Sterling Commerce, Inc. Connect:Direct with Secure+ Option v4.5 on IBM OS/390 and z/OS

Security Target

Document Version 0.1

Prepared for:

Sterling Commerce, Inc.
750 W. John Carpenter Freeway
Irving, TX 75039

Prepared by:

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

Table of Contents

List of Tables

List of Figures

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The TOE is the Connect:Direct with Secure+ Option v4.5 on IBM OS/390 and z/OS. This ST is the basis for agreement between developers, evaluators, and consumers on the security properties of the TOE and the scope of this evaluation. The audience for this ST is not only the Common Criteria (CC) evaluators but also developers and those responsible for purchasing, installing, configuring, operating, and using the TOE.

This ST contains the following sections:

- Security Target Introduction (Section 1) – Provides a brief summary of the content of the ST and describes the organization of other sections of this document.
- TOE Description (Section 2) – Provides an overview of the TOE security functions and describes the physical and logical boundaries of the TOE.
- Security Environment (Section 3) – Describes the threats, organizational security policies and assumptions that pertain to the TOE and the environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and the environment.
- Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE and the environment.
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE to satisfy the security requirements and objectives.
- Protection Profile Claims (Section 7) – Provides the identification of any ST Protection Profile claims and the justification to support such claims.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.
- Acronyms (Section 0) – Defines the acronyms used within this ST.

1.1 Security Target, TOE and CC Identification

Table 1: ST and TOE Identification

ST Title	Sterling Commerce, Inc. Connect:Direct with Secure+ Option v4.5 on IBM OS/390 and z/OS Security Target
ST Version	0.1

ST Date	September 5th 2006
TOE Identification	Connect:Direct with Secure+ Option v4.5 on IBM OS/390 and z/OS
Common Criteria (CC) Identification	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005; Parts 2 and 3 (aligned with International Standards Organization 15408:2005). See section 1.2 for more details regarding the TOE's conformance to Common Criteria.
Assurance Level	Evaluation Assurance Level (EAL) 2 augmented with ALC_FLR.2 (Flaw reporting procedures)
Operating System	IBM OS/390 and z/OS 1.6
Keywords	file transfer, secure file transfer, SSL, TLS

1.2 Conformance Claims

This Security Target covers the Sterling Commerce, Inc. Connect:Direct with Secure+ Option v4.5 on IBM OS/390 and z/OS. This ST is conformant to Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005. It is conformant to Part 2 extended and Part 3 augmented.

Sterling Commerce, Inc.'s Connect:Direct with Secure+ Option is being evaluated to Evaluation Assurance Level 2 (EAL2) augmented with ALC_FLR.2 under the Canadian Common Criteria Scheme (CCS) using the Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 2.3, August 2005.

This ST does not claim conformance to any Protection Profile.

1.3 Strength of Environment

The Evaluation Assurance Level chosen for this evaluation is 2 augmented with Flaw Remediation (EAL2+). EAL2+ was chosen to provide a low to moderate level of independently assured security based on availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment.

1.4 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows four operations to be performed on security requirements; *assignment*, *refinement*, *selection*, and *iteration*. The following operations are used within this ST. These operations are presented in the same manner in

which they appear in Parts 2 and 3 of the CC with the following exceptions:

- Completed assignment statements are identified using [*italicized text in brackets*].
- Selections are identified using [*italicized and underlined text in brackets]*.
- Refinements are identified using ***bold and italicized text***.
- Iterations are identified by appending a letter in parenthesis following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

2 TOE Description

This section describes the TOE as an aid to understanding the general capabilities and security provided by the TOE. The TOE description provides the boundary of evaluation, detailing what is being evaluated and what is outside the scope of evaluation.

2.1 Product Type

The Connect:Direct with Secure+ Option (C:D SP) is an application that enables secure peer-to-peer file transfer over an insecure network. For this evaluated TOE configuration, the targeted platform is IBM OS/390 and z/OS[1]. The application consists of two major components:

- Connect:Direct server application
- Connect:Direct Secure+ security enhancement application

The evaluation addresses the configuration of the product with both Connect:Direct Server and Connect:Direct Secure + installed onto a dedicated computer.

2.2 Product Description

C:D SP provides server-based software file-transfer solutions for high-volume applications. C:D SP installations perform periodic, high-capacity file transfers between specific servers, often for financial services or federal government applications. The Transport Layer Security (TLS) protocol is used to perform authentication between servers, and to provide an encrypted channel over which file transfers are performed. This provides security to protect against eavesdropping, tampering, and message forgery.

Connect:Direct (C:D) is a peer-to-peer solution, therefore the Secure+ option must be installed at both end points in order to use cryptography. It is often the case, however, that an organization will require robust security during some file transfers while others may be transferred “in the clear”, because the network between them is considered secure or because the nature of the data does not require protection. C:D SP supports these secure and non-secure data exchange scenarios. Figure 1 illustrates various options for deploying C:D SP within an e-business community.

[1]From here on IBM OS/390 and z/OS platforms will be simply referred to as IBM mainframe, unless explicitly needed.

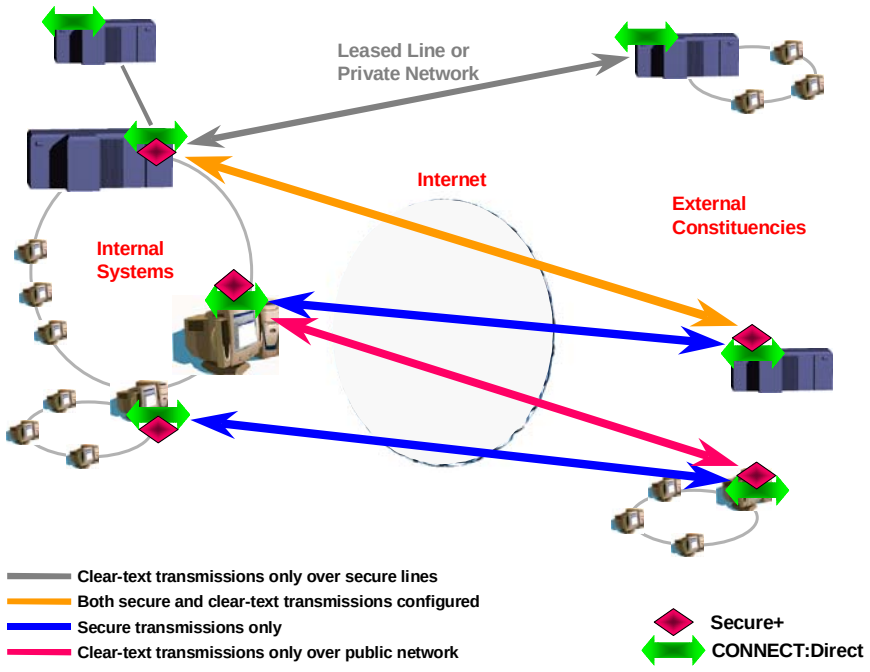

Figure 1: C:D SP Deployment Scenario within an E-business Community

The C:D SP server executes statements and commands submitted through the user interfaces listed below:

- **Applications Programming Interface** (API): The API enables third parties to write programs that work with C:D SP. Through this connection users and administrators issue commands to a C:D SP server application.
- **Command Line Interface** (CLI): The CLI allows users and administrators to access the C:D SP server application. With the CLI users and administrators are able to issue C:D SP commands, monitor jobs, and display job statistics.
- **Interactive User Interface** (IUI): IUI allows users and administrators to build, submit, and monitor C:D SP jobs from an IBM mainframe terminal or with a terminal emulator running from a PC workstation. An administrator can perform tasks, such as viewing and changing the remote server information or initialization parameters.
- **Browser User Interface** (BUI): The BUI allows users and administrators to build, submit, and monitor C:D SP jobs from an Internet browser, such as Microsoft Internet Explorer. An administrator can perform tasks, such as viewing and changing the remote server information and initialization parameters.
- **SPAdmin Tool**: This is the interface through which an administrator will set up the secure connection parameters for C:D SP.

2.3 TOE Boundaries and Scope

2.3.1 Physical Boundary

The physical boundary of the TOE is around the C:D SP applications. It includes the following components:

- SPAdmin
- C:D
- Secure+
- Cryptographic Toolkit
- Stat Manager

Figure 2 illustrates the physical scope and boundary of the TOE and TOE Environment.

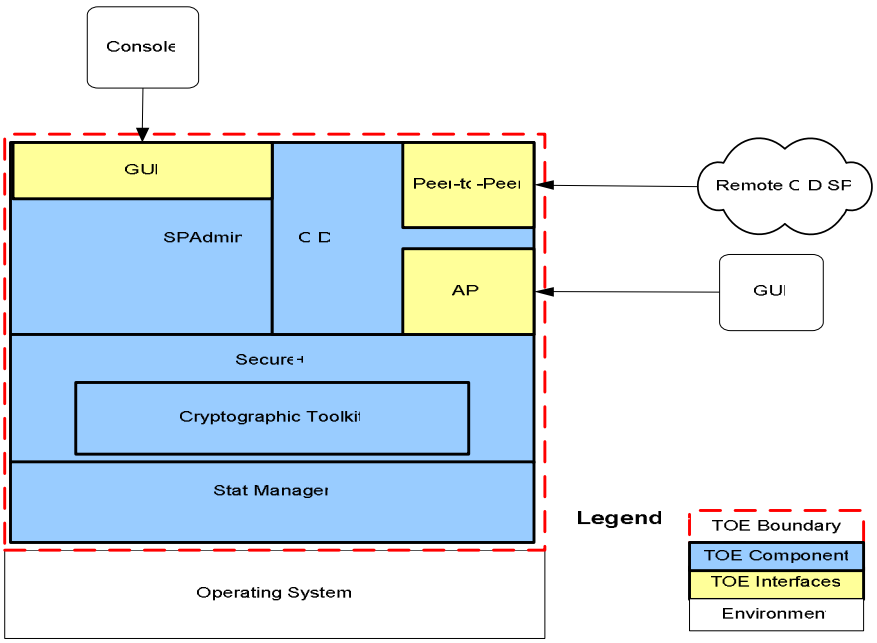

Figure 2: TOE Physical Boundary

C:D, Secure+, and SPAdmin

C:D and Secure+ are discussed in section 2.2. The administrator uses SPAdmin to communicate with and configure Secure+ options. These are the core components of the TOE, and combined they provide the functionality required for secure file transfer operations.

Stat Manager

The Stat Manager is a component of the TOE which is responsible for collecting audit information about the user activities and file transfer operations.

Cryptographic Toolkit

All cryptographic operations within the TOE are performed by the IBM SSL toolkit which relies on a cryptographic hardware module within the mainframe. This module must be installed by an authorized vender of the IBM mainframe systems. This cryptographic toolkit is FIPS 140-2 validated.

2.3.2 TOE Environment Requirements

The TOE is installed on servers that are located in an internal network behind perimeter defenses. The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- TOE software running on machines compliant to minimum requirements as stated in Table 2.
- IUI access inside the protected network for IBM mainframe administration of the TOE compliant to the minimum requirements as stated in Table 2.

Table 2 shows machines compliant to minimum requirements on which to install and run the TOE process.

Table 2: TOE Environment Minimum Requirements

Memory	It is detailed in the “Planning the Installation” chapter of the “Installation Guide” under the heading, “Planning DASD Requirements” on page 4.
Processor	See statement above.

Operating System	IBM OS/390 and z/OS 1.6
Disk Space	It is detailed in the "Planning the Installation" chapter of the "Installation Guide" under the heading, "Planning DASD Requirements" on page 4.
Display	IBM mainframe operator console, terminal, or a terminal emulator from desktop a workstation.
Other Requirements	Crypto chip

2.3.3 Logical Boundary

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Security Management
- Protection of the TOE Security Functions
- Resource Utilization
- Trusted Path/Channel

Security Audit

The TOE logs critical security functions related to user data protection and security management. Audit records are generated by the TOE when users or administrators submit a job or change the configuration. A job is a request for an authorized file transfer. Data related to jobs such as the owner of the job, the status of job, and queue position is written into log files by the Stat Manager. Data relating to specific file transfers, such as progress of file transfer, success or failure, is also gathered. The log files are stored in the TOE environment.

Audit data can be reviewed by an administrator or a user. An administrator can restrict a user's access to have limited or no audit viewing privileges. The audit data that is collected can be included or excluded based on the types of commands that are issued to the TOE. For example 'select statistics' is a command that can be audited or not. This configuration option is set by an administrator. Audit data about file transfer operations can be viewed

from the BUI, IUI, and CLI.

Cryptographic Support

The TOE uses TLS to establish a secure communication channel between a remote system running C:D SP and itself before authorized file transfers can begin. During the TLS handshake the TOE and the remote C:D SP mutually authenticate. The servers then agree on cipher suites and exchange a key which is used as the shared secret during the session. The files are then transferred protected by TLS. Keys are generated and destroyed securely. All cryptographic operations are performed by a FIPS 140-2 validated cryptographic module.

User Data Protection

The user data the TOE is protecting are the transferred files. Users authenticate with the TOE environment and submit jobs to the TOE. Jobs specify the file name, location, and a remote C:D SP node. From a job request, the TOE will determine whether there is a valid entry in the access list for the remote C:D SP node. If so, then the TOE and the remote C:D SP node will mutually authenticate. Then the remote C:D SP node will determine if the TOE user who submitted the job is allowed access to it. If granted access, then the TOE can service user requests to either receive or transmit files.

Security Management

The TOE allows a user who possesses the appropriate privileges to perform management functions. Only authorized TOE users can access management functionality. They must authenticate with the TOE environment before they can access this TSF.

TOE users can take three roles:

- Administrative users access the software to configure the system, update network maps, update security parameters, start and stop the system, create new users and assign privileges, submit jobs, and monitor all activity on the server.
- Users can submit jobs, monitor jobs, and view statistics related to their own jobs. A user cannot monitor the jobs of another user.
- Console operators can access the TOE from a console terminal, perform all the duties of a user, and can shutdown the TOE.

Protection of TOE Security Functions

Non-bypassability of the TOE is provided by basic configuration and enforcement of the security policy rules. The user and administrators' machines are located on the protected network. Administrators must successfully authenticate themselves before performing any security management or policy changes to the TOE. The security policy rules enforced by the TOE are applied to the C:D SP so that every file transfer occurs within the constraints of the policy rules.

The TOE runs only processes that are needed for its proper execution and does not run any other user processes. Portions of the TOE self-protection enforcement (e.g., against physical tampering) are ensured by the TOE environment. In particular, it is assumed that the servers hosting the TOE on the protected network will remain attached to the physical connections made by an authorized administrator responsible for the proper installation of the TOE so that the TOE cannot be bypassed.

Resource Utilization

The TOE provides the means to utilize resources when it is operating on objects for file transfer. The TOE is able to manage utilization of these resources because it services jobs based on their priority and their position in the queue.

Trusted Path/Channel

The TOE provides the means to establish a trusted path between two nodes. The TOE uses TLS to establish the trusted path with a remote server. The TLS protocol's mutual authentication is performed as part of the TLS handshake that initiates a secure communication session. This secure communication session is the trusted path that is used to transfer files between the TOE and a remote C:D SP server.

2.3.4 Exclusions

The following features are not part of the evaluated TOE configuration:

- Strong Access Control
- File Agent
- Station to Station (STS) protocol
- Secure Socket Layer (SSL) protocol

Proxy Access Control

The TOE can use a form of proxy identification and authentication. In this mode a user is given a unique username and password which are then mapped onto username and passwords known to the operating system in the TOE environment. This means that users do not need to be given direct access to accounts on the underlying operating system. This mode is not included in this evaluation.

File Agent

File Agent is an application integration product. It works with files in one or more monitored directories. The File Agent scans these directories for new files. When a file is detected in a watched directory, File Agent either submits a default job to the C:D or performs the actions specified by the rules for the file. The File Agent is not part of the evaluated TOE configuration.

STS Protocol

C:D SP has the option to use STS for file transfer operations. STS is a Sterling Commerce, Inc. proprietary protocol that includes a variation of the basic Diffie-Hellman protocol. STS enables one to establish a shared secret key between two C:D nodes with mutual authentication. To learn more about this protocol, refer to the "Connect:Direct® Secure+ Implementation Guide" Chapter 1. The STS protocol is not part of the evaluated TOE configuration.

SSL Protocol

C:D SP has the option to use SSL as the secure communication channel for file transfer operations. The SSL protocol is not part of the evaluated TOE configuration.

3 Security Environment

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed.

3.1 Secure Usage Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE. The operational environment must be managed in accordance with documentation for delivery and operation. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in environments where this TOE is employed:

Table 3: Assumptions

IDENTIFICATION	DESCRIPTION
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.PHYSICAL	Physical security will be provided for the TOE and its environment.

3.2 Threats to Security

A threat consists of an agent, an asset, and an attack. Threats originate from two types of threat agent: an unauthorized individual and a TOE user. An unauthorized individual has a high motivation to do harm to the TOE but has low skills and resources. These offset and result in a low threat classification. A TOE user has low motivation to do harm to the system and limited resources. Their knowledge of the TOE gives them high skills. These offset and result in a low threat classification.

Table 4 identifies the threats to security.

Table 4: TOE Threats

IDENTIFICATION	DESCRIPTION
T.UNAUTH	An unauthorized individual may breach the confidentiality or integrity of data transferred between TOEs.
T.HOG	A TOE user may prevent high priority tasks from occurring by using too many system resources to process low priority tasks.

3.3 Organizational Security Policies

Table 5 identifies the Organizational Security Policy that the TOE helps to enforce.

Table 5: Organizational Security Policies

IDENTIFICATION	DESCRIPTION
P.VALIDATED_CRYPTO	The TOE shall provide cryptographic functions for its own use. These functions will be provided by a FIPS 140-2 validated cryptographic module.

4 Security Objectives

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

4.1 Security Objectives for the TOE

This section describes the security functionality that is to be achieved by the TOE. Security objectives for the TOE map to threats addressed by the TOE.

The TOE satisfies the following objectives.

Table 6: Security Objectives for the TOE

IDENTIFICATION	DESCRIPTION
O.ADMIN	The TOE must provide a secure method of administrative control of the TOE, ensuring that TOE users with the appropriate privileges, and only these TOE users, can exercise such control.
O.AUDIT	The TOE must provide a robust means of recording security relevant events in sufficient detail to help TOE users detect attempted security violations.
O.VALIDATED_CRYPTO	The TOE shall provide cryptographic functions for its own use. These functions will be provided by a FIPS 140-2 validated cryptographic module.
O.PROTECT	The TOE must protect transmitted files from unauthorized reading or modification.
O.BYPASS [2]	The TOE must ensure that the TSF cannot be bypassed.
O.PRIORITIZE	The TOE must be able to allocate resources based on the priority of the task.

4.2 Security Objectives for the TOE Environment

The Security Objectives for the TOE Environment describe the objectives which must be satisfied if the TOE is to operate securely.

---

[2] *Application Note: Preventing bypass involves ensuring that files which appear to be sent through the TOE are really subject to the TOE's security policies and mechanisms. This depends on the underlying OS in the environment preventing other subjects from bypassing the TOE application (hence OE.BYPASS) and the TOE application ensuring that all it's security mechanisms are invoked and succeed each time the system is used (hence O.BYPASS).*

The TOE Environment satisfies the following IT security objectives.

Table 7: IT Security Objectives for the TOE Environment

IDENTIFICATION	DESCRIPTION
OE.I&A	The TOE environment must uniquely identify all users, and will authenticate the claimed identity before granting a user access to the TOE and resources protected by the TOE.
OE.TIMESTAMPS	The TOE environment must provide reliable timestamps for the use of the TOE.
OE.BYPASS [2]	The TOE environment must ensure that the TSF cannot be bypassed.
OE.AUDITPROTECT	The TOE environment must protect audit files from unauthorized modification or deletion.

The TOE Environment satisfies the following non-IT objectives.

Table 8: Non-IT Security Objectives for the TOE Environment

IDENTIFICATION	DESCRIPTION
OE.MANAGE	Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.
OE.NOEVIL	Sites using the TOE shall ensure that TOE administrators are non-hostile, appropriately trained and follow all administrator guidance.
OE.PHYSICAL	The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects. .

5 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 1.4.

5.1 TOE Security Functional Requirements

The following table provides a summary of the security functional requirements implemented by the TOE. The majority of the SFRs are drawn from Common Criteria Part 2, but the Explicit TSF domain separation SFR (TOE_SEP_(EXP).1) is explicitly stated.

Table 9: Functional Requirements for the TOE Mapped to ST Operations

SFR ID	Description	Selection	Assignment	Refinement	Iteration
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1(a)	Audit review		✓		
FAU_SAR.1(b)	Audit review		✓		
FAU_SEL.1	Selective Audit	✓	✓		
FCS_CKM.4	Cryptographic Key destruction		✓		
FCS_COP.1	Cryptographic Operation		✓		
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FDP_ITC.1	Import of user data without security attributes		✓		
FDP_UCT.1	Basic data exchange confidentiality	✓	✓		
FDP_UIT.1	Data exchange integrity	✓	✓		
FMT_MOF.1 (a)	Management of security functions behaviour	✓	✓		✓
FMT_MOF.1 (b)	Management of security functions behaviour	✓	✓		✓
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.2	Secure Security Attributes				

SFR ID	Description	Selection	Assignment	Refinement	Iteration
FMT_MSA.3	Static Attribute Initialization	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_RVM.1	Non-bypassability of the TOE Security Policy (TSP)				
FRU_PRS.1	Limited Priority of Service		✓		
FTP_ITC.1	Inter-TSF trusted channel	✓	✓		
TOE_SEP_(EXP).1	Explicit TSF domain separation				

Section 5.1 contains the functional components from the CC Part 2 with the operations completed. For the conventions used in performing CC operations please refer to Section 1.4.

5.1.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*not specified*] level of audit; and
c) [*All audit events detailed in Table 10*].

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 ST, [no additional information].

Table 10: Audit Events

Event
Start-up and shutdown of audit functions
Submitting commands to the TOE through BUI, IUI, and CLI
Identification to the TOE through BUI, IUI, and CLI.
Modification made through BUI, IUI, and CLI functions
File Transfer operations

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1(a) Audit Review

FAU_SAR.1.1(a)

The TSF shall provide [*the administrator*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2(a)

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

FAU_SAR.1(b) Audit Review

FAU_SAR.1.1(b)

The TSF shall provide [*the restricted user*] with the capability to read [*all audit information relating to that users actions*] from the audit records.

FAU_SAR.1.2(b)

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_SEL.1 Selective Audit

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*]

b) [*None*].

Dependencies: FAU_GEN.1 Audit data generation, FMT_MTD.1 Management of TSF data

5.1.2 Class FCS: Cryptographic Support

FCS_COP.1 Cryptographic operation

FCS_COP.1.1

The TSF shall perform [*list of cryptographic operations - see table below*] in accordance with a specified cryptographic algorithm [*cryptographic algorithm – see table below*] and cryptographic key sizes [*cryptographic key sizes – see table below*] that meet the following: [*Standard – See table below*].

Table 11: Cryptographic Standards

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Digital signatures	Digital Signature Algorithm (DSA)	1024	FIPS 186-2 (certificate #129, 130, 131)
	Rivest, Shamir, Adleman (RSA)	1024, 2048	PKCS#1 (certificate #55, 56)
	Triple DES (Electronic Code Book (ECB),CBC modes)	168	FIPS 46-3 (certificate #319, 320, 321, 322, 323, 325, 326)
	Advanced Encryption Standard (AES) (ECB, CBC modes)	128, 192, 256	FIPS 917 (certificate #229, 230, 231, 232, 233, 234, 235)
Hashing	Secure Hash 1 (SHA -1)	NA	FIPS 180-2 (certificate #308, 309, 310, 311, 312, 313, 314)
MAC	Hashed Message Authentication Code (HMAC) with SHA-1	160	FIPS 198 (certificate #41, 42, 43, 44, 45; SHA-1 certificate #308, 309, 310, 311, 314 respectively)

Dependencies: FDP_ITC.1 Import of user data without security attributes, FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1

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

Dependencies: FDP_ITC.1 Import of user data without security attributes, FMT_MSA.2 Secure security attributes

5.1.3 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

FDP_ACC.1.1

The TSF shall enforce the [*SECURE FILE TRANSFER SFP*] on

[*a)Subjects: Processes;*

b) Objects: Files;

c) Operations: copy.

].

Application Note: The subjects are processes running on the TOE acting on behalf of an authorised user.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1

The TSF shall enforce the [*SECURE FILE TRANSFER SFP*] to objects based on the following:

[*SUBJECT attributes:*

1) TOE IP address;

2) TOE X.509 public key certificate

3) User access control permissions

OBJECT attributes:

1) File name;

2) File location;

3) IP address of the C:D SP;

4) Identity of the C:D SP].

FDP_ACF.1.2

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

[*a) A valid subject of the TOE is a allowed to copy an object to a remote node if the object is located within the file system of the IT system the TOE is installed on ;*

b) A valid subject of the TOE is allowed to copy an object to the file system of the IT system the TOE is installed on if they have access rights to the remote location;

c) A valid subject of the TOE is allowed to read an object from a remote C:D SP if all the object attributes are valid;

*d) A valid subject of the TOE is allowed to copy an object from a remote C:D SP to a local C:DSP if all the object attributes are valid;***].**

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*all cryptographic keys will be imported securely from the key generation software installed on the underlying hardware*].

Application Note: The TOE is installed on a IBM mainframe computer which will be located in a physically secure location. Cryptographic keys are generated on demand for the TOE by the crypto module installed by IBM. The keys are passed internally to the TOE through the IBM operating system.

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [*no additional rules*].

Dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialisation

FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1

The TSF shall enforce the [*SECURE FILE TRANSFER SFP*] when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the

TSC.

FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [*no additional rules*].

Dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization

FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1

The TSF shall enforce the [*SECURE FILE TRANSFER SFP*] to be able to [*transmit, receive*] objects in a manner protected from unauthorised disclosure.

Dependencies: FDP_ACC.1 Subset access control, FTP_ITC.1 Inter-TSF trusted channel

FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1

The TSF shall enforce the [*SECURE FILE TRANSFER SFP*] to be able to [*transmit, receive*] user data in a manner protected from [*modification, deletion, insertion, replay*] errors.

FDP_UIT.1.2

The TSF shall be able to determine on receipt of user data, whether [*modification, deletion, insertion, replay*] has occurred.

Dependencies: FDP_ACC.1 Subset access control, FTP_ITC.1 Inter-TSF trusted channel

5.1.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 (a)

The TSF shall restrict the ability to [*disable, enable, modify the behavior of*] the functions [*listed in Table 12*] to [*an administrator*].

Table 12: TOE Management Functions

TOE Management Functions
Assign file transfer control rights: Submit/Delete/Change/Monitor/View jobs
Assign resource utilization rights: Ability to change job execution priority
Assign control over TOE: Stop
TOE startup configuration
Assign ability to view audit data
Assign user access to the TOE
Assign remote C:D SP access to the TOE
Loading or removing X.509 certificates used for remote C:D SP authentication
Cryptographic operation used for TLS

FMT_MOF.1.1 (b)

The TSF shall restrict the ability to [*modify the behavior of*] the functions [*listed in Table 13*] to [*an administrator*].

Table 13: Audit Control Functions

Audit Control Functions
Maximum size in of an individual log data file
Whether issued TOE commands are written to the log file, excluding 'select process' or 'select statistics' commands
Whether TOE creates a log record when 'select process' or 'select statistics' commands are issued
Specifies how old a log file must be before it is archived

Dependencies: FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1

The TSF shall enforce the [*SECURE FILE TRANSFER SFP*] to restrict the ability to [*modify*] the security attributes [*user access control privileges*] to [*an administrator*].

Dependencies: FDP_ACC.1 Subset access control, FMT_SMR.1 Security roles, FMT_SMF.1 Specification of management functions

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1

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

Dependencies: ADV_SPM.1 Informal TOE security policy model, FDP_ACC.1 Subset access control, FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1

The TSF shall enforce the [*SECURE FILE TRANSFER SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the *SFP*.

Application Note: The only security attributes which can take default values are user access control privileges.

FMT_MSA.3.2

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

Dependencies: FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1

The TSF shall restrict the ability to [*view, sort*] the [*audit data*] to [*an administrator or user with log viewing permissions*].

Dependencies: FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

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

[*a) Management of security functions behaviour;*

b) Management of TSF data;

c) Management of security attributes].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

FMT_SMR.1.1

The TSF shall maintain the roles [*the authorised identified roles listed in Table 14*].

Table 14: Security Roles

Roles	Description
User	By default, this role allows control over the user specific tasks. They are job submission, monitor status of jobs, change priority of jobs, halting jobs, deleting job, and view statistics of jobs (audit data).
Administrator	This role has access rights to all security management functions (see Table 12) and user functionality.
Console Operator	A mainframe console operator has user functionality and can shutdown the TOE.

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.5 Class FPT: Protection of TOE Security Functions

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within

the TSC is allowed to proceed.

Dependencies: No dependencies

5.1.6 Class FRU: Resource Utilization

FRU_PRS.1 Limited priority of service

FRU_PRS.1.1

The TSF shall assign a priority to each subject in the TSF.

FRU_PRS.1.2

The TSF shall ensure that each access to [*secure file transfer sessions*] shall be mediated on the basis of the subjects assigned priority.

Dependencies: No dependencies

5.1.7 Class FTP: Trusted Path/Channel

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1

The TSF shall provide a trusted channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2

The TSF shall permit [*the TSF and a remote trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [*the file transfer operation*].

Dependencies: No dependencies

5.1.8 Class TOE: Explicitly Stated Requirements

TOE_SEP_(EXP).1 – Explicit TSF domain separation

TOE_SEP_(EXP).1.1

The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

TOE_SEP_(EXP).1.2

The TSF shall enforce separation between the security domains of subjects in the TOE Scope of Control (TSC).

Application Note: A secure and separate domain is provided for the TOE through a combination of mechanisms in the TOE and in the environment. The TOE SFR, TOE_SEP_(EXP).1 ensures that the TOE protects itself from interference through its own interfaces. The environmental SFR, FPT_SEP.1ensures that the TOE is protected from interference by the operating system in the TOE environment.

5.2 TOE Environmental Security Functional Requirements

The following table provides a summary of the security functional requirements implemented by the Environment.

Table 15: Functional Requirements for the TOE Environment

SFR ID	Description	Selection	Assignment	Refinement	Iteration
FAU_STG.1	Protected audit trail storage	✓		✓	
FCS_CKM.1	Cryptographic key generation		✓		
FPT_SEP.1	TSF domain separation			✓	
FPT_STM.1	Reliable time stamps			✓	
FIA_UID.2	User identification before any action			✓	
FIA_UAU.2	User authentication before any action			✓	

5.2.1 Class FAU: Security Audit

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1

The ***TOE environment*** shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2

The ***TOE environment*** shall be able to [*prevent*] unauthorized modifications to the audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

5.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1

The ***TOE environment*** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*cryptographic key generation algorithm – see Table 16 below*] and specified cryptographic key sizes [*cryptographic key sizes see table below*] that meet the following: [*list of standards see table below*].

Dependencies: FCS_COP.1 Cryptographic operation, FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes.

Table 16: Cryptographic Key Generation Standards

Key Generation Type	Algorithm and Key Size	Standards (Certificate #)
Session key generation	TDES CBC 2/3 key	FIPS 46-3 (certificate #319, 320, 321, 322, 323, 325, 326)
	AES CBC 128/256 key	
Public key generation	RSA 1024 bit public key	PKCS#12 (certificate #55, 56)
PRNG seed generation	Triple-DES (168 bits)	FIPS 186-2 PRNG seed
	AES (128, 192, 256 bits)	
	HMAC-SHA-1 (160 bits)	

5.2.3 Class FPT: Protection of TSF

FPT_SEP.1 TSF domain separation

FPT_SEP.1.1

The ***TOE environment*** shall maintain a security domain for ***the TOE's*** execution that protects ***the TOE*** from interference and tampering by untrusted subjects.

FPT_SEP.1.2

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

Dependencies: No dependencies

Application Note: A secure and separate domain is provided for the TOE through a combination of mechanisms in the TOE and in the environment. The TOE SFR, TOE_SEP_(EXP).1 ensures that the TOE protects itself from interference through its own interfaces. The environmental SFR, FPT_SEP.1ensures that the TOE is protected from interference by the operating system in the TOE environment.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1

The ***TOE environment*** shall be able to provide reliable time stamps for ***the use of the TOE.***

Dependencies: No dependencies

5.2.4 Class FIA: Identification and Authentication

FIA_UID.2 User identification before any action

FIA_UID.2.1

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

Dependencies: No dependencies

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1

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

Dependencies: FIA_UID.1 Timing of identification

5.3 TOE Security Assurance Requirements

This chapter defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 17 – Assurance Components summarizes the components.

Table 17: Assurance Components

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

6 TOE Summary Specification

This section details how the TOE meets the functional and assurance requirements described in previous sections of this ST.

6.1 TOE Security Functions

This section provides a high-level definition of the IT security functions provided by the TOE to meet the SFRs and SARs specified in this ST.

6.1.1 Security Audit

Audit Generation

The TOE logs critical security functions related to user data protection and security management. Audit records are generated by the TOE when users or administrators submit a job or change TOE configuration. A job is a request for an authorized file transfer. Data related to jobs such as the owner of the job, the status of jobs, and queue position is written into log files by the Stat Manager. Data relating to specific file transfers, such as progress of file transfer, success or failure, is also gathered. The log files are stored in the TOE environment. See Table 10 for the list of functions that are audited. The audit data that is collected can be included or excluded based on the types of commands that are issued to the TOE. For example the 'select statistics' is a command that can be audited or not. This is set by an administrator.

Audit Review

The audit data can be reviewed by an administrator or a user. A user can be restricted by the administrator to have limited or no audit viewing privileges. While an administrator can read all audit information; restricted users can only read audit information relating to their actions. Audit data about a file transfer operation can be viewed from the BUI, IUI, and CLI. Reports can be generated through the BUI, IUI, and CLI.

TOE Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1(a and b), and FAU_SEL.1.

6.1.2 Cryptographic Support

The TOE uses TLS to establish a secure communication channel between a remote C:D SP node and itself before authorized file transfers can begin. During the TLS handshake's mutual authentication steps, X.509 digital certificates are used for remote C:D SP authentication. The TOE authentication is done using user ID and

password, but optionally it can be configured to use X.509 digital certificates. The servers then agree on cipher suites and exchange a cryptographic key which is used as a shared secret.

During file transfer the sender computes and transmits an HMAC for each payload transmitted (file segments), using the key agreed upon during the handshake phase. The receiver independently computes the HMAC and compares this with the received HMAC. If the comparison fails, it triggers an immediate termination of the file transfer and error messages are generated at both ends. All transmitted files are encrypted using the agreed symmetric algorithm and key. At the end of the session, the key is destroyed by zeroization. Zeroizing keys are done in accordance with the 'Key Zeroization' requirements in FIPS 140-2.

The TOE's cryptographic support is provided by a FIPS 140-2-validated cryptographic module in the TOE. Cryptographic keys are generated on demand for the TOE by the crypto module installed by IBM (i.e. in the environment). The keys are passed internally to the TOE through the IBM operating system. Keys used for each TLS session are generated and exchanged using standards listed in "Table 16: Cryptographic Key Generation Standards". The TOE ensures that only secure values are accepted for the cryptographic keys. During the TLS operation, the payload is encrypted using one of the symmetric encryption algorithms listed in "Table 11: Cryptographic Standards".

FIPS 140-2 certification for C:D SP on IBM mainframe is currently pending with the National Institute of Standards and Technology. .

TOE Functional Requirements Satisfied: FCS_COP.1, FCS_CKM.1, FCS_CKM.4, and FMT_MSA.2.

6.1.3 User Data Protection

The TOE's primary function is to transfer files between itself and a remote C:D SP node. Files being transmitted or received by C:D SP are considered user data within the TOE. Successful file transfer enforces the *SECURE FILE TRANSFER Security functional Policy (SFP)* using the following attributes:

[SUBJECT attributes:

1) TOE IP address;
2) TOE X.509 public key certificate
3) User access control permissions

OBJECT attributes:

1) File name;

2) File location;

3) IP address of the C:D SP;

4) Identity of the C:D SP].

For these attributes, the subject is a process and the objects are files. The policy rule states that a process is allowed to copy an object to a remote node if the object is located within the file system of the IT system the TOE is installed on.

The TOE will deliver the files in the following manner. Users authenticate with the TOE environment and submit jobs to the TOE. Jobs specify the file name, location, and a remote C:D SP node. From the job request, the TOE will determine whether there is a valid entry in the access list for the remote C:D SP node. If so, the TOE and the remote C:D SP node will mutually authenticate. Then the remote C:D SP node will determine if the TOE user who submitted the job is allowed access to the files. If granted access then the TOE can begin to service user requests to either receive or transmit files.

When servicing TOE user requests, the TOE initiates a connection to transmit or receive files. If transmitting files, the TOE reads the files from the TOE environment and transmits it to the remote C:D SP node. If receiving files, the TOE will receive the files and write them to the TOE environment. File transfer operations will occur over an encrypted TLS connection.

The user types for file transfer are described in Table 14. Once a request for a file transfer is submitted, the user does not have to be logged into the TOE during the file transfer operation.

For this evaluated configuration, the end-to-end transport and network layer connection will be established using the TCP/IP protocol. The secure file transfer uses a TLS session. During this operation, sender and receiver compute HMAC for each file segments transmitted. The sender transmits the HMAC and the receiver compares it. When comparisons fail and the TOE is the receiving end-point, it will trigger an immediate termination of the file transfer operation and error messages at both ends of the transaction will be generated. If the transmission was a success, the TOE will acknowledge it by notifying the remote C:D SP node. This mechanism ensures that modification, deletion, insertion, or replay has not occurred on receipt of files.

TOE Functional Requirements Satisfied: FDP_ACF.1, ADP_ACC.1, FDP_UCT.1, and FDP_UIT.1.

6.1.4 Security Management

The TOE allows a user who possesses the appropriate privileges to perform management functions. Only authorized TOE users can access management functionality. They must authenticate with the TOE environment before they

can access this TSF.

TOE users can take three roles:

- Administrative users access the software to configure the system, update network maps, update security parameters, start and stop the system, create new users and assign privileges, submit jobs, and monitor all activity on the server, and modify the TOE audit settings to include or exclude some event types. See section 5.1.1 under "FAU_SEL.1 Selective Audit" for specific details.
- Users can submit jobs, monitor jobs, and view audit data (statistics) related to their own jobs. A user cannot monitor the job of another user. These features can be further restricted by an administrator.
- Console operators can access the TOE from a console terminal, perform all the duties of a user, and can shutdown the TOE.

The administrator must have a user ID and password to authenticate to the server where the TOE is running. Access to start the TOE is controlled by the standard access control mechanisms of the TOE environment. These may be file permissions for the executable files, access control lists, rules enforced by access control software or whatever mechanism the organization has chosen to govern access to executable files. The TOE is shipped with a default administrator user ID and default password.

The TOE may be shut down in two ways by the administrator or the console operator. A normal, managed shutdown is accomplished by logging onto the TOE and executing the appropriate shutdown sequence. An emergency or unmanaged shutdown can be accomplished using operating system kill or cancel facilities. The user must have operating system level authority to execute the kill/cancel operation.

Table 12 and Table 13 in section 5 lists the TOE management functions.

TOE Functional Requirements Satisfied: FMT_MOF.1 (a), FMT_MOF.1 (b), FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1.

6.1.5 Protection of TOE Security Functions

Non-bypassability of the TOE is provided by the basic configuration and enforcement of the security policy rules. The functions that enforce the TSP will always be invoked before any function within the TSF scope of control is allowed to proceed. The TOE can be accessed through the API based applications, the CLI on the system hosting the TOE, the BUI, IUI and SPAdmin from the IBM mainframe terminal or terminal emulator from a PC workstation.

The user and administrator consoles are located on a protected network. They must successfully authenticate before performing any security management or policy changes to the TOE. The security policy rules enforced by the TOE are applied to C:D SP, so that every file transfer occurs within the constraints of that policy.

The TOE runs only processes that are needed for its proper execution and does not run any other user processes. Aspects of TOE protection are ensured by the TOE environment. In particular, it is assumed that the servers hosting the TOE on the protected network will remain attached to the physical connections made by an authorized administrator responsible for the proper installation of the TOE, so that the TOE cannot be bypassed.

Separation of domain is provided by the operating system and explicitly by the TOE. A user or an administrator must authenticate to the operating system before accessing the TOE. The permissions and credentials of that user account will enforce access control rights to the files on which the TOE will operate during file transfer. The TOE maintains a security domain for its own execution and enforces separation between the security domains of subjects in its scope of control through concurrent sessions. This allows multiple users to connect to the TOE during job submission, reviewing audit data, administration, and while multiple file transfer operations occur.

TOE Functional Requirements Satisfied: FPT_SEP_.1, and FPT_RVM.1.

6.1.6 Resource Utilization

The TOE provides the means to utilize resources when it is operating on objects for file transfer. The TOE is able to manage utilization of these resources because it services jobs based on their priority and position in the queue. The TOE accepts job submissions for file transfer from the TOE user and administrator. During submission, jobs are assigned a priority of execution and order of execution. The priority of the job submission is entered by the user or administrator as a request parameter, 1–15, where 15 is the highest priority. If no priority number is specified during submission, the default is 10.

When jobs are submitted to the TOE they enter the Transmission Control Queue (TCQ). The TCQ controls when jobs will get serviced. The TCQ is divided into four logical queues: **Execution**, **Wait**, **Timer**, and **Hold**. Jobs are placed into the appropriate logical queue based on submission parameters. Jobs can only be serviced from the **Execution** queue.

By the usage of these mechanisms, the TOE is able to manage the utilization of resources because it services jobs based on priority and position in the queue. When a job enters the **Execution** queue, its position in the queue is determined by priority.

TOE Functional Requirements Satisfied: FRU_PRS.1.

6.1.7 Trusted Path/Channel

The TOE provides the means to establish a trusted path between two C:D SP nodes. The TOE looks up the previously configured network information for the node the file needs to be sent to. This information includes the Server-ID (a logical name given during C:D SP setup), DNS name, and IP address. Once a TCP/IP connection is established, the TOE uses the previously configured security information to establish a TLS session with a remote C:D SP server. It performs mutual authentication and exchanges cryptographic keys as part of the TLS handshake. The established TLS session is the trusted path used to transfer files between the TOE and a remote C:D SP server.

TOE Functional Requirements Satisfied: FTP_ITC.1.

6.2 TOE Security Assurance Measures

This section of the ST maps assurance requirements to measures used for development and maintenance of the TOE. The following table provides a mapping of the appropriate documentation to the assurance requirements.

Table 18: Assurance Measures Mapping to SARs

Assurance Component	Assurance Measure
ACM_CAP.2	[ACM_CAP.2] Configuration Management Document v0.1
ADO_DEL.1	[ADO_DEL.1] Secure Delivery Procedure Document v0.1
ADO_IGS.1	[ADO_IGS.1] Installation and Setup Procedure Document v0.1
ADV_FSP.1	[ADV_FSP.1] TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence v0.1
ADV_HLD.1	[ADV_HLD.1] TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence v0.1

Assurance Component	Assurance Measure
ADV_RCR.1	[ADV_RCR.1] TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence v0.1
AGD_ADM.1	Administration Guide.pdf (IBM mainframe C:D) Installation Guide.pdf (IBM mainframe C:D) ConsoleOperatorsGuide.pdf (IBM mainframe C:D) Implementation Guide.pdf (IBM mainframe Secure+)
AGD_USR.1	[AGD_USR.1] BUI AdminGuide.pdf (Windows/UNIX/IBM mainframe)
	Release_Notes.pdf UserGuide.pdf (IBM mainframe) OS390_Secure+.pdf (IBM mainframe) SecureOS390RN.pdf (IBM mainframe)
ALC_FLR.2	[ALC_FLR.2] Life Cycle Support: Flaw Remediation v0.1
ATE_COV.1	[ATE_COV.1] Functional Tests and Coverage v0.1
ATE_FUN.1	[ATE_FUN.1] Functional Tests and Coverage v0.1
AVA_SOF.1	[AVA_SOF.1] Vulnerability Assessment v0.1
AVA_VLA.1	[AVA_VLA.1] Vulnerability Assessment v0.1

6.2.1 ACM_CAP.2: Configuration Management Document

The Configuration Management document provides a description of the various tools used to control the configuration items and how they are used internally at Sterling Commerce, Inc. This document provides a complete configuration item list and a unique referencing scheme for each configuration item. Additionally, the configuration management system is described, including procedures that are used by developers to control and

track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

6.2.2 ADO_DEL.1: Delivery and Operation Document

The Delivery and Operation document provides a description of the secure delivery procedures implemented by Sterling Commerce, Inc. to protect against TOE modification during product delivery. The Installation Documentation provided by Sterling Commerce, Inc. details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the TOE Users on configuring the TOE and how they affect the TSF.

6.2.3 ADO_IGS.1: Installation Guidance, AGD_ADM.1: Administrator Guidance, AGD_USR.1: User Guidance

The installation guidance document provides the procedures necessary for the secure installation, generation, and start-up of the TOE for administrators and users of the TOE. The administrator guidance documentation provides detailed procedures for the administration of the TOE and description of the security functions provided by the TOE. The User Guidance documentation provided directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they need to be exercised.

6.2.4 ALC_FLR.2: Flaw reporting procedures

The Sterling Commerce, Inc. Life Cycle documentation deals with establishing discipline and control in developing and maintaining the TOE. Confidence in the correspondence between the TOE security requirements and the TOE is greater if security analysis and the production of the evidence are done on a regular basis as an integral part of the development and maintenance activities. There is a category within Life Cycle claimed for EAL 2 augmented with ALC_FLR.2 assurance level Flaw Reporting Procedures. The corresponding CC Assurance Component is Flaw Remediation.

6.2.5 ADV_FSP.1: Informal Functional Specification, ADV_HLD.1: High Level Design, ADV_RCR.1: Representation Correspondence.

The Sterling Commerce, Inc. design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and error messages for each external TSF interface.
- The High-Level Design provides a top-level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the

basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.

- The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

6.2.6 ATE_COV.1: Test Coverage Analysis, ATE_FUN.1: Functional Testing

There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates that testing is performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested, as well as the level of detail to which the TOE was tested. Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided in order to meet the assurance requirement Functional Testing.

6.2.7 AVA_VLA.1: Vulnerability Analysis, AVA_SOF.1: Strength of Function Analysis

A Vulnerability Analysis is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, this document provides evidence of how the TOE is resistant to obvious attacks. The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements.

7 Protection Profile Claims

No Protection Profile conformance is claimed for this evaluation.

8 Rationale

This section provides the rationale for the selection of the security requirements, objectives, assumptions, and threats. In particular, it shows that the security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the Security Target.

Table 19: Security Objective Mapping

OBJECTIVES / Threats, Organizational Security Policies and Assumptions	O.ADMIN	O.AUDIT	O.VALIDATED_CRYPTO	O.PROTECT	O.BYPASS	O.PRIORITIZE	OE.I&A	OE.TIMESTAMPS	OE.BYPASS	OE.AUDITPROTECT	OE.MANAGE	OE.NOEVIL	OE.PHYSICAL
T.UNAUTH	×	×	×	×	×		×	×	×	×			
T.HOG	×	×			×	×		×	×	×			
P.VALIDATED_CRYPTO.			×										
A.MANAGE											×		
A.NOEVIL												×	
A.PHYSICAL													×

The following table provides descriptions of the mapping between the objectives and threats.

Table 20: Relationship of Security Threats to Objectives

T.UNAUTH **An unauthorized individual may breach the confidentiality or integrity of data transferred between TOEs.**

The threat is removed by the TOE protecting transmitted files from unauthorized reading or modification (O.PROTECT). It does so using cryptographic mechanisms provided by a FIPS 140-2 validated module (O. VALIDATED_CRYPTO).

This removal of the threat is supported by ensuring that the cryptographic protection mechanisms as always applied. This is provided by ensuring that only authorised users access the system (OE.I&A), by ensuring that those users have a secure method of administering the TOE (O.ADMIN) and by ensuring that the security functionality cannot be bypassed, either through the TOE or through the underlying TOE environment (O.BYPASS, OE.BYPASS). These in turn are supported by a robust audit mechanism (O.AUDIT) and (OE.AUDITPROTECT) which allows problems to be detected and corrected. The audit functionality is supported by timestamps provided by the environment (OE.TIMESTAMPS).

T.HOG **A TOE user may prevent high priority tasks from occurring by using too many system resources to process low priority tasks.**

The threat is removed by the TOE ensuring that resources are allocated based on the priority of the task (O.PRIORITIZE).

This removal of the threat is supported by ensuring that this mechanism cannot be bypassed. This is provided by ensuring that users have a secure method of administering the TOE (O.ADMIN) and by ensuring that the security functionality cannot be bypassed, either through the TOE or through the underlying TOE environment (O.BYPASS, OE.BYPASS). These in turn are supported by a robust audit mechanism (O.AUDIT) and (OE.AUDITPROTECT) which allows problems to be detected and corrected. The audit functionality is supported by timestamps provided by the environment (OE.TIMESTAMPS).

P.VALIDATED_CRYPTO **The TOE shall provide cryptographic functions for its own use. These functions will be provided by a FIPS 140-2 validated cryptographic module.**

The TOE shall provide cryptographic functions for its own use. These functions are provided by a FIPS 140-2 validated cryptographic module (O.VALIDATED_CRYPTO).

O.VALIDATED_CRYPTO satisfies this organizational security policy.

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

Those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use.

OE.MANAGE satisfies this assumption.

A.NOEVIL **Administrators are non-hostile, appropriately trained and follow all administrator guidance.**

Sites using the TOE ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.

OE.NOEVIL satisfies this assumption.

A.PHYSICAL **Physical security will be provided for the TOE and its environment.**

Physical security is provided within the domain for the value of the IT resources protected by the operating system and the value of the stored, processed, and transmitted information.

OE.PHYSICAL satisfies this assumption.

8.2 Security Functional Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective. The following table provides the mapping between the SFRs met by the TOE and the Objectives for the TOE.

Table 21: TOE Objective Mapping

	O.ADMIN	O.AUDIT	O.VALIDATED_CRYPTO	O.PROTECT	O.BYPASS	O.PRIORITIZE	OE.I&A	OE.TIMESTAMPS	OE.BYPASS	OE.AUDITPROTECT
FAU_GEN.1		×								
FAU_SAR.1 (a & b)		×								
FAU_SEL.1		×								
FCS_CKM.4			×	×						
FCS_COP.1			×	×						
FDP_ACC.1				×						
FDP_ACF.1				×						
FDP_ITC.1			×	×						
FDP_UCT.1				×						
FDP_UIT.1				×						

Sterling Commerce, Inc.

	O.ADMIN	O.AUDIT	O.VALIDATED_CRYPTO	O.PROTECT	O.BYPASS	O.PRIORITIZE	OE.I&A	OE.TIMESTAMPS	OE.BYPASS	OE.AUDITPROTECT
FMT_MOF.1(a)	×									
FMT_MOF.1(b)	×									
FMT_MSA.1	×									
FMT_MSA.2	×									
FMT_MSA.3	×									
FMT_MTD.1	×									
FMT_SMF.1	×									
FMT_SMR.1	×									
TOE_SEP_(EXP).1					×					
FPT_RVM.1					×					
FRU_PRS.1						×				
FTP_ITC.1				×						
FIA_UID.2							×			
FIA_UAU.2							×			
FTP_STM.1								×		
FTP_SEP.1									×	
FAU_STG.1										×

The following is a table that provides a rationale for the SFRs for the TOE and the IT Environment meeting the Objectives for the TOE and the IT Environment.

Table 22: Security Objective Rationale

O.ADMIN	**The TOE must provide a secure method of administrative control of the TOE, ensuring that TOE users with the appropriate privileges, and only these TOE users, can exercise such control.**

The TOE defines a set of roles (FMT_SMR.1). Only some of those roles are given the right to control the behaviour of the TSF (FMT_MOF.1(a), FMT_MOF.1(b)) and to access TSF data (FMT_MTD.1). These management functions are specified (FMT_SMF.1). The security attributes used by the TOE are secure because the security attributes which can be initialized with default values are initialized with restrictive values (FMT_MSA.3). Further, security attributes can only be changed to secure values (FMT_MSA.2) and can only be changed by authorized users (FMT_MSA.1).

O.AUDIT	**The TOE must provide a robust means of recording security relevant events in sufficient detail to help an administrator of the TOE detect attempted security violations.**

The TOE generates audit records for a wide range of security relevant events in each case recording sufficient information for the audit record to be useful (FAU_GEN.1). These audit records are reviewable by authorized users in a readable format (FAU_SAR.1 a & b). The level of audit information provided is selectable (FAU_SEL.1)

O.VALIDATED_CRYPTO	**The TOE shall provide cryptographic functions for its own use. These functions will be provided by a FIPS 140-2 validated cryptographic module.**

The TOE implements FIPS-approved algorithms in both hardware and software. (FCS_COP.1) The keys are created by the environment and imported to the TOE securely (FDP_ITC.1). Key destruction is implemented in a FIPS-approved manner by a FIPS 140-2 validated cryptographic module (FCS_CKM.4):

- Digital signatures: DSA, RSA.
- DSA key generation.
- RSA key generation.
- Symmetric encryption: DES, 3DES, AES

O.PROTECT	**The TOE must protect transmitted files from unauthorized reading or modification.**

The TOE has an access control policy which ensures that only authorised entities gain access to the transmitted files (FDP_ACC.1, FDP_ACF.1). This policy is enforced by protecting the confidentiality (FDP_UCT.1) and integrity (FDP_UIT.1) of the transmitted files through a trusted channel (FTP_ITC.1). This channel is implemented cryptographically (FCS_COP.1). The keys are created by the environment and imported to the TOE securely (FDP_ITC.1). The keys are destroyed (FCS_CKM.4) in a secure manner.

O.BYPASS	**The TOE must ensure that the TSF cannot be bypassed.**

The TOE maintain a security domain that protects it from interference and tampering (TOE_SEP_(EXP).1) and ensures that enforcement functions are invoked and succeed before each function is allowed to proceed (FPT_RVM.1).

O.PRIORITIZE **The TOE must be able to allocate resources based on the priority of the task.**

The TOE will allocate resources based on the priority of the task (FRU_PRS.1).

OE.I&A **The TOE environment must uniquely identify all users, and will authenticate the claimed identity before granting a user access to the TOE and/or resources protected by the TOE.**

The TOE will not give any access to a user until the TOE environment has identified (FIA_UID.2) and authenticated (FIA_UAU.2) the user.

OE.TIMESTAMPS **The TOE environment must provide reliable timestamps for the use of the TOE.**

The TOE relies on the timestamp that is derived from the operating system. The timestamp is used for audit record labeling and arranging logs in chronological order (FPT_STM.1).

OE.BYPASS **The TOE environment must ensure that the TSF cannot be bypassed.**

The TOE relies on the operating system to maintain a security domain that protects it from interference and tampering (FPT_SEP.1).

OE.AUDITPROTECT **The TOE environment must protect audit files from unauthorized modification or deletion.**

The TOE relies on the environment to protect stored audit records from unauthorized modification or deletion (FAU_STG.1).

8.3 Security Assurance Requirements Rationale

The TOE is designed as a server based software application for file transfer that is protected against eavesdropping, tampering, and message forgery. An assurance level of EAL 2+, structurally tested, was selected as the threat to the system resources and to the internal network security is considered to be unsophisticated attackers. It is felt that an evaluation at this level provides evidence that the TOE functions in a manner consistent with its documentation and that it provides useful protection against the identified threats.

8.4 Explicitly Stated Requirements Rationale

An explicitly stated requirement was created for stating the TSF Domain Separation requirement. The requirement TOE_SEP_(EXP).1 states “The TSF shall explicitly maintain a security domain that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.” This requirement differs from the standard SFR because it is stating that the TOE only protects itself from interference through its own interfaces. The TOE depends on the TOE environment, though the environmental SFR, FPT_SEP.1, to ensure that the TOE is

protected from interference by the operating system in the TOE environment.

This SFR needed to be explicitly stated because there were no requirements in Common Criteria Part 2 which expressed this functionality.

8.5 Dependency Rationale

This ST satisfies all requirement dependencies of the Common Criteria. Table 23 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 23: Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	FPT_STM dependency is met by the TOE environment.
FAU_SAR.1(a) FAU_SAR.1(b)	FAU_GEN.1	✓	
FAU_SEL.1	FAU_GEN.1	✓	
	FMT_MTD.1	✓	
	FMT_MSA.2	✓	
FCS_CKM.4	FDP_ITC.1	✓	
	FMT_MSA.2	✓	
FCS_COP.1	FDP_ITC.1	✓	
	FCS_CKM.4	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_ITC.1	FDP_ACC.1		
	FMT_MSA.3	✓	
FDP_UCT.1	FTP_ITC.1	✓	
	FDP_ACC.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FDP_UIT.1	FTP_ITC.1	✓	
	FDP_ACC.1	✓	
FMT_MOF.1(a) FMT_MOF.1(b)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.2	ADV_SPM.1	✓	Will be met by assurance documentation.
	FDP_ACC.1	✓	
	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No Dependencies		
FMT_SMR.1	FIA_UID.1	✓ (FIA_UID.2)	FIA_UID.2 is hierarchical to FIA_UID.1 and therefore satisfies this dependency. The dependency is met by the TOE environment.
TOE_SEP_(EXP).1	No Dependencies		
FPT_RVM.1	No Dependencies		
FRU_PRS.1	No Dependencies		
FTP_ITC.1	No Dependencies		
Environmental SFRs			
FAU_STG.1	FAU_GEN.1	✓	
FCS_CKM.1	FCS_COP.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FCS_CKM.4	✓	
	FMT_MSA.2	✓	
FPT_SEP.1	No Dependencies		
FPT_STM.1	No Dependencies		
FIA_UID.2	No Dependencies		
FIA_UAU.2	FIA_UAU.1	✓ (FIA_UID.2)	FIA_UID.2 is hierarchical to FIA_UID.1 and therefore satisfies this dependency. The dependency is met by the TOE environment.

8.6 TOE Summary Specification Rationale

This section demonstrates that the combination of the specified IT security functions work together so as to satisfy the TOE security functional requirements.

Table 24: Rationale Mapping between TSF and SFRs

SECURITY FUNCTION	SFR	RATIONALE
Security Audit	FAU_GEN.1 FAU_SAR.1 (a & b) FAU_SEL.1	The TOE logs critical security functions related to user data protection and security management. Audit records are generated by the TOE when users or administrators submit a job or change the configuration. A job request is for an authorized file transfer. Data related to the jobs such as the owner of the job, the status of jobs, and queue position are written into log files by the Stat Manager. Data relating to file transfers are also gathered, such as progress of file transfer, success, and failure. The log files are stored in the TOE environment. *(FAU_GEN.1)* The audit data can be reviewed by an administrator or a user. A user can be restricted by the administrator to have limited or no audit viewing privileges. Audit data about a file transfer operation can be viewed from the IUI, and CLI. Reports can be generated through the IUI, and CLI. Collection of audit can be changed based on the attributes found in Table 10 under section 5.1.1. *(FAU_SAR.1, FAU_SEL.1)*

Cryptographic Support	FCS_COP.1 FDP_ITC.1 FCS_CKM.4 FMT_MSA.2	The TOE performs encryption, decryption, digital signing, digital signature verification, and hashes in accordance with FIPS standards. *(FCS_COP.1)* The The keys are created by the environment and imported to the TOE securely (FDP_ITC.1). The TOE provides key destruction by zeroizing keys in accordance with the Key Zeroization requirements in FIPS 140-2. Key zeroization occurs when keys are no longer needed or valid on the TOE. *(FCS_CKM.4)* The TOE ensures that only secure values are accepted for cryptographic keys. The keys are generated by FIPS validated algorithms. *(FMT_MSA.2*)
User Data Protection	FDP_ACC.1 FDP_ACF.1 FDP_UCT.1 FDP_UIT.1	The TOE provides user data protection by enforcing the *SECURE FILE TRANSFER SFP* on requests for a secure file transfer of files protected by the TOE. *(FDP_ACC.1, FDP_ACF.1)* The secure file transfer is done through the TLS connection. During this operation, sender and receiver compute an HMAC for each file segment transmitted. When hash comparisons fail, and the TOE is the receiving end-point, it will trigger an immediate termination of the file transfer operation and error messages at both ends of the transaction are generated. This mechanism ensures that modification, deletion, insertion, or replay has not occurred on receipt of files. *(FDP_UCT.1, FDP_UIT.1)*

Security Management	FMT_MOF.1 (a) FMT_MOF.1 (b) FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1	The TOE lets a user who possesses the appropriate privileges to perform management functions. All management functionality is allowed only by authorized TOE users. They must authenticate with the TOE operating environment before they can access this TSF. TOE users can take three roles: • Administrative users access the software to configure the system, update network maps, update security parameters, start and stop the system, create new users and assign privileges, submit jobs and monitor all activity on the server, and modify the TOE audit settings. *(FMT_MOF.1(a), FMT_MOF.1(b), FMT_SMF.1*) • Users can submit jobs, monitor, view, and sort audit data related to their own jobs. A user cannot monitor the jobs of another user. The audit viewing feature can be further restricted by an administrator. *(FMT_MDT.1)* • Console operators can access the TOE from a console terminal, perform all the duties of a user, and can shutdown the TOE. *(FMT_SMR.1, FMT_MSA.1)* The TOE's ability to provide restrictive default values which can only be overridden by the administrator to specify alternative initial values is *not-applicable*. *(FMT_MSA.3)*
Protection of TSF	FPT_RVM.1 TOE_SEP_(EXP).1	The functions that enforce the TSP must succeed first before any other function can proceed. No other administrator functions can be performed before identification and authentication of the user is completed. *(FPT_RVM.1)* The TOE maintains different domains of execution enforcing domain separation between human/IT Entity-initiated and TOE-internal processes. *(FPT_SEP_(EXP).1)*
Resource Utilization	FRU_PRS.1	The TOE provides the means to utilize resources when it is operating on objects for file transfer. This is managed through priority and queue position of submitted file transfer jobs. *(FRU_PRS.1)*

Trusted Path/Channel	FTP_ITC.1	The TOE provides the means to establish a trusted path between two C:D SP nodes. The TOE will use TLS to establish the trusted path with a remote C:D SP server. TLS performs mutual authentication and exchanges cryptographic keys as part of the TLS handshake that initiates the secure communication session. The established TLS session is the trusted path that is used to transfer files between the TOE and a remote C:D SP server. *(FTP_ITC.1)*

8.7 TOE Summary Specification Rationale for the Security Assurance Requirements

EAL2 augmented with Flaw Remediation was chosen to provide a basic level of independently assured security in the absence of ready availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment.

The TOE is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. The chosen assurance level was also selected for conformance with the client's needs. See section 6.2 for detailed description of each of the assurance requirements used for development and maintenance of the TOE.

8.8 Strength of Function Rationale

A strength of function rating of SOF-basic is claimed for this TOE to meet the EAL 2+ assurance requirements. This SOF is sufficient to resist the threats identified in Section 3. Section 4 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The evaluated TOE is intended to operate in commercial and DoD low-robustness environments processing unclassified information.

The relevant security functional requirement which has probabilistic or permutational functions is:

FIA_UAU.2 User Authentication before any action

The only mechanism within the TOE Environment that is probabilistic and permutational in nature is the password used to authenticate users to the TOE. The TOE requires that the minimum password length used to authenticate an entity would be equal to or greater than eight characters, containing at least one non-alphanumeric character (from a

set of 33), at least one numeric character (from a set of 10), and at least two alpha characters (from a set of 52, since upper- and lower-case characters are differentiated), for a total character set of 95 characters.

In accordance with annex A.8 in the CEM, the elapsed time of attack results in a strength of function rating exceeding SOF-basic.

9 Acronyms

Table 25: Acronyms

Acronym	Description
API	Applications Programming Interface
BUI	Browser User Interface
C:D	Connect: Direct
CC	Common Criteria
CCS	Canadian Common Criteria Scheme
C:D SP	Connect: Direct with Secure+
CLI	Command Line Interface
EAL	Evaluation Assurance Level
EAL2	Evaluation Assurance Level 2
EAL2+	Evaluation Assurance Level 2 augmented with Flaw Remediation
FIPS	Federal Information Processing Standards
HMAC	Hashed Message Authentication Code
IUI	Interactive User Interface
SARs	Security Assurance Requirements
SFRs	Security Functional Requirements
SSL	Secure Socket Layer
STS	Station to Station
ST	Security Target
TCQ	Transmission Control Queue
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TOE Scope of Control

Acronym	Description
TSF	TOE Security Function
TSP	TOE Security Policy