Overview

The central component of the SecureSpan product suite is the SecureSpan Gateway, which is a policy driven XML message processor providing protection from generalized and specific attacks or threats. In addition to threat protection, the SecureSpan Gateway provides support for industry standards such as Extensible Stylesheet Language Transformations (XSLT), (XSLT is a language for transforming XML documents into other XML documents), encryption, identity federation, authentication and authorization. The SecureSpan Gateway mediates communication between web service endpoints and controls the flow of information through the use of policy decisions or assertions. Assertions dictate the requirements that must be satisfied by a message in order to pass the gateway and can limit messages according to their content, attributes, destination, and identity information. The Policy language used by the gateway supports actions such as message blocking, auditing, notifications, message transformation, and will only allow a message to continue if the message satisfies the assertions within the policy.

The SecureSpan Manager is the primary interface provided to configure the SecureSpan Gateway component. The manager enables the administrator to manage users, monitor the operation of the SecureSpan Gateway, and edit or publish policies that enforce the access controls for the protected web services. The SecureSpan Gateway can also be managed by directly connecting a terminal to the appliance. Though this interface is only used if the network is not setup or during troubleshooting as the SecureSpan Gateway appliance comes with SecureSpan Gateway preinstalled and configured.

2.2 TOE Architecture

The TOE is comprised of two components:

SecureSpan Gateway

The SecureSpan Gateway is a hardware-based XML firewall and service gateway designed to protect Web services, and mediate communications between client and services residing in different identity, security or middleware domains.

The SecureSpan Gateway provides runtime control over service level authentication, authorization, credentialing, integrity, confidentiality, schema validation, content inspection, data transformation, threat protection, routing, and logging. The SecureSpan Gateway enforces all security policies including an information flow policy for network traffic, as well as administrator's access to TSF data.

The SecureSpan Gateway interfaces with client-side applications that require communication with web services. Client systems send message requests intended for the web service to the SecureSpan Gateway. The SecureSpan Gateway then functions as a client-side proxy, applying necessary requirements such as identities, protocols, headers, and/or transformations to the message as required by the policy in use. Policies modified on the SecureSpan Gateway through the SecureSpan Manager are automatically applied in real time[1] by the SecureSpan Gateway to ensure that all subsequent messages conform to the updated policy.

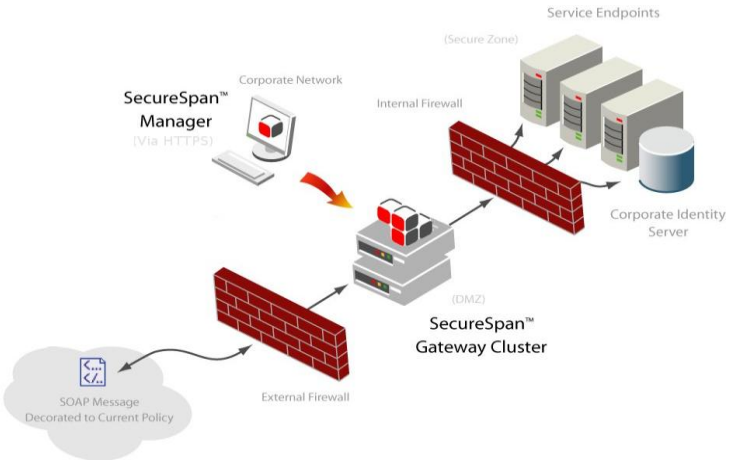
Communication between the SecureSpan Gateway and the SecureSpan Manager occurs over SSL using server certificates.

SecureSpan Manager

[1] 'real time' in this instance is referring to the actual time during which a process takes place or an event occurs and not a technical timing capability.

The SecureSpan Manager application is a GUI application that provides the user with an administrative interface to manage the SecureSpan Gateway. The SecureSpan Gateway, as configured by Layer 7, will only allow communication with the manager on the network that has been designated as "internal". The SecureSpan Manager communicates over SSL, thus encrypting all communication. An Administrator uses SecureSpan Manager to construct Web service and XML application policies, publish XML applications and web services, manage policy users, configure identity bridging, configure auditing and alerting, and monitor the performance of the SecureSpan Gateway. The SecureSpan Manager includes both security management roles and non-security management roles. The security management roles include the authorized Administrator , who has complete control of all management functions and a limited set that are restricted to functions allowed for the particular role. The limited set includes Operators, users assigned to the Manage Internal Users and Groups role, and users assigned to View audit Records and Log role. The complete set of roles and their respective permissions are described in Section 6.1.5 of this ST.

The following diagram illustrates the TOE components setup within a network. The diagram is meant to serve as a visual element to support the discussion. As depicted, there is more than one SecureSpan Gateway (hence a 'cluster'[2]). The diagram also depicts the SecureSpan Gateway being installed inside the corporate DMZ as well as a corporate identity server. It is recommended that the TOE be installed inside the DMZ, however it is not required. As for the Corporate Identity Server, if a Federated Identity Provider (FIP) or LDAP Identity Providers (LIPs) were being used, it would be appropriate for the environment to include an identity server to support the function. However, FIPs and LIPs are not supported in the evaluated configuration, only Internal Identity providers are supported. In addition, the SecureSpan Gateway's capability for virtual partitions, where multiple virtual Gateways can be configured on a single appliance, is not supported in the evaluated configuration. For complete TOE installation procedures, refer to the Layer 7 Administration Guide.



2.2.1 Physical Boundaries

The TOE includes the following components:

- The SecureSpan Gateway application/appliance –The SecureSpan Gateway is hosted in a Sun Fire X4100m2 server running Linux Red Hat Enterprise Server version 4.
- The SecureSpan Manager application - The SecureSpan Manager is available as stand-alone software executable for Windows 2000 or greater, Red Hat Enterprise Linux 4.0 or greater or Solaris 10. However, the standalone version of the SecureSpan Manager must be specifically requested by the purchaser, as it is not shipped with the SecureSpan Gateway. The SecureSpan Manager is required in the evaluated configuration. The TOE is shipped with a Java applet version of the SecureSpan Manager that provides the

[2] Setting up a cluster requires additional configuration steps and additional external components (e.g., a load balancer would be required in the operating environment to support this configuration). The evaluated configuration includes a single SecureSpan Gateway or a SecureSpan cluster.

same level of SecureSpan Gateway manipulation and interaction as the SecureSpan Manager stand-alone application, however it is not included in the evaluated configuration as it does not enforce session locking due to inactivity.

The SecureSpan Gateway appliance includes the following sub-components:

- The Appliance Hardware - SecureSpan Gateway is available in four form factors for maximum deployment flexibility. These include the XML Accelerator, the XML Data Screen, the XML Firewall and VPN and the XML Networking Gateway. The XML Networking Gateway comprises all of the functionality available in the SecureSpan Gateway. There is a single code base and the availability of the features is determined by the license that the customer has purchased. The XML Networking Gateway is the form factor version included in the evaluated configuration.[3]
- Java 1.6.0_02 Virtual Machine
- Redhat Enterprise Linux 4.0 with a custom modified configuration.
- Apache Tomcat Web Container 5.5.28
- Database: My SQL 4.1.20-2
- Sun Crypto Accelerator 6000 PCI-E Adapter. The Sun Crypto Accelerator 6000 PCI-E Adaptor is FIPS 140-2 Level 3 certified, certificate #778

Each sub-component of the SecureSpan Gateway appliance provides services to the SecureSpan Gateway appliance and none of the sub-components exports an interface outside of the SecureSpan Gateway, except for low-level communication support. The sub-components are included in the evaluated configuration.

Communication from the SecureSpan Gateway appliance to the SecureSpan Manager occurs using encrypted communication. No unencrypted communication is accepted by the SecureSpan Gateway. Communication between all TOE components occurs over an SSL secured connection.

The SecureSpan Gateway is also available as a software only product, however the evaluated configuration includes the SecureSpan Gateway application/appliance.

2.2.2 Logical Boundaries

The logical boundaries of the TOE include the security functions implemented at the TOE interfaces. These functions include:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access

2.2.2.1 Security audit

The TOE has the capability to generate audit records of management activities performed by an authorized administrator and of information flow control decisions taken by the SecureSpan Gateway component. Generated audit records contain information that includes date and time of event, type of event, the identity of the subject that caused the event, and the outcome (success or failure) of the event. It should be noted that the SecureSpan Gateway

[3] Refer to Appendix B in the SecureSpan User Guidance for the list of supported features available in each of the form factor versions.

provides the timestamp for the audit records while the IT environment is relied upon to provide a reliable timestamp for the SecureSpan Manager component.

Access to the audit records is restricted to the authorized administrator, thus protecting from unauthorized modification and deletion. The SecureSpan Manager provides a GUI interface for an authorized administrator to review the audit records including searching and sorting the records based on date/time, severity, node identifier, service name, and message text. The TOE also allows an authorized administrator to select which events will be audited. The TOE can be also be configured to send SNMP Trap notifications and/or e-mail message notifications. If SNMP Trap notifications and/or e-mail message notifications assertions are configured, an SNMP server and/or an SMTP server will be required in the operating environment to support this capability.

2.2.2.2 Cryptographic support

The TOE implements cryptographic functionality to support SSL that is used to protect communication between the TOE components from disclosure and modification. The TOE also ensures the cryptographic operations are validated in the policy context and the routing decisions are made in that context. The Sun Crypto Accelerator 6000 PCI-E Adaptor is FIPS 140-2 Level 3 certified, certificate #778.

2.2.2.3 User data protection

TOE enforces the information flow control security policy on service requests sent by consumers to services (SOAP Web services and XML applications) published via the TOE, and on service responses sent by published services to consumers. The information flow does not involve consumers sending messages to other consumers, or web services sending responses to other web services. The TOE enforces the information flow control policy using consumer identities to authenticate the user and policy assertions to validate the content/structure of incoming messages. Accepted messages are routed to the destination service.

2.2.2.4 Identification and authentication

The TOE maintains user IDs, authentication data, and role information for TOE users and user ID, authentication data, and groups for Web service consumers. The Internal Identity Provider (IIP) users and groups are controlled by the TSF. The IIP is populated during installation and configuration of the TOE. There are two types of users defined in the IIP; those that logon to the TOE (TOE users) and those that only appear in the message traffic (Web service consumers). The TOE allows unauthenticated access to Web services on behalf of the user to be performed before the user is successfully identified and authenticated. The TOE also supports multiple authentication methods, credentials such as passwords and X.509 client certificates.

2.2.2.5 Security management

The TOE maintains security management roles and non-security management roles. The users that are assigned to security management roles are considered to be authorized Administrators. The TOE provides the authorized Administrators with the ability to manage the policy assertions (i.e. edit policies), manage user accounts, manage the audit trail, and manage the time interval of user inactivity for session locking using the SecureSpan Manager.

2.2.2.6 Protection of the TSF

The TOE, using SSL creates a secure channel to protect the communication between the SecureSpan Manager and the SecureSpan Gateway. In addition, the TOE ensures that the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. Refer to 6.1.6 Protection of the TSF for detailed information. The SecureSpan Gateway provides the timestamp for the audit records while the IT environment is relied upon to provide a reliable timestamp for the SecureSpan Manager component.

2.2.2.7 TOE access

The TOE provides the capability for the TSF to determinate when there is user inactivity and terminates the session. A user will have to re-authenticate and start a new session.

2.3 TOE Documentation

Layer 7 offers a series of documents that describe the installation process for the SecureSpan Product Suite as well as guidance for subsequent use and administration of the applicable security features. Refer to Section 6.2 TOE Security Assurance Measures for information about these and other documentation associated with the SecureSpan Product Suite.

3. Security Environment

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed. The statement of the TOE security environment defines the following:

- Threats that the TOE is designed to counter
- Assumptions made on the operational environment and the method of use intended for the TOE

3.1 Threats

T.MEDIAT	An unauthorized user may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.
T.NOAUTH	An unauthorized user may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.TRANSMIT	An unauthorized user may eavesdrop on communications between separate parts of the TOE allowing them to intercept and modify transmitted information.
T.TUSAGE	The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized users.

3.2 Assumptions

A.LOCATE	The components of the TOE critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

4. Security Objectives

This section defines the security objectives of the TOE and its supporting environment. Security objectives, categorized as either IT Security Objectives for the TOE, IT Security Objectives for the Environment, and Non-IT Security Objectives for the Environment, reflect the stated intent to counter identified threats and address the identified assumptions. All of the identified threats and assumptions are addressed under one of the categories below.

4.1 Security Objectives for the TOE

O.AUDIT The TOE must protect and generate audit records for data accesses and use of the TOE functions.

O.CRYPTO-OPS All cryptographic operation performed by the system will be compliant with the requirements of FIPS 140-1 or FIPS 140-2.

O.DATA_TRANSFER The TSF must have the capability to protect TSF data in transmission between distributed parts of the TOE.

O.IDAUTH The TOE must uniquely identify and authenticate all users before granting a user access to protected TOE functions.

O.MEDIAT The TOE shall control the flow of all information passing through the TOE and enforce the information flow rules for the TOE.

O.SECFUN The TOE must provide functionality that enables an authorized user to use the TOE security management functions, and must ensure that only authorized users are able to access such functionality.

O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass the TOE security functions.

4.2 Security Objectives for the IT Environment

OE.TOE_PROTECTION The IT Environment will protect the TOE and its assets from interference or tampering.

OE.TIME The IT Environment will provide reliable timestamp for the use of the SecureSpan Manager component.

4.3 Security Objectives for the Non-IT Environment

OE.GUIDAN The TOE must be delivered, installed, administered, and operated in a manner that maintains security.

OE.LOCATE Those responsible for the TOE must ensure that the parts of the TOE critical to security policy enforcement are protected from physical attack that might compromise the TOE security objectives.

OE.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

OE.NOEVIL The administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

5. IT Security Requirements

This section defines the security functional requirements for the TOE as well as the security assurance requirements against which the TOE has been evaluated. The SFRs were drawn from the Part 2 Common Criteria version 2.3. The overall strength of function claim for the TOE is SOF-Medium. The security functional requirement that is associated with permutational or probabilistic mechanisms is related to Identification and Authentication security function, more specifically user authentication (FIA_UAU.2). The cryptographic mechanisms are outside the scope of the CC and not associated with the strength of function claim.

5.1 TOE Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by SecureSpan Product Suite.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit data generation
	FAU_SAR.1: Audit review
	FAU_SAR.3: Selectable audit review
	FAU_SEL.1: Selective audit
	FAU_STG.1: Protected audit trail storage
FCS: Cryptographic support	FCS_COP.1: Cryptographic operation
FDP: User data protection	FDP_IFC.1: Subset information flow control
	FDP_IFF.1: Simple security attributes
FIA: Identification and authentication	FIA_ATD.1a,b: User attribute definition
	FIA_UAU.1: Timing of authentication
	FIA_UAU.5: Multiple authentication mechanisms
	FIA_UID.1: Timing of identification
FMT: Security management	FMT_MOF.1: Management of security functions behaviour
	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_MTD.1a: Management of TSF data
	FMT_MTD.1b: Management of TSF data
	FMT_MTD.1c: Management of TSF data
	FMT_MTD.1d: Management of TSF data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_ITT.1: Basic internal TSF data transfer protection
	FPT_RVM.1a: Non-bypassability of the TSP
	FPT_SEP.1a: TSF domain separation
	FPT_STM.1a: Reliable time stamps
FTA: TOE access	FTA_SSL.3: TSF-initiated termination

Table 1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1)

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) [**Use of the authentication mechanism, adding and removing users, modifying user's attributes, adding and modifying information flow policies, and message traffic information related to message traffic passing between consumers and services**].

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, [**date/time, severity, node identifier, service name, and message text**].

5.1.1.2 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [**authorized Administrator, Operator, and users assigned to the View Audit Records and Logs role]** with the capability to read [**all audit data**] 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.

5.1.1.3 Selectable audit review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to perform [***searches, sorting***] of audit data based on: [**date/time, severity, node identifier, service name, and message text**].

5.1.1.4 Selective audit (FAU_SEL.1)

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes: a) [***event type***] and b) [**no additional attributes**].

5.1.1.5 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

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

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1 The TSF shall perform [**the following cryptographic operations:**

a.) **digital signature generation/verification**

b.) **encryption and decryption**

in accordance with a specified cryptographic algorithm [**listed below**] and cryptographic key sizes [**listed below**] that meet the following:[**listed below**].

a.) **digital signature generation/verification**[4]

- **algorithm: RSA based on standard PKCS#1 v1.5, key size: 512, 1024, or 2048 bits (cert #142), HMAC based on standard FIPS PUB 198 (cert # 34/88), SHA-1 based on FIPS PUB 180-1 (cert # 171/172), DSA based on FIPS PUB 186-2 (cert #92)**
- **Modes of operation: N/A**

b.) **encryption and decryption**

- **algorithm: 3DES based on standard: FIPS PUB 46-3, Certificate #190**
- **key size: 168 bits**
- **Modes of operation: CBC**

c.) **encryption and decryption**

- **algorithm: AES based on standard: FIPS 197, Certificate #79**

[4] Signatures are applied in accordance with the W3C XML Signature Syntax and Processing specifications (http://www.w3.org/TR/xmldsig-core/).

- **key size: 128 or 256 bits**
- **Modes of operation: CBC**

5.1.3 User data protection (FDP)

5.1.3.1 Subset information flow control (FDP_IFC.1)

FDP_IFC.1.1 The TSF shall enforce the [**information flow control policy**] on [
subjects: consumers, Web services;
information: XML and SOAP service requests, Web service responses;
operations: submit request, generate response].

5.1.3.2 Simple security attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the [**information flow control policy**] based on the following types of subject and information security attributes:
[**subject security attributes:**
Web service: address, policy
information security attributes:
Destination address (All information types)
User name and password (All information types)
Message Content (All information types)
XML Schema Validation (XML messages only)
XML Signature Validation (XML messages only)
Port on which the gateway accepts messages (All information types)
Local endpoint descriptor the gateway exposes to consumers (All information types)
Version of SOAP to use for transactions (SOAP messages only)
Requested SOAP Action HTTP Header Value (SOAP messages only)].

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:
[**a: Consumers can cause XML and SOAP service requests to flow through the TOE to a Web service if all the information security attribute values are unambiguously permitted by the receiving Web service policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator.**
b: Web services can cause Web service responses to flow through the TOE to a consumer if all the information security attribute values are unambiguously permitted by the sending Web service policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator].

FDP_IFF.1.3 The TSF shall enforce the [**no additional rules**].

FDP_IFF.1.4 The TSF shall provide the following [**schema validations and malicious or restricted content inspection of the XML and SOAP messages**].

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: [**no additional rules**].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [**The request will be rejected if all parts of the message intended for the requested web service is not included**].

5.1.4 Identification and authentication (FIA)

5.1.4.1 User attribute definition (FIA_ATD.1a)

FIA_ATD.1a.1 The TSF shall maintain the following list of security attributes belonging to individual **TOE** users: [**user ID, authentication data (password), roles**].

5.1.4.2 User attribute definition (FIA_ATD.1b)

FIA_ATD.1b.1 The TSF shall maintain the following list of security attributes belonging to individual **Web service consumer** users: [**user ID, authentication data, groups**].

5.1.4.3 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [**unauthenticated access to Web services, changing the inactivity timeout**] on behalf of the user to be performed before the user is authenticated.

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

5.1.4.4 Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1 The TSF shall provide [**credentials such as passwords and X.509 client certificates**] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**authentication mechanism specified by the authorized administrator**].

5.1.4.5 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow [**unauthenticated access to Web services, changing the inactivity timeout**] on behalf of the user to be performed before the user is identified.

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

5.1.5 Security management (FMT)

5.1.5.1 Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to [***modify, disable, and enable***] the functions [**configuring information flow control policies**] to [**authorized Administrator, Web Service Manager**].

5.1.5.2 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the [**information flow control policy**] to restrict the ability to [***query, modify, delete***] the security attributes [**subject security attributes**] to [**authorized Administrator, Web Service Manager**].

5.1.5.3 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [**information flow control policy**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**no role**] to specify alternative initial values to override the default values when an object or information is created.

5.1.5.4 Management of TSF data (FMT_MTD.1a)

FMT_MTD.1a.1 The TSF shall restrict the ability to [***query [modify the set of audited events, and view]***] the [**audit data**] to [**authorized Administrator (all operations), Cluster Manager (modify), Operator (query and view), and users assigned to the View Audit Records and Logs role (query and view)**].

5.1.5.5 Management of TSF data (FMT_MTD.1b)

FMT_MTD.1b.1 The TSF shall restrict the ability to [***query [and view]***] the [**information flow control policies**] to [**authorized Administrator, Operator, View Service Metrics, and Web Service Manager,**].

5.1.5.6 Management of TSF data (FMT_MTD.1c)

FMT_MTD.1c.1 The TSF shall restrict the ability to [***modify, delete [create]***] the [**user security attributes**] to [**authorized Administrator and users assigned to Manage Internal Users and Group role (create and modify)**].

5.1.5.7 Management of TSF data (FMT_MTD.1d)

FMT_MTD.1d.1 The TSF shall restrict the ability to [***modify, delete [import]***] the [**X.509 client certificates**] to [**authorized Administrator and Manage Certificates role**].

5.1.5.8 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [**management of audit functions, management of information flow control policy and associated security attributes, management of user accounts, management of user inactivity session locking intervals, and management of X.509 client certificates**].

5.1.5.9 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [**authorized Administrator, Operator, users assigned to the Manage Internal Users and Group role, Web Service Manager, Cluster Manager, View Service Metrics, users assigned to View Audit Records and Logs role, and Manage Certificates role**].

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

5.1.6 Protection of the TSF (FPT)

5.1.6.1 Basic internal TSF data transfer protection (FPT_ITT.1)

FPT_ITT.1.1 The TSF shall protect TSF data from [***disclosure***, ***modification***] when it is transmitted between separate parts of the TOE.

5.1.6.2 TSF domain separation (FPT_SEP.1a)

FPT_SEP.1a.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1a.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.6.3 Non-bypassability of the TSP (FPT_RVM.1a)

FPT_RVM.1a.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.6.4 Reliable time stamps (FPT_STM.1a)

FPT_STM.1a.1 The ~~TSF~~ **SecureSpan Gateway** shall be able to provide reliable time stamps for its own use.

5.1.7 TOE access (FTA)

5.1.7.1 TSF-initiated termination (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [**configurable time interval of user inactivity**]..

5.2 IT Environment Security Functional Requirements

This section defines the security functional requirements for the IT Environment in which the TOE operates. The SFRs were drawn from the Part 2 Common Criteria version 2.3.

Requirement Class	Requirement Component
FPT: Protection of the TSF	FPT_RVM.1b: Non-bypassability of the TSP
	FPT_SEP.1b: TSF domain separation
	FPT_STM.1b: Reliable time stamps

5.2.1 Protection of the TSF (FPT)

5.2.1.1 Non-bypassability of the TSP (FPT_RVM.1b)

FPT_RVM.1b.1 The ~~TSF~~ **IT Environment** shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2.1.2 TSF domain separation (FPT_SEP.1b)

FPT_SEP.1b.1 The ~~TSF~~ **IT Environment** shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1b.2 The ~~TSF~~ **IT Environment** shall enforce separation between the security domains of subjects in the ~~TSC~~ **IT environment's scope of control**.

5.2.1.3 Reliable time stamps (FPT_STM.1b)

FPT_STM.1b.1 The ~~TSF~~ **IT Environment** shall be able to provide reliable time stamps for ~~its own use~~ **the use of the SecureSpan Manager component**.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL4 augmented with ALC_FLR.2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_AUT.1: Partial CM automation
	ACM_CAP.4: Generation support and acceptance procedures
	ACM_SCP.2: Problem tracking CM coverage
ADO: Delivery and operation	ADO_DEL.2: Detection of modification
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.2: Fully defined external interfaces
	ADV_HLD.2: Security enforcing high-level design
	ADV_IMP.1: Subset of the implementation of the TSF
	ADV_LLD.1: Descriptive low-level design

Requirement Class	Requirement Component
	ADV_RCR.1: Informal correspondence demonstration
	ADV_SPM.1: Informal TOE security policy model
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ALC: Life cycle support	ALC_DVS.1: Identification of security measures
	ALC_FLR.2: Flaw reporting procedures
	ALC_LCD.1: Developer defined life-cycle model
	ALC_TAT.1: Well-defined development tools
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.1: Testing: high-level design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.2: Validation of analysis
	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.2: Independent vulnerability analysis

Table 2 EAL4 augmented with ALC_FLR.2 Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Partial CM automation (ACM_AUT.1)

ACM_AUT.1.1d The developer shall use a CM system.
ACM_AUT.1.2d The developer shall provide a CM plan.
ACM_AUT.1.1c The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation.
ACM_AUT.1.2c The CM system shall provide an automated means to support the generation of the TOE.
ACM_AUT.1.3c The CM plan shall describe the automated tools used in the CM system.
ACM_AUT.1.4c The CM plan shall describe how the automated tools are used in the CM system.
ACM_AUT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 Generation support and acceptance procedures (ACM_CAP.4)

ACM_CAP.4.1d The developer shall provide a reference for the TOE.
ACM_CAP.4.2d The developer shall use a CM system.
ACM_CAP.4.3d The developer shall provide CM documentation.
ACM_CAP.4.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.4.2c The TOE shall be labeled with its reference.
ACM_CAP.4.3c The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.
ACM_CAP.4.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.4.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.4.6c The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE..
ACM_CAP.4.7c The CM system shall uniquely identify all configuration items that comprise the TOE..
ACM_CAP.4.8c The CM plan shall describe how the CM system is used.
ACM_CAP.4.9c The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.4.10c The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.4.11c The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.4.12c The CM system shall support the generation of the TOE.
ACM_CAP.4.13c The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.
ACM_CAP.4.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.3 Problem tracking CM coverage (ACM_SCP.2)

ACM_SCP.2.1d The developer shall provide a list of configuration items for the TOE.
ACM_SCP.2.1c The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.
ACM_SCP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

5.3.2.1 Detection of modification (ADO_DEL.2)

ADO_DEL.2.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.2.2d The developer shall use the delivery procedures.
ADO_DEL.2.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.2.2c The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.
ADO_DEL.2.3c The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.
ADO_DEL.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.
ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Fully defined external interfaces (ADV_FSP.2)

ADV_FSP.2.1d The developer shall provide a functional specification.
ADV_FSP.2.1c The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.2.2c The functional specification shall be internally consistent.
ADV_FSP.2.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.
ADV_FSP.2.4c The functional specification shall completely represent the TSF.
ADV_FSP.2.5c The functional specification shall include rationale that the TSF is completely represented.
ADV_FSP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1d The developer shall provide the high-level design of the TSF.
ADV_HLD.2.1c The presentation of the high-level design shall be informal.
ADV_HLD.2.2c The high-level design shall be internally consistent.
ADV_HLD.2.3c The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.2.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.2.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.2.6c The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.2.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
ADV_HLD.2.8c The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.
ADV_HLD.2.9c The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.
ADV_HLD.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.2.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Subset of the implementation of the TSF (ADV_IMP.1)

ADV_IMP.1.1d The developer shall provide the implementation representation for a selected subset of the TSF.
ADV_IMP.1.1c The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.
ADV_IMP.1.2c The implementation representation shall be internally consistent.
ADV_IMP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_IMP.1.2e The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.4 Descriptive low-level design (ADV_LLD.1)

ADV_LLD.1.1d The developer shall provide the low-level design of the TSF.
ADV_LLD.1.1c The presentation of the low-level design shall be informal.
ADV_LLD.1.2c The low-level design shall be internally consistent.
ADV_LLD.1.3c The low-level design shall describe the TSF in terms of modules.
ADV_LLD.1.4c The low-level design shall describe the purpose of each module.
ADV_LLD.1.5c The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.
ADV_LLD.1.6c The low-level design shall describe how each TSP-enforcing function is provided.
ADV_LLD.1.7c The low-level design shall identify all interfaces to the modules of the TSF.
ADV_LLD.1.8c The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.
ADV_LLD.1.9c The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.
ADV_LLD.1.10c The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.
ADV_LLD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_LLD.1.2e The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.5 Informal correspondence demonstration (ADV_RCR.1)

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

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

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

5.3.3.6 Informal TOE security policy model (ADV_SPM.1)

ADV_SPM.1.1d The developer shall provide a TSP model.

ADV_SPM.1.2d The developer shall demonstrate correspondence between the functional specification and the TSP model.

ADV_SPM.1.1c The TSP model shall be informal.

ADV_SPM.1.2c The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3c The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4c The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

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

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

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

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

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

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

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

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

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

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

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

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

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.

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

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

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

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

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

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

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

5.3.5 Life cycle support (ALC)

5.3.5.1 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1d The developer shall produce development security documentation.

ALC_DVS.1.1c The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2c The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

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

ALC_DVS.1.2e The evaluator shall confirm that the security measures are being applied.

5.3.5.2 Flaw reporting procedures (ALC_FLR.2)

ALC_FLR.2.1d The developer shall provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2d The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3d The developer shall provide flaw remediation guidance addressed to TOE users.

ALC_FLR.2.1c The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2c The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4c The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5c The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6c The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

ALC_FLR.2.7c The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8c The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

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

5.3.5.3 Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1d The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2d The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1c The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2c The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.
ALC_LCD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.4 Well-defined development tools (ALC_TAT.1)

ALC_TAT.1.1d The developer shall identify the development tools being used for the TOE.
ALC_TAT.1.2d The developer shall document the selected implementation-dependent options of the development tools.
ALC_TAT.1.1c All development tools used for implementation shall be well-defined.
ALC_TAT.1.2c The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.
ALC_TAT.1.3c The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.
ALC_TAT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6 Tests (ATE)

5.3.6.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1d The developer shall provide an analysis of the test coverage.
ATE_COV.2.1c The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.2.2c The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.
ATE_COV.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.2 Testing: high-level design (ATE_DPT.1)

ATE_DPT.1.1d The developer shall provide the analysis of the depth of testing.
ATE_DPT.1.1c The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.
ATE_DPT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.3 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.
ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.4 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
ATE_IND.2.1c The TOE shall be suitable for testing.
ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability assessment (AVA)

5.3.7.1 Validation of analysis (AVA_MSU.2)

AVA_MSU.2.1d The developer shall provide guidance documentation.
AVA_MSU.2.2d The developer shall document an analysis of the guidance documentation.
AVA_MSU.2.1c The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AVA_MSU.2.2c The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.2.3c The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.2.4c The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_MSU.2.5c The analysis documentation shall demonstrate that the guidance documentation is complete.
AVA_MSU.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_MSU.2.2e The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.
AVA_MSU.2.3e The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.
AVA_MSU.2.4e The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

5.3.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.
AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.
AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.7.3 Independent vulnerability analysis (AVA_VLA.2)

AVA_VLA.2.1d The developer shall perform a vulnerability analysis.
AVA_VLA.2.2d The developer shall provide vulnerability analysis documentation.
AVA_VLA.2.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

AVA_VLA.2.2c The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

AVA_VLA.2.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.2.4c The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

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

AVA_VLA.2.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.2.3e The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.2.4e The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.2.5e The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

Each of the security function descriptions is organized by the security requirements corresponding to the security function. Hence, each function is described by describing how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions are suitable to satisfy the necessary requirements.

6.1.1 Security audit

The TOE has the capability to generate audit records for the following types of events, use of the authentication mechanism; adding and removing users; modifying user's attributes; adding and modifying information flow policies; and message traffic information related to message traffic passing between consumers and services. The audit events related to the message traffic are those events pertaining to the processing of a policy, such as assertion violations, authentication failures, routing errors, etc.

Generated audit records contain information that includes date and time of event, type of event, the identity of the subject that caused the event, and the outcome (success or failure) of the event. The audit record also includes the date/time, severity level (e.g. INFO, WARNING, SEVERE), node identifier, service name, and message text. The audit records are stored on the SecureSpan Gateway in MySQL and are protected from unauthorized modification and deletion. The SecureSpan Manager provides a GUI interface for the authorized Administrator, Operator, and View Audit Records and Logs role to review the audit records including searching and sorting the records based on the date/time, severity level, node identifier, service name, and events with a specific message text.

The TOE can be configured to send SNMP Trap notifications and/or e-mail message notifications. SNMP Trap assertions are typically used to trigger an alert based on the result of a previous assertion. For example, if the assertion requiring validation fails, then the Send SNMP Trap assertion will execute, hence broadcasting the alert. An e-mail message assertion allows the administrator to instruct the SecureSpan Gateway to deliver a pre-configured e-mail message whenever the assertion is encountered in a policy. For example, the assertion could be placed in an 'At least one assertion must evaluate to true' assertion folder after an 'Evaluate Response XPath' assertion. If the required response message element is not found and the 'Evaluate Response XPath' assertion fails, then the Send E-mail Message assertion will execute. If SNMP Trap notifications and/or e-mail message notifications assertions are configured, the servers to support this capability will be required in the operating environment.

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE generates audit events for the not specified level of audit and the additional events listed above. In addition, the start-up and shutdown of audit functions, the audit function automatically starts at system start-up and can only be shutdown at system shutdown. In both instances, a record of the event is recorded. It is noted that the SecureSpan Gateway component provides timestamps for its own use, while the IT environment provides time stamps for the use of the SecureSpan Manager component.
- FAU_SAR.1: The TOE provides the means for the authorized Administrator, Operator, and View Audit Records and Logs role to read (interpret) all audit records (data).
- FAU_SAR.3: The TOE provides the means to search and sort the audit records by date/time, severity level, node identifier, service name, and events with a specific message text.
- FAU_SEL.1: The TOE provides the means to include or exclude audit events based on event type.
- FAU_STG.1: The TOE restricts access to the audit records, therefore preventing unauthorized modification and deletion.

6.1.2 Cryptographic support

The TOE implements cryptographic functionality to protect communication between the Gateway and Manager components by communicating using SSL connections. The TOE also supports processing by the Gateway of secured messages.

A message being processed by the TOE must include cryptographic information to trigger the cryptographic operations (e.g. HTTPS transport). The message communicates with the TOE software, the TOE software makes a call to the JAVA software that is pre-installed and configured, the JAVA software then calls the Sun Crypto Accelerator 6000 PCI-E Adapter. The adapter (and JAVA) performs the necessary operations to satisfy the cryptographic requirements in the policy context and sends the results back to the TOE software. The message is either passed or denied based on the results and the context of the policy that is in place. The Sun Crypto Accelerator 6000 PCI-E Adapter is installed and configured in strict FIPS mode and only FIPS certified algorithms are used regardless of what other algorithms are available.

The SecureSpan Gateway includes the Sun Crypto Accelerator 6000 PCI-E Adapter. The cryptographic functions include digital signature/verification and encryption/decryption. The SecureSpan Manager Java JVM provides the client side cryptographic implementation. The Sun Crypto Accelerator 6000 PCI-E Adaptor is FIPS 140-2 Level 3 certified, certificate #778.

The evaluated configuration uses an "off-the-shelf" Sun Crypto Accelerator 6000 PCI-E Adapter hardware crypto module with no modifications. The Sun Crypto Accelerator 6000 PCI-E Adapter is initialized in “strict FIPS mode” and used exactly as specified by the FIPS 140-2 validation testing; therefore, the dependencies of key generation, key destruction, and secure key values are satisfied by this module's validation as FIPS PUB 140-2 compliant.

The Cryptographic support function is designed to satisfy the following security functional requirements:

- FCS_COP.1: The TOE implements cryptographic functionality to support SSL that is used to protect communication between the TOE components from disclosure and modification. The TOE also supports processing by the Gateway of secured messages.

6.1.3 User data protection

The TOE includes a security policy that mediates the flow of information through the TOE. The TOE mainly brokers which messages (service request and web service response) are allowed to pass through the TOE and which messages (service request and web service response) are rejected. The authorized Administrator can develop a set of policies that are used to control the flow of messages. Policies are composed of assertions that dictate requirements to be satisfied by a message.

For each assertion, if the requirement is met, the assertion is considered to have passed otherwise it is failed. The composition of the assertions allows for a branching of processing based on passes and failures. At the conclusion of a policy evaluation, the policy is considered to have passed if its assertions have passed (or if there was a branch through the processing of the policy that passed). If, and only if, the policy passes, the message is allowed to pass through the gateway. These assertions can be based on the message type (whether or not the TOE recognizes a particular type of message); the message contents (specific elements in the message, identity of the user that is sending the message, or particular headers, for example); destination address; whether or not the message is encrypted or signed, and other protocol artifacts such as whether a web service is intended to be available to a requester.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_IFC.1: The TOE enforces the information flow control policy on SOAP and XML service request and Web service response operations to be sent through the TOE from one subject to another. The information flow does not involve consumers sending messages to other consumers, or web services sending responses to other web services. The subject may be a human user or external IT entity (consumer or Web service).
- FDP_IFF.1: The TOE enforces the information flow control policy using the identity of the subject to authenticate the user of a service, using the SecureSpan Gateway to validate incoming messages and to manage traffic for SOAP and XML messages. The TOE also performs schema validations and malicious or restricted content inspection of the XML and SOAP messages.

6.1.4 Identification and authentication

The TOE can support three different identity providers to identify users and their associated group during authentication, Federated Identity Provider (FIP); LDAP Identity Providers (LIPs); and Internal Identity Provider (IIP). However, FIPs and LIPs are not supported in the evaluated configuration, only Internal Identify Providers are supported.

The Internal Identity Provider (IIP) users and groups are controlled by the TSF. A single Internal Identity Provider (IIP) is pre-configured as the authentication database inside the SecureSpan Gateway. The SecureSpan Manager provides an interface to log onto the TOE and for an authorized Administrator and the Manage Internal Users and Group to modify the users and groups in the IIP. The IIP is populated during installation and configuration of the TOE. There are two types of users defined in the IIP; those that logon to the TOE and those that only appear in the message traffic.

The subjects (consumers) sending messages through the TOE do not log onto the TOE. Authentication requirements for the consumers are dependent on the configuration and requirements for a given Web service.

The SecureSpan Gateway maintains user ID, authentication data (password), roles attribute information for the TOE users and the user ID, authentication data, and groups for Web service consumers. The SecureSpan Gateway performs TOE user authentication using an internal password mechanism. The TOE uses the user ID and password attributes to identify and authenticate all TOE users. TOE users must be successfully identified and authenticated before they are allowed access the TOE and its resources. The password must be between six and thirty-two characters long.

This security function has a strength of function claim of SOF-Medium, more specifically the security functional requirement, FIA_UAU.2.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1: The TOE maintains user IDs, authentication data (passwords), and role information for TOE users and the user ID, authentication data, and groups for Web service consumers.
- FIA_UAU.1: The TOE allows unauthenticated access to Web services on behalf of the user to be performed before the user is authenticated.
- FIA_UAU.5: The TOE provides credentials such as passwords and X.509 client certificates to support user authentication.
- FIA_UID.1: The TOE allows unauthenticated access to Web services on behalf of the user to be performed before the user is identified.

6.1.5 Security management

The TOE includes several functions that need to be managed including the audit function; user accounts, determining the behaviour of the information flow control policies (assertions) to include querying, modifying, deleting, and changing the default security attributes; and the time interval for session locking.

After authenticating to the SecureSpan Manager, the authorized administrator uses the SecureSpan Manager's graphical user interface to create, modify, delete, configure, and implement the information flow policies that permit information flows between consumers and services. By default, no messages can pass through the TOE. Once the information flow policies have been created they are deployed to the SecureSpan Gateway. The TOE uses SSL to protect TSF data transmitted between the SecureSpan Manager and the SecureSpan Gateway.

The authorized Administrator and users assigned to the Manage Internal Users and Groups role uses the SecureSpan Manager to create, modify, and delete user accounts. A user must be assigned to at least one role. A user that is added to a role automatically inherits all the permissions defined for that role. A user can be assigned to multiple roles. The user receives permissions from all of the roles. Note that although a user in the “Manage Certificates” role can import and delete certificates and edit certificate usage options, the “Manage Internal Users and Groups” role associates a certificate with a user account.

Following are the roles supported by the TOE.

Role	Permissions	For more information see
Administrator	Create, read, update, and delete any object in the system	This role provides unrestricted access to the SecureSpan Gateway The SecureSpan Manager describes the features from an Administrator perspective
Users assigned to Manage Internal Users and Groups	Create, read, update, and delete users or groups in the Internal Identity Provider	Internal Identity Provider Users and Groups
Operator	Read-only access to the SecureSpan Gateway	Similar to the Administrator role, except permissions are read only
Users assigned to View Audit Records and Logs	View audit and log details in the SecureSpan Manager	Gateway Audit Events Gateway Log Events
Manage Certificates	Import, read, update, and delete any trusted certificate	Managing Certificates Workflow Using an X.509 Certificate
Manage Cluster Properties	Create, read, update, and delete any cluster property	Managing Cluster-Wide Properties Gateway Cluster Properties
Manage Web Services	Publish any new Web service and edit existing users	Publishing a SOAP Web Service Searching Identity Providers Service Properties
Manage [name of service] Service	Delete, view, update named service	Managing Services Service Properties
View Service Metrics	View any cluster node information, published service, service metrics bin, service usage record	Gateway (Cluster) Status

Note, the reference for more information is information that is provided in the SecureSpan Manager User Manual.

Table 3 TOE Security Management roles

The TOE also supports other roles, though they do not perform any security management functions. Following are the additional roles:

Role	Permissions	For more information see
Manage Cluster Status	Create, read, update, and delete cluster status information	Gateway (Cluster) Status
Manage JMS Connections	Create, read, update, and delete JMS connections	JMS Routing Assertion
Publish External Identity Providers	Create any external (LDAP or Federated) Identity Provider	Federated Identity Providers LDAP Identity Providers
Publish Web	Publish any new web service	Publish SOAP Web Service Wizard

Role	Permissions	For more information see
Services		Searching Identity Providers
Search Users and Groups	Search and view users and groups in all identity providers	Searching Identity Providers

Note, the reference for more information is information that is provided in the SecureSpan Manager User Manual

Table 4 TOE Non-Security Management roles

The SecureSpan Manager is used to set the inactivity timeout. Note that any user that can start the SecureSpan Manager (i.e. has access to the workstation where it is installed) can set the inactivity timeout. Each user can set their own inactivity timeout value. This is not a global value that is set by one administrator or user to cover all other authorized Administrators or users. The timeout period can be set between 1 and 60 minutes. When the time interval has been reached, the SecureSpan Manager will automatically be disconnected from the SecureSpan Gateway. The default value is zero, which disables the timeout. In the evaluated configuration, the timeout must be set to a number greater than zero.

The authorized administrator, Operator, and users assigned to the View Audit Records and Logs role use the SecureSpan Manager to query and view the audit records. The audit records include internal records, such as use of the authentication mechanism, adding and removing users, and modifying information flow policies. The audit trail also includes audit records related to processing a policy on the message traffic.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1: The management functions to modify, disable, and enable the information flow policies are limited to the authorized Administrator.
- FMT_MSA.1: The TOE restricts the ability to query, modify, and delete the subjects security attributes, to the authorized Administrator.
- FMT_MSA.3: The TOE provides restrictive default values for security attributes used to enforce the information flow control policies. The TOE allows no role to specify alternative initial values. After a service is published (using either the Publish SOAP Web Service Wizard, Create WSDL Wizard, or Publish XML Application Wizard), it appears in the [Services] tab and an initial policy is created in the Policy Development window. If the WSDL document of a published Web service contains at least one HTTP(S) binding URL, then the initial policy will include an HTTP(S) Routing assertion preconfigured to point to the HTTP(S) binding URL. It is important to note that before a service is adequately protected, additional policy assertions may need to be defined and configured into a policy that is saved in the SecureSpan Gateway.
- FMT_MTD.1a: The TOE restricts the ability to modify the set of auditable events and query and view the audit records to the authorized Administrator, Operator, and users assigned to the View Audit Records and Logs role.
- FMT_MTD.1b: The TOE restricts the ability to query and view the information flow control policies to the authorized Administrator and Operator.
- FMT_MTD.1c: The TOE provides the ability for the authorized Administrator and users assigned to the Manage Internal Users and Group role to create, modify, and delete the user security attributes.
- FMT_MTD.1d: The TOE provides the ability for the authorized Administrator and users assigned to the Manage Certificate role to import, modify, and delete X.509 client certificates.
- FMT_SMF.1: The required management functions provided by the TOE include the management of audit functions, management of information flow control policy and associated security attributes, management of user accounts, management of user inactivity session locking intervals, and management of X.509 client certificates.
- FMT_SMR.1: The TOE supports the roles identified in the above table. The ‘end-users’ of the TOE do not perform any security management functions. They are the consumers of the information allowed to flow through the TOE. The term consumer can represent an individual human user or external IT entity.

6.1.6 Protection of the TSF

When users access the SecureSpan Gateway via the SecureSpan Manager, the TOE creates a secure channel using SSL to protect the communication between the SecureSpan Manager and the SecureSpan Gateway. This secure communication ensures that the TSF data that is transmitted is protected from modification and disclosure.

The SecureSpan Manager ensures that access to TOE configuration data is restricted to the authorized users (identified in **Table 3 TOE Security Management roles** in Section 6.1.5) by controlling access to the functions provided by the GUI. Similarly, the SecureSpan Gateway ensures that access to web services using the TOE is restricted to authorized consumers by controlling access to its network interfaces.

The TOE, with support from the IT environment, provides the secure operating system for a real-time domain where the TOE software executes. This cooperation ensures that the TOE will not be bypassed or tampered with.

The SecureSpan Gateway provides the timestamp for the audit records.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_ITT.1: The TOE uses SSL to protection communications between the TOE components.
- FPT_RVM.1a: Only authorized users can access the TOE and perform the requested functions. In addition, the information flow control policy cannot be bypassed by its consumers (users).
- FPT_SEP.1a: The TOE is designed to work with the host operating system to actively identify and block attempts to access the TOE and its data.
- FPT_STM.1: The SecureSpan Gateway provides the timestamp for the audit records while the IT environment is relied upon to provide a reliable timestamp for the SecureSpan Manager component.

6.1.7 TOE access

The TOE provides the capability for the TSF to determine activity/inactivity of a user's session. When the time interval has been reached, the SecureSpan Manager will automatically be disconnected from the SecureSpan Gateway and the user must re-authenticate before establishing a new session. The 'user' in this case is referring to the users of the TOE as identified in the Table in Section 6.1.5 and not the consumer (user) of the TOE.

The TOE access function is designed to satisfy the following security functional requirements:

- FTA_SSL.3: The TOE provides the capability for the TSF to determine activity/inactivity of a user's session.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by Layer 7 ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Layer 7 ensures changes to the implementation representation are controlled with the support of automated tools and that TOE associated configuration item modifications are properly controlled. Layer 7 performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, life-cycle documentation, vulnerability analysis documentation, configuration management documentation, and security flaws.

These activities are documented in:

- Layer 7 Configuration Management

The Configuration management assurance measure satisfies the following EAL4 augmented with ALC_FLR.2 assurance requirements:

- ACM_AUT.1

- ACM_CAP.4
- ACM_SCP.2

6.2.2 Delivery and operation

Layer 7 provides delivery documentation and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. Layer 7's delivery procedures describe all applicable procedures to be used to detect modification to the TOE. Layer 7 also provides documentation that describes the steps necessary to install SecureSpan Product Suite in accordance with the evaluated configuration.

These activities are documented in:

- Layer 7 Delivery Procedures
- *Layer 7 Installation Guide found within the* Layer 7SecureSpan Administrator Guidance

The Delivery and operation assurance measure satisfies the following EAL4 augmented with ALC_FLR.2 assurance requirements:

- ADO_DEL.2
- ADO_IGS.1

6.2.3 Development

Layer 7 has numerous documents describing all facets of the design of the TOE. In particular, they have a functional specification that describes the accessible TOE interfaces; a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and their interfaces; a low-level design that further decomposes the TOE architecture into modules and describes each module and their interfaces; and, correspondence documentation that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the actual implementation of the TOE. Furthermore, Layer 7 has a security model that describes each of the security policies implemented by SecureSpan Product Suite. Of course, the implementation of the TOE itself is also available as necessary.

These activities are documented in:

- Layer 7 Design

The Development assurance measure satisfies the following EAL4 augmented with ALC_FLR.2 assurance requirements:

- ADV_FSP.2
- ADV_HLD.2
- ADV_IMP.1
- ADV_LLD.1
- ADV_RCR.1
- ADV_SPM.1

6.2.4 Guidance documents

Layer 7 provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- Layer 7 SecureSpan Administrator Guidance, version 4.1CC, May 26, 2010

- Layer 7 SecureSpan User Guidance, version 4.1CC, May 26, 2010

The Guidance documents assurance measure satisfies the following EAL4 augmented with ALC_FLR.2 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Life cycle support

Layer 7 ensures the adequacy of the procedures used during the development and maintenance of the TOE through the use of a comprehensive life-cycle management plan. Layer 7 applies security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure development of the TOE. Layer 7 has procedures that define the process for accepting and acting upon user reports of security flaws. These procedures describe the acceptance criteria for security flaws, how all security flaws and the status of fixes for each security flaw is tracked, and how corrections and corrective measures are made available as applicable. Layer 7 has a documented model of the TOE life cycle that ensures that the TOE is developed and maintained in a well-defined manner. Layer 7uses well-defined development tools in order to ensure consistent and predictable results while developing the TOE.

These activities are documented in:

- Layer 7 Life Cycle and Flaw Remediation

The Life cycle support assurance measure satisfies the following EAL4 augmented with ALC_FLR.2 assurance requirements:

- ALC_DVS.1
- ALC_FLR.2
- ALC_LCD.1
- ALC_TAT.1

6.2.6 Tests

Layer 7 has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. Layer 7 has documented each test as well as an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested. Actual test results are created on a regular basis to demonstrate that the tests have been applied and that the TOE operates as designed.

These activities are documented in:

- Layer 7 Test Plan and Procedures

The Tests assurance measure satisfies the following EAL4 augmented with ALC_FLR.2 assurance requirements:

- ATE_COV.2
- ATE_DPT.1
- ATE_FUN.1
- ATE_IND.2

6.2.7 Vulnerability assessment

The TOE administrator and user guidance documents describe the operation of SecureSpan Product Suite and how to maintain a secure state. These guides also describe all necessary operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and

reasonable administrator and user references. Furthermore, Layer 7 has conducted a misuse analysis demonstrating that the provided guidance is complete.

Layer 7 has conducted a strength of function analysis wherein all permutational or probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the minimum strength of function claim, SOF-Medium.

Layer 7 performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

These activities are documented in:

- Layer 7 Vulnerability Assessment and Analysis

The Vulnerability assessment assurance measure satisfies the following EAL4 augmented with ALC_FLR.2 assurance requirements:

- AVA_MSU.2
- AVA_SOF.1
- AVA_VLA.2

7. Protection Profile Claims

This Security Target makes no Protection Profile claim.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

	T.MEDIAT	T.NOAUTH	T.TRANSMIT	T.TUSAGE	A.LOCATE	A.MANAGE	A.NOEVIL
O.AUDIT		X		X			
O.CRYPTO-OPS			X				
O.DATA_TRANSFER			X				
O.IDAUTH		X					
O.MEDIAT	X						
O.SECFUN		X		X			
O.SELPRO		X					
OE.TOE_PROTECTION		X					
OE.TIME		X		X			
OE.GUIDAN				X			
OE.LOCATE					X		
OE.MANAGE						X	
OE.NOEVIL							X

Table 5 Environment to Objective Correspondence

8.1.1.1 T.MEDIAT

An unauthorized user may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.

This Threat is satisfied by ensuring that:

- O.MEDIAT: The TOE shall control the flow of all information passing through the TOE and enforce the information flow rules for the TOE.

8.1.1.2 T.NOAUTH

An unauthorized user may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

This Threat is satisfied by ensuring that:

- O.AUDIT: This security objective requires that the TOE generate audit records for data access and use of the TOE functions and therefore ensuring unauthorized attempts to bypass the TOE security can be detected and appropriate action taken.
- O.IDAUTH: This security objective requires that users be uniquely identified and authenticated before accessing the TOE.
- O.SECFUN: This security objective requires that the TOE provide functionality that ensures that only authorized users have access to the TOE security management functions.
- O.SELPRO: This security objective requires that the TOE protect itself from attempts to bypass TOE security functions.
- OE.TOE_PROTECTION: This security objective further protects TOE from inappropriate access as well as protecting application components from interference or tampering.
- OE.TIME: This security objective ensures a reliable timestamp is provided for the use of the SecureSpan Manager component.

8.1.1.3 T.TRANSMIT

An unauthorized user may eavesdrop on communications between separate parts of the TOE allowing them to intercept and modify transmitted information.

This Threat is satisfied by ensuring that:

- O.CRYPTO-OPS: This security objective requires that all cryptographic operations will be compliant with the requirements of FIPS 140-1 or FIPS 140-2.
- O.DATA_TRANSFER: This security objective requires all information that passes through the TOE to be protected.

8.1.1.4 T.TUSAGE

The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized users.

This Threat is satisfied by ensuring that:

- O.AUDIT: This security objective requires that the TOE generate audit records for data access and use of the TOE functions and therefore ensuring inadvertent configuration, use, or administration of the TOE in an insecure manner can be detected and appropriate action taken.
- O.SECFUN: This security objective requires that the TOE provide functionality that ensures that only authorized users have access to the TOE security management functions.
- OE.TIME: This security objective ensures a reliable timestamp is provided for the use of the SecureSpan Manager component.
- OE.GUIDAN: This non-IT security objective requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.

8.1.1.5 A.LOCATE

The components of the TOE critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.

This Assumption is satisfied by ensuring that:

- OE.LOCATE: Those responsible for the TOE must ensure that the parts of the TOE critical to security policy enforcement are protected from physical attack that might compromise the TOE security objectives.

8.1.1.6 A.MANAGE

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

This Assumption is satisfied by ensuring that:

- OE.MANAGE: There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

8.1.1.7 A.NOEVIL

The administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

This Assumption is satisfied by ensuring that:

- OE.NOEVIL: Authorized administrators are non-hostile and follow all administrator guidance.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 6** indicates the requirements that effectively satisfy the individual objectives.

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.AUDIT	O.CRYPTO-OPS	O.DATA_TRANSFER	O.IDAUTH	O.MEDIAT	O.SECFUN	O.SELPRO	OE.TOE_PROTECTION	OE.TIME
FAU_GEN.1	X								
FAU_SAR.1	X								
FAU_SAR.3	X								
FAU_SEL.1	X								
FAU_STG.1	X								
FCS_COP.1		X							
FDP_IFC.1					X				
FDP_IFF.1					X				
FIA_ATD.1a,b				X					
FIA_UAU.1				X					
FIA_UAU.5				X					

	O.AUDIT	O.CRYPTO-OPS	O.DATA_TRANSFER	O.IDAUTH	O.MEDIAT	O.SECFUN	O.SELPRO	OE.TOE_PROTECTION	OE.TIME
FIA_UID.1				X					
FMT_MOF.1						X			
FMT_MSA.1						X			
FMT_MSA.3					X				
FMT_MTD.1a						X			
FMT_MTD.1b						X			
FMT_MTD.1c						X			
FMT__MTD.1d						X			
FMT_SMF.1						X			
FMT_SMR.1						X			
FPT_ITT.1			X						
FPT_RVM.1a							X		
FPT_RVM.1b								X	
FPT_SEP.1a			X						
FPT_SEP.1b								X	
FPT_STM.1a	X								
FPT_STM.1b	X								X
FTA_SSL.3				X			X		

Table 6 Objective to Requirement Correspondence

8.2.1.1 O.AUDIT

The TOE must protect and generate audit records for data accesses and use of the TOE functions.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: The TOE is required to generate audit records for all management activities performed by the administrator and all information flow control decisions.
- FAU_SAR.1: The TOE is required to provide the administrator and operator with the capability to read and interpret all the audit records.
- FAU_SAR.3: The TOE is required to provide the administrator and operator with the capability to sort and search audit records based on user identity and event type.
- FAU_SEL.1: The TOE is required to provide the ability to include or exclude audit records based on event type.
- FAU_STG.1: The TOE is required to protect the audit records from unauthorized modifications and deletions.
- FPT_STM.1a: The SecureSpan Gateway is required to provide a reliable timestamp for the audit records.
- FPT_STM.1b: The IT Environment provides a reliable timestamp for the use of the SecureSpan Manager component.

8.2.1.2 O.CRYPTO-OPS

All cryptographic operation performed by the system will be compliant with the requirements of FIPS 140-1 or FIPS 140-2.

This TOE Security Objective is satisfied by ensuring that:

- FCS_COP.1: The encryption/decryption performed in the TOE's secure domain is compliant with the requirements of FIPS 140-1 or FIPS 140-2.

8.2.1.3 O.DATA_TRANSFER

The TSF must have the capability to protect TSF data in transmission between distributed parts of the TOE.

This TOE Security Objective is satisfied by ensuring that:

- FPT_ITT.1: The TOE is required to protect TSF data from modification when transmitted between TOE components.

8.2.1.4 O.IDAUTH

The TOE must uniquely identify and authenticate all users before granting a user access to protected TOE functions.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1a,b: The TOE is required to manage user attributes.
- FIA_UAU.1: The Web services that do not require authentication are not considered protected TOE functions, therefore he TOE allows unauthenticated access to Web services on behalf of the user to be performed before the user is authenticated. .
- FIA_UAU.5: The TOE provides credentials such as passwords and X.509 client certificates to support user authentication.
- FIA_UID.1: The Web services that do not require authentication are not considered protected TOE functions; therefore the TOE allows unauthenticated access to Web services on behalf of the user to be performed before the user is identified.
- FTA_SSL.3: The TOE is required to terminate the session after an administrator specified time interval of user inactivity and require the user to re-authenticate prior to establishing a new session.

8.2.1.5 O.MEDIAT

The TOE shall control the flow of all information passing through the TOE and enforce the information flow rules for the TOE.

This TOE Security Objective is satisfied by ensuring that:

- FDP_IFC.1: The TOE is required to mediate information flowing through the TOE.
- FDP_IFF.1: The TOE is required to enforce information flow rules established by an administrator.
- FMT_MSA.3: The TOE is required to ensure appropriate default information flow settings and restrict access to change those settings appropriately.

8.2.1.6 O.SECFUN

The TOE must provide functionality that enables an authorized user to use the TOE security management functions, and must ensure that only authorized users are able to access such functionality.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MOF.1: The TOE is required to restrict the ability to determine the behavior of the information flow policy and restrict access to change those settings appropriately.
- FMT_MSA.1: The TOE is required to restrict access to security attributes appropriately.
- FMT_MTD.1a: The TOE is required to restrict the ability to query, modify, and view the audit records to the authorized Administrator, Operator, and View Audit Records and Logs role.

- FMT_MTD.1b: The TOE is required to restrict the ability to query and view the information flow control policies to the authorized Administrator and Operator.
- FMT_MTD.1c: The TOE is required to restrict the ability to manage TSF data and restrict access to change those settings appropriately.
- FMT_MTD.1d: The TOE is required to restrict the ability to manage X.509 client certificates and restrict access to the authorized Administrator and Manage Certificates role.
- FMT_SMF.1: The TOE is required to offer the functions necessary for effective management of the TOE security functions.
- FMT_SMR.1: The TOE is required to define an administrator and operator roles that will be able to perform the applicable security management functions.

8.2.1.7 O.SELPRO

The TOE must protect itself against attempts by unauthorized users to bypass the TOE security functions.

This TOE Security Objective is satisfied by ensuring that:

- FPT_RVM.1a: The TOE is designed to encapsulate its protected resources and offer access only through well-defined interfaces that ensure that the applicable security policies are enforced as configured by an administrator.
- FPR_SEP.1a: The TOE is designed to keep its own functions distinct and separate from those of the untrusted subjects it instantiates and also to keep all of its untrusted subjects distinct and separate from one another.
- FTA_SSL.1: The TOE is required to terminate the session after an administrator specified time interval of user inactivity and require the user to re-authenticate prior to establishing a new session.

8.2.1.8 OE.TOE_PROTECTION

The IT Environment will protect the TOE and its assets from interference or tampering.

This IT Environment Security Objective is satisfied by ensuring that:

- FPT_RVM.1b, FPT_SEP.1: The IT Environment is relied on to ensure that TOE interfaces cannot be bypassed and to provide a secure runtime environment.

8.2.1.9 OE.TIME

The IT Environment will provide reliable timestamp for the use of the SecureSpan Manager component.

This IT Environment Security Objective is satisfied by ensuring that:

- FPT_STM.1b: The IT Environment provides a reliable timestamp for the use of the SecureSpan Manager component.

8.3 Security Assurance Requirements Rationale

This security target claims an assurance rating of EAL 4 augmented with ALC_FLR.2. This target was chosen to ensure that the TOE has a moderate level of assurance in enforcing its security functions when instantiated in its intended environment which imposes no restrictions on assumed activity on applicable networks. Augmentation was chosen to provide the added assurances from having flaw remediation procedures and correcting security flaws as they are reported.

8.4 Strength of Functions Rationale

The overall strength of function claim of SOF-Medium is believed to be commensurate with the overall assurance claim of EAL4 augmented with ALC_FLR.2. The only applicable mechanism of a probabilistic or permutational nature included in this Security Target is associated with the security function, Identification and Authentication where passwords are used by users as evidence of their claimed identities; FIA_UAU.2. The intent is that the

password mechanism meets or exceeds SOF-Medium and the evidence can be found in the strength of function analysis included in Layer 7 Vulnerability Analysis

8.5 Requirement Dependency Rationale

The following table demonstrates that all dependencies among the claimed security requirements are satisfied and therefore the requirements work together to accomplish the overall objectives defined for the TOE.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1a and FPT_STM.1b
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1 and FMT_MTD.1	FAU_GEN.1 and FMT_MTD.1a
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FCS_COP.1	FDP_ITC.1 or FCS_CKM.1) and FCS_CKM.4 and FMT_MSA.2	[FCS_CKM.1] and [FCS_CKM.4] and [FMT_MSA.2]
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.1 and FMT_MSA.3
FIA_ATD.1a,b	none	none
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.5	none	none
FIA_UID.1	none	none
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MSA.1	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_IFC.1
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1 and FMT_SMR.1
FMT_MTD.1a	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1b	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1c	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1d	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_ITT.1	none	none
FPT_RVM.1a	none	none
FPT_RVM.1b	none	none
FPT_SEP.1a	none	none
FPT_SEP.1b	none	none
FPT_STM.1a	none	none
FPT_STM.1b	none	none
FTA_SSL.3	none	none

Functional component FCS_COP.1 depends on the following functional components: FCS_CKM.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction, and FMT_MSA.2 Secure Security Attributes. The cryptographic module is FIPS 140-2 validated. The TOE initializes this module in “strict FIPS mode” and uses this module exactly as specified by the FIPS 140-2 validation testing; therefore, the dependencies of key destruction and secure key values are satisfied by this module's validation as FIPS 140-2 compliant.

8.6 Explicitly Stated Requirements Rationale

There are no explicitly stated requirements in this Security Target.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 7 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security audit	Cryptographic support	User data protection	Identification and authentication	Security management	Protection of the TSF	TOE access
FAU_GEN.1	X						
FAU_SAR.1	X						
FAU_SEL.1	X						
FAU_SEL.3	X						
FAU_STG.1	X						
FCS_COP.1		X					
FDP_IFC.1			X				
FDP_IFF.1			X				
FIA_ATD.1a,b				X			
FIA_UAU.1				X			
FIA_UAU.5				X			
FIA_UID.1				X			
FMT_MOF.1					X		
FMT_MSA.1					X		
FMT_MSA.3					X		
FMT_MTD.1a					X		
FMT_MTD.1b					X		
FMT_MTD.1c					X		
FMT_MTD.1d					X		
FMT_SMF.1					X		
FMT_SMR.1					X		
FPT_ITT.1						X	
FPT_RVM.1a						X	
FPT_STM.1a						X	
FTA_SSL.3							X

Table 7 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.