Connect:Direct Secure+ Option
(3.7 on UNIX, 4.5 on z/OS)

FIPS 140-2 Non-Proprietary Security Policy

Level 1 Validation
Version 1.13

September, 2006

Table of Contents

Introduction

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Connect:Direct Secure+ Option from Sterling Commerce. This Security Policy describes how the Connect:Direct Secure+ Option meets the security requirements of FIPS 140-2 and how to run the modules in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the modules.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/cryptval/.

The Connect:Direct Secure+ Option is referred to in this document as the Connect:Direct, the C:D, the cryptographic modules, the software modules, or the modules.

References

This document deals only with operations and capabilities of the modules in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Sterling Commerce website (http://sterlingcommerce.com/) contains information on the full line of products from Sterling Commerce.
- The CMVP website (http://csrc.ncsl.nist.gov/cryptval/140-1/140val-all.htm) contains contact information for answers to technical or sales-related questions for the module.

Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Sterling Commerce. With the

exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Sterling Commerce and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Sterling Commerce.

CONNECT:DIRECT SECURE+ OPTION

Overview

Sterling Commerce is the world's leading provider of multi-enterprise collaboration solutions for the Global 5000. Their software and services help companies operate more profitably by giving them visibility and control over the processes they share with business and supply chain partners. To protect documents and systems, Sterling Commerce has developed Connect:Direct software. Connect:Direct provides server-based software file-transfer solutions for high-volume applications. Connect:Direct installations typically perform periodic, high-capacity file transfers between specific servers, often for financial services or federal government applications. This software supports multiple server platforms, including mainframe operating systems, UNIX platforms, and Windows servers.

As an addition to the basic Connect:Direct product, the Connect:Direct Secure+ Option allows authentication and encryption to be applied between servers to ensure secure file transfer. With Secure + Option, TLS is used to perform authentication between servers, and provides data encryption for transferring file .

Because Connect: Direct is a peer-to-peer solution, Secure+ must be installed at both end points in order to use its cryptographic features. It is often the case, however, that an organization will require robust security for some files while others may be transferred “in the clear”, either because both end points are within the firewall or because of the nature of the data. In some cases, the remote site may not have Secure+. In other cases, the connection is a private network or leased line, which is secure. Occasionally, the data to be transmitted is such that clear-text transmission across a public network is acceptable. Connect: Direct supports all of these secure and non-secure data exchange scenarios. Figure 1 illustrates various options for deploying Secure+ within an e-business community.

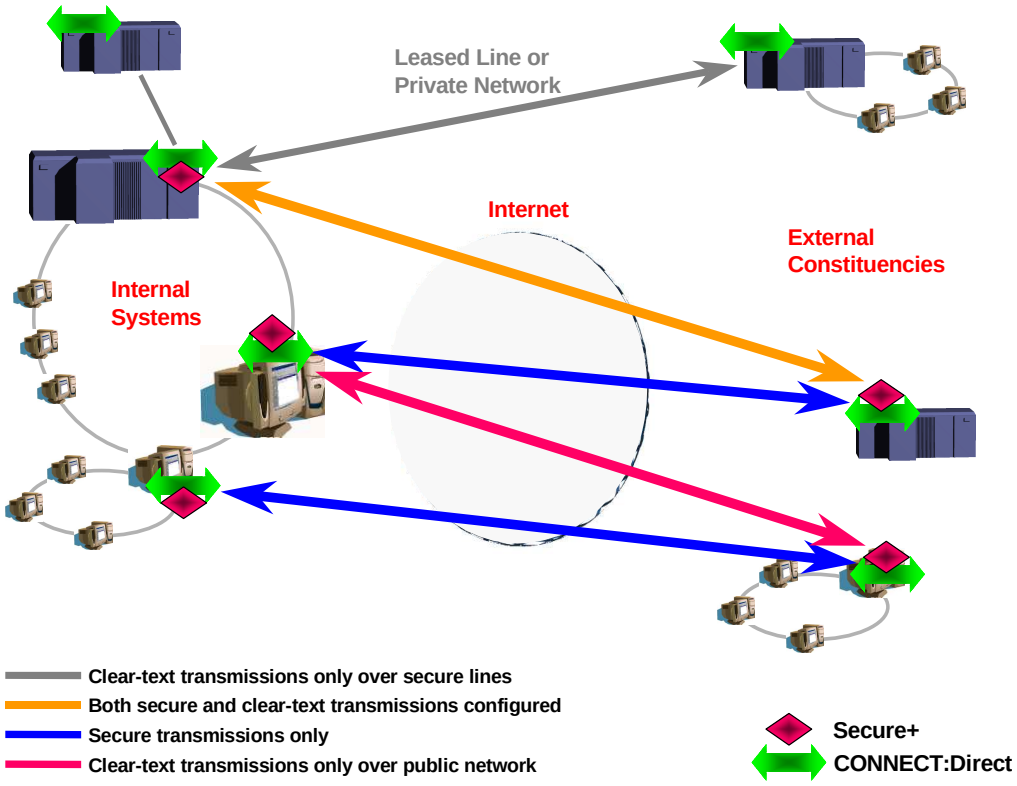

Figure 1 - Deployment Architecture

Module Specifications

The Connect:Direct Secure+ Option modules comprise a set of binaries that are installed on various platforms. For this validation, the modules are tested on UNIX and z/OS platforms. The modules are classified as multi-chip standalone modules that meet overall level 1 FIPS 140-2 requirements.

Section	Section Title	Level (UNIX)	Level (z/OS)
1	Cryptographic Module Specification	1	1
2	Cryptographic Module Ports and Interfaces	1	1
3	Roles, Services, and Authentication	1	1
4	Finite State Model	1	1
5	Physical Security	N/A	1
6	Operational Environment	1	1
7	Cryptographic Key Management	1	1
8	EMI/EMC	1	1
9	Self-Tests	1	1
10	Design Assurance	1	1
11	Mitigation of Other Attacks	N/A	N/A

Table 1 – Security Level Per FIPS 140-2 Section

Logically, the modules comprise software running on UNIX and z/OS machines with TCP/IP connectivity. The C:D is being tested for use on four different OS platforms: three flavors of UNIX and z/OS 1.6. The UNIX operating system variations are: Sun Solaris 10, IBM AIX 5.3, and HP-UX 11i. The logical cryptographic boundary for the modules is shown in Figure 2 below. On z/OS platform, the cryptographic boundary includes IBM eServer zSeries 900 CMOS Cryptographic Coprocessor (certificate #118).

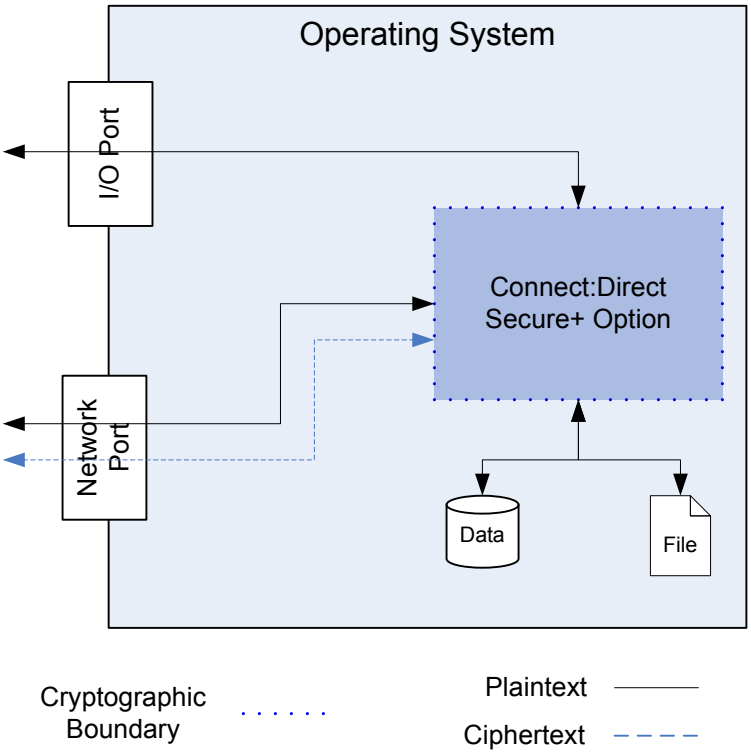

Figure 2 - Logical Cryptographic Boundary

The Security Policy covers two versions of Connect:Direct Secure+ Option: version 3.7 on UNIX running on Sun Solaris 10, IBM AIX 5.3, and HP-UX 11i and version 4.5 on z/OS running on z/OS version 1.6. Standard servers consist of the integrated circuits of the motherboard, the central processing unit (CPU), random access memory (RAM), read only memory (ROM), server case, power supply, and fans. Other devices may be attached to the server, such as a display monitor, keyboard, mouse, floppy disk drive, CD-ROM drive, fixed disk drive, printer, audio adapter, or network adapter. Figure 3 shows the block diagram of a standard server.

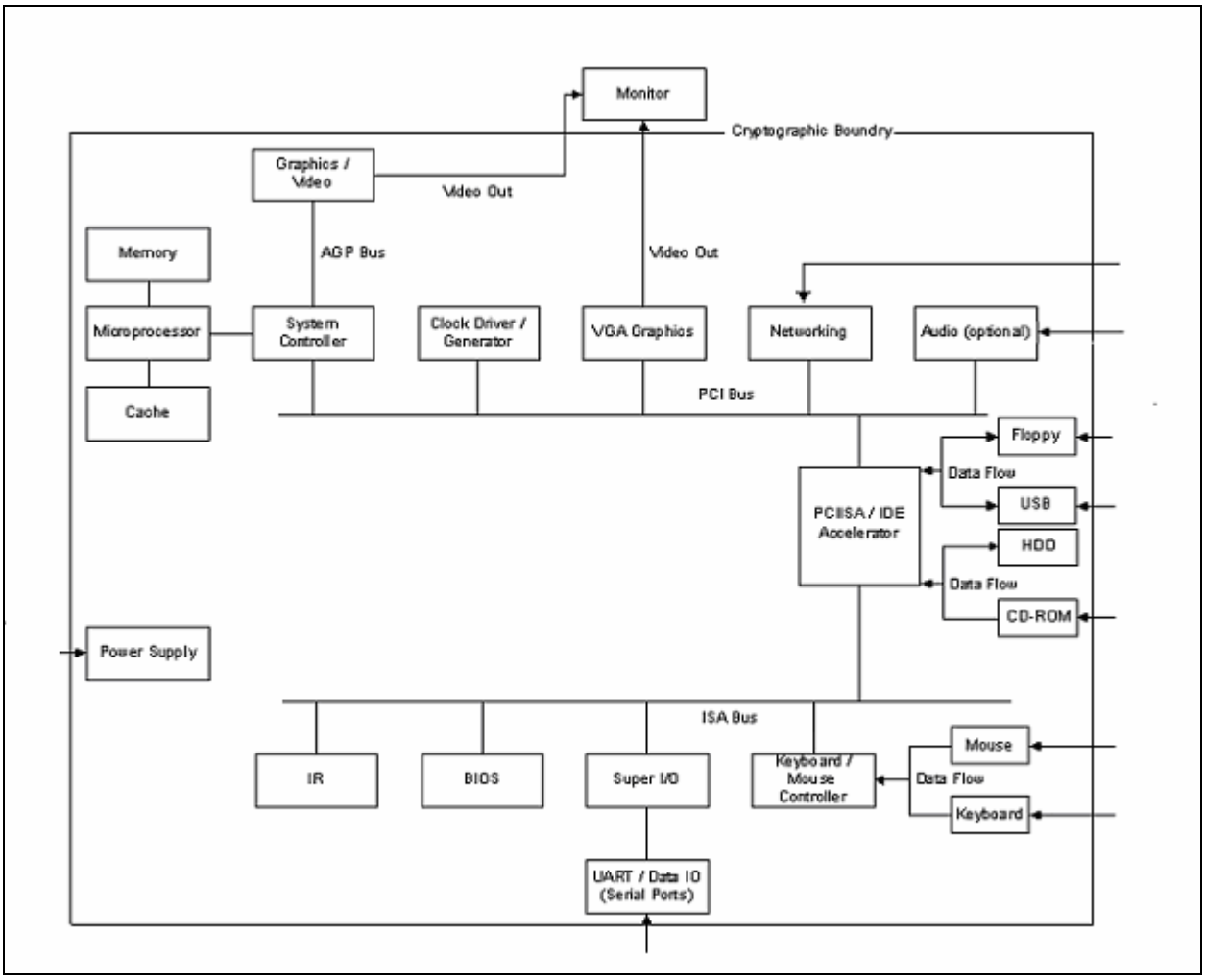

Figure 3 - Standard server Block Diagram

Similar to the standard server, mainframe contains integrated circuits of the motherboard, the central processing unit (CPU), random access memory (RAM), read only memory (ROM), metal case, power supply, and fans. Mainframe can communicate through Ethernet port. A mainframe block diagram is shown in Figure 4. The module utilizes FIPS 140-1 validated IBM Hardware Cryptographic implementation (certificate 118) for TLS service, which is inside the mainframe's enclosure and within the cryptographic boundary. The mainframe's CPU directly communicates with the IBM Hardware module.

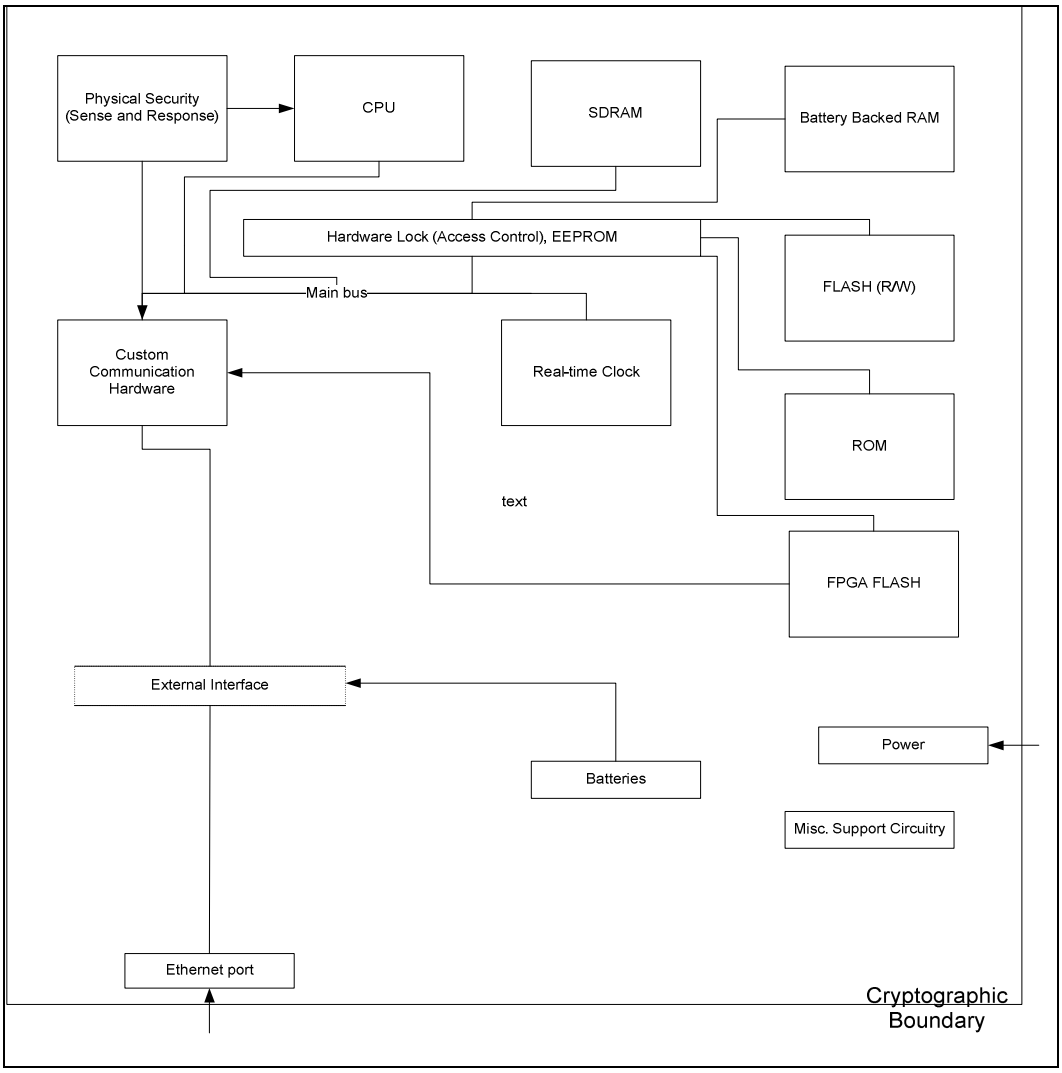

Figure 4 - Standard Mainframe Block Diagram

The physical cryptographic boundaries of the modules are defined by the metal and/or plastic device case, which physically encloses the complete set of hardware and software, including the operating system and the modules.

Module Interfaces

The modules feature the physical ports of the host server or mainframe system, as depicted in Figure 3 and Figure 4, respectively. The modules' manual controls, physical indicators, and physical, logical, and electrical characteristics are those

of the host device and the logical interfaces exist at a low level in the software processes. The modules' design separates its interfaces into four logically distinct and isolated categories. The logical interface is mapped to the following four logical interfaces:

- Data Input
- Data Output
- Control Input
- Status Output

The logical interfaces and their module and physical interface mappings are described in the following table:

Logical Interfaces	Physical Interface Mapping (UNIX server)	Physical Interface Mapping (Mainframe)	Module Mapping
Data Input Interface	Keyboard, CD-ROM, floppy disk, and serial/USB/parallel/network ports	Ethernet port	Transferred file from remote node, API calls that contain data used or processed by the module.
Data Output Interface	Floppy disk, monitor, and serial/USB/parallel/network ports	Ethernet port	File to be transferred, API calls that contain data from the module.
Control Input Interface	Keyboard, CD-ROM, floppy disk, mouse, and serial/USB/parallel/network port	Ethernet port	API calls that are use to maintain operation of the module and configuration files.
Status Output Interface	Floppy disk, monitor, and serial/USB/parallel/network ports	Ethernet port	API calls that show the status of the module and the log files.
Power Interface	Power Interface	Power Interface	Not Applicable

Table 2 - Ports and Interfaces

Control Input Interface lists "Configuration files", which refers to Netmap, Initparm, and Parmfile. The modules identify the remote nodes that the local node is able to communicate with through the use of Network map (Netmap). The Network map includes the names of all the remote nodes that the modules can communicate with, the paths to contact those remote nodes, and characteristics of the sessions for communication. Initialization Parameter file (Initparm) includes initialization parameters for the modules. During start-up, the modules read from this file for configuration and settings. Parameter File (Parmfile) is intended to contain all the parameters that Secure+ Option needs to operate. This file is organized in the same way as the Network Map. Parmfiles store, along with Netmap information, cipher suite to be used to establish TLS session with remote nodes and certificates to authenticate them.

Status of the modules or their activity is journalized in a file, which can be viewed by administrators in multiple ways. This log file forms a large part of the Status Output Interface.

Roles, Services, Authentication

The modules support two operator roles: “Crypto-Officer” and “User.” Operators on the modules must assume one of the roles is implicitly assumed based upon the service performed. No authentication is required. Both of the roles and their responsibilities are described below.

Crypto-Officer Role

The Crypto-Officer installs, uninstalls, configures, and monitors the module’s services using the GUI and command line interfaces (CLI) offered by the modules. The role has administrator rights on a machine to view (monitor) and manage (configure) C:D services or user settings. A separate administrative tool (SPADMIN) is used to enter identifying information about the endpoint server, including TLS public key certificates and encryption options. This role has the highest level of administrative rights. Descriptions of the services available to the Crypto-Officer role are provided in the table below.

Service	Description	Input	Output	Key and CSP	Type of Access to Key and CSP
Installation	Installing the C:D with Secure+	Commands	Result of installation	None	--
Uninstall	Uninstall the module	Commands	Module uninstalled	None	--
Configuration and Management	Configure C:D	Commands and control data input	Module configured or status viewed	Server Authentication Key Server Public Key Client Authentication Key	Read/Write Read/Write Read/Write
SP Configuration and Management	Configure Secure+ Option	Commands and control data input	Secure+ Option configured or status	Access File Key	Read/Write
Viewing Statistics	Shows the status of the module	Commands	Status output	None	--
Schedule file transfers	Send/request files	Commands and file name	File scheduled to be sent or received	None	--
Secure API	TLS Session	TLS packet	Secure channel established over network	Session Key Server Authentication Key Server Public Key Client	Read/Write Read Read

Service	Description	Input	Output	Key and CSP	Type of Access to Key and CSP
				Authentication Key PRNG seed (UNIX)	Read Read/Write
Run Self-Test	Perform the self-test on demand	Command	Self-test performed	None	--

Table 3 – Crypto-Officer Services, Descriptions, and Accessed Keys and CSPs

User Role

The User establishes and utilizes file transfer services over TLS sessions from remote nodes. The user can access the offered services based on the permissions set by the Crypto-Officer. The role does not have administrator rights to view or manage C:D configuration or User settings. Service descriptions and inputs/outputs are listed in the following table:

Service	Description	Input	Output	Key and CSP	Type of Access to Key and CSP
Initiate Secure Session	Performs TLS handshake	TLS handshake packet	Secured session established	Access File Key Session Key Server Authentication Key Server Public Key Client Authentication Key PRNG seed (UNIX)	Read Read/Write Read Read Read Read/Write
Send/Receive Files Securely	Initiate or request file transfer	TLS packet with file	File transmitted	Session Key	Read/Write
Send/Receive Files in plaintext	Initiate or request file transfer in plaintext (alternating bypass mode)	TLS packet with file	File transmitted	None	--

Table 4 – User Services, Descriptions, and Accessed Keys and CSPs

Bypass Mode

The modules support alternating bypass mode, which enables the modules to transfer files in plaintext. Before transitioning to the bypass mode, the Crypto-Officer must configure the Parmfile to allow the plaintext transmission by specifying the NULL cipher. NULL cipher enables the nodes to negotiate a plaintext session. Please see "Configuration and Management" section of this document for more information.

Authentication Mechanisms

The modules do not require an authentication mechanism in order to access its services, although an authentication mechanism may be used. Authentication is not being tested or claimed for this level 1 validation.

The Crypto-Officer can authenticate to the modules using the Operating System during local access. Even if the Operating System performs authentication of operators, the modules do not authenticate the CO role separately when remotely accessed. Rather, the Crypto-Officer and User roles are implicitly selected by virtue of the functions accessed by the operator. The User remotely accessing the modules can be additionally required to authenticate to the modules using digital certificates during TLS session negotiation.

Physical Security

The modules are classified as multi-chip standalone modules. The z/OS version of Connect:Direct Secure+ Option meets Physical Security Level 1 requirements. Physical Security requirements are not applicable to the UNIX version of Connect:Direct Secure+ Option.

For z/OS platform, the module is tested on production-grade mainframes that include a surrounding metal-reinforced plastic and/or metal case. The case of the tested platform entirely surrounds the internals of the Connect:Direct with Secure+ Option cryptographic module.

Operational Environment

The Connect:Direct with Secure+ Option is being tested for FIPS 140-2 Level 1 requirements running on the following operating systems and the corresponding hardware:

- Sun Solaris 10 running on Sun SPARC systems
- IBM AIX 5.3 running on IBM RISC System p5 Server
- HP UX 11i running on HP 9000 series
- z/OS 1.6 running on z900 series

The Connect:Direct with Secure+ Option products are software modules that are run on standard workstations and IBM mainframes. All workstations and IBM mainframes in the US have to meet FCC requirements to be sold. So the machines

have also been FCC approved, and the manufacturer can provide this information if required.

Cryptographic Key Management

The Connect:Direct with Secure+ Option cryptographic modules have multiple cryptographic libraries providing different services to them. On a UNIX platform, the module uses three toolkits and implements the following FIPS-approved algorithms:

i. Certicom Security Builder (SB) 2.0
   - Triple DES - CBC; 1 and 2 keying option; encrypt/decrypt (certificate #423)
   - SHA-1 Byte oriented (certificate #451)

ii. RSA BSAFE Crypto-C 6.2.10
   - DSA (1024 bit key)- sign verification (certificate #164)
   - SHA-1 Byte oriented (certificate #453)

iii. RSA BSAFE SSL-C 2.6.1.0 (uses FIPS validated Crypto-C Cryptographic Module)
   - Triple DES - CBC; 1 and 2 keying option; encrypt/decrypt (certificate #288 and #424)
   - AES - CBC; 128/256 bit key; encrypt/decrypt (certificate #192 and #380)
   - SHA-1 Byte oriented (certificate #272 and #452)
   - HMAC SHA-1 – (certificate #7 and #168)
   - FIPS 186-2 Appendix 3.1 PRNG – (certificate #39 and #182)

The module depends on a couple of toolkits for cryptographic operations on the z/OS operating system.

i. Certicom Security Builder (SB) 2.0
   - Triple DES - CBC; 1 and 2 keying option; encrypt/decrypt (certificate #423)
   - SHA-1 Byte oriented (certificate #451)
   - ECDSA (K-163 curve) – verification (certificate #25)

ii. IBM Hardware Cryptographic implementation
   - Triple DES - CBC; 1 and 2 keying option; encrypt/decrypt (certificate #28)
   - DSA/SHA-1 Byte oriented (certificate #37)

The services that establish the TLS tunnel control the IBM eServer zSeries 900 CMOS Cryptographic Coprocessor (certificate #118).

On a UNIX platform, the module performs the following non-FIPS approved algorithm operations using RSA BSAFE Crypto-C toolkit.

- RSA 1024 bits key encrypt/decrypt (PKCS#1, key wrapping; key establishment methodology provides 80 bits of encryption strength)
- DES
- MD5

These operations are performed on certificates in Parmfiles which are stored encrypted using a PKCS#5 mechanism. For FIPS purposes, these certificates are considered to be stored in plaintext, with no security impact from the use of the non-FIPS-approved algorithms.

The modules support the following critical security parameters:

Key or CSP	Key Type	Generation and Input	Output	Storage and Zerorization	Use
Access File Key	TDES 2 key CBC	Externally generated, entered in plaintext	--	Stored in plaintext in hard disk; zerorized upon deletion of ACF or overwriting	Encrypts and decrypts Parmfiles
Session Key (UNIX)	TDES CBC 2/3 key; AES CBC 128/256 key	Internally generated using FIPS 140-2 validated RSA BSAFE SSL-C 2.6.1.0 library or entered encrypted	Outputted encrypted	Plaintext in volatile memory; ephemeral keys zerorized after the session is over or by power cycle.	Provides confidentiality to secure session data
Session Key (z/OS)	TDES CBC 2/3 key	Externally generated, entered into the volatile memory in plaintext	--	Plaintext in volatile memory; ephemeral keys zerorized after the session is over or by power cycle.	Provides confidentiality to secure session data
Server Authentication Key	RSA 1024 bit private key	Externally generated, entered in plaintext	--	Encrypted in hard drive; zerorized on demand, by uninstalling the module or overwriting	Authenticates during TLS handshake protocol
Server Public Key	RSA 1024 bit public key	Externally generated, entered in plaintext	Outputted in plaintext or encrypted	Encrypted in hard drive; zerorized on demand, by uninstalling the module or overwriting	Authenticates during TLS handshake protocol
Client Authentication Key	RSA 1024 bit public key	Externally generated, entered in plaintext	Outputted in plaintext or encrypted	Encrypted in hard drive; zerorized on demand, by uninstalling the module or overwriting	Authenticates during TLS handshake protocol
PRNG seed (UNIX)	FIPS 186-2 PRNG seed	Internally generated using FIPS 140-2 validated RSA BSAFE SSL-C 2.6.1.0 library	--	Volatile memory in plaintext; zerorized by power cycle	Seeds FIPS approved PRNG on UNIX platform

Table 5 – Listing of Key and Critical Security Parameters

Access Policy

The Crypto-Officer has access to all of the CSPs mentioned in Table 5. User may access all the CSPs.

Self-Tests

The module performs the following Power-up and Conditional self-tests on software cryptographic implementations on the UNIX platform:

Power-up Self-tests:

- Software Integrity Test using DSA signature verification
- Cryptographic Algorithm Tests
  - Triple-DES-CBC (2-key) KAT
  - SHA-1 KAT
- Critical Function Test
  - Asset Protection (AP) Test

Conditional Self-tests:

- Bypass Mode Test

On the UNIX platform following power-up self-tests are performed by embedded FIPS validated cryptographic module:

- AES KAT
- TDES KAT
- SHA-1 KAT
- HMAC SHA-1 KAT
- PRNG KAT
- Software integrity test

The embedded cryptographic toolkit performs the following conditional self-tests:

- Continuous random number generator test for FIPS 186-2 PRNG

The module performs the following Power-up and Conditional self-tests on software cryptographic implementations on the z/OS platform:

Power-up Self-tests:

- Software Integrity Test using ECDSA signature verification
- Cryptographic Algorithm Tests
  - Triple-DES-CBC (2-key) KAT
  - ECDSA sign/verify
- Critical Function Test
  - Asset Protection (AP) Test
  - APF Authorization Test
  - Ensuring availability of critical operating system elements

Conditional Self-tests:

- Bypass Mode Test

The IBM eServer zSeries 900 CMOS Cryptographic Coprocessor (certificate #118) also performs self-tests separately.

The Initparm file includes an initialization parameter, “FIPS”. This parameter has three levels of value defined as NO, WARN, or HALT.

Parameter	Description
NO	FIPS mode of operation is disabled.
WARN	FIPS mode of operation is disabled. However, Self-tests will be performed and warning message is logged if the tests failed.
HALT	FIPS mode of operation is enabled. If Self-test fails to run successfully, the module stops initialization process.

Table 6 - Levels of Initialization Parameter Value

Self-tests would be performed when the parameter is coded as WARN or HALT. In WARN mode the modules may continue to function in non-FIPS mode of operation when any of the self-tests fail and an error message is logged. The Crypto-Officer can review the log file via management interfaces.

Design Assurance

Sterling Commerce uses Concurrent Versioning System (CVS) 1.11.20 for UNIX development and Endevor tool release 4.0 to manipulate source code on z/OS. CVS is a widely used version control system that records the history of source files. It contains a database of files with full modification history. Endevor is an automated Mainframe software configuration management tool from Computer Associates. Endevor is the software tool used by IBM Mainframe development and Level 3 Support to store all the Connect:Direct source code, macros, ISPF panels, messages, etc.

Additionally, Microsoft Visual Source Safe (VSS) version 6.0 is used to provide configuration management for the modules' FIPS documentation. This software provides access control, versioning, and logging.

Mitigation of Other Attacks

The modules do not claim to mitigate other attacks in a FIPS mode of operation.

SECURE OPERATION

The Connect:Direct Secure+ Option meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the modules in FIPS-approved mode of operation.

Initial Setup

Before the modules can be installed, the Crypto-Officer must have a standard server running Solaris, IBM AIX, or HP-UX, or a mainframe running z/OS, configured for single operator mode and disallowing remote login. For mainframe platform, the Crypto-Officer must ensure that the IBM eServer zSeries 900 CMOS Cryptographic Coprocessor is installed and active.

To ensure that Operating System is running in single user mode, the Crypto-Officer must –

- Remove all login accounts except “root”.
- Disable NIS and other named services for users and groups.
- Turn off all remote login, remote command execution, and file transfer daemons.

The specific procedures for each of the UNIX variants and mainframe are described below.

Sun Solaris:

1. Login as the "root" user.
2. Edit the system files /etc/passwd and /etc/shadow and remove all the users except "root" and the pseudo-users (daemon users). Make sure the password fields in /etc/shadow for the pseudo-users are either a star (*) or double exclamation mark (!!). This prevents login as the pseudo-users.

   Also make sure the shell for daemon users is /dev/null, or something else that is not exploitable.
3. Edit the system file /etc/nsswitch.conf and make "files" the only option for "passwd", "group", and "shadow". This disables NIS and other name services for users and groups.
4. Edit the system file /etc/inet/inetd.conf, and comment out all unnecessary services (by prepending a hash ('#') sign to the beginning of each unnecessary service line).
   sadmind - Solstice network administration agent server
   rpc.ttdbserverd - Sun tool-talk server
   kcms_server - Kodak Color Management System server
   fs.auto - Sun font server

cachefsd - NFS cache service
rquotad - remote disk quota server
rpc.metad - Disksuite remote metaset service
rpc.metamhd - Disksuite remote multihost service
rpc.metamedd - Disksuite component service
ocfserv - Smartcard service
dtspcd - Part of the CDE package
rpc.cmsd - remote calendar server
in.comsat - biff, mail notification server
in.talkd - talk server
gssd - RPC application authentication
in.tnamed - deprecated name server
rpc.smserverd - removable media device sensor service (disabling requires manual CD mounting)
dcs - remote dynamic configuration server
ftpd - ye olde FTP server
ktkt_warnd - Kerberos warning server
chargen - deprecated network service
daytime - deprecated network time
time - legacy time service
discard - deprecated network service
echo - network 'echo' service
ufsd - part of RPC
in.uucpd - unix-to-unix copy server

5. Disable service startup scripts within /etc/rc2.d. Many additional services (not bound to inetd) are started by default. To disable startup scripts, files can be renamed to make sure they do not begin with a capital ‘S’ (which denotes Startup). Disable startup scripts that are not pertinent to the setup.
   nscd - NIS-related
   snmpdx - SNMP services
   cachefs.daemon - NFS-caching
   rpc - Remote Procedure Call services
   sendmail - Sendmail
   lp - line printer daemon
   pppd - Point-to-point Protocol services
   uucp - Unix-to-Unix copy daemon
   ldap - LDAP services

   Reboot the system for the changes to take effect.

HP-UX:

1. Log in as the "root" user.
2. Edit the system file /etc/passwd and remove all the users except "root" and the pseudo-users. Make sure the password fields for the pseudo-users are a star (*). This prevents login as the pseudo-users.

3. Edit the system file /etc/nsswitch.conf. Make sure that "files" is the only option for "passwd" and "group". This disables NIS and other name services for users and groups.
4. Edit the system file /etc/inetd.conf. Remove or comment out the lines for remote login, remote command execution, and file transfer daemons such as telnetd, rlogind, remshd, rexecd, ftpd, and tftpd.
5. Reboot the system for the changes to take effect.

IBM AIX:

1. Log in as the "root" user.
2. Edit the system file /etc/passwd and remove all the users except "root" and the pseudo-users. Make sure that for the pseudo-users, either the password fields are a star (*) or the login shell fields are empty. This prevents login as the pseudo-users.
3. Remove all lines that begin with a plus sign (+) or minus sign (-) from /etc/passwd and /etc/group. This disables NIS and other name services for users and groups.
4. Edit the system file /etc/inetd.conf. Remove or comment out the lines for remote login, remote command execution, and file transfer daemons such as telnetd, rlogind, krlogind, rshd, krshd, rexecd, ftpd, and tftpd.
5. Reboot the system for the changes to take effect.

z/OS:

1. The SYS1.PARMLIB member named IEASYSxx that will be used for the IPL must have an entry for CMD that specifies an entry which starts only administrator approved tasks to run Connect:Direct in FIPS mode.
2. The SYS1.PARMLIB member named IEASYSxx that will be used for the IPL must have an entry for MAXUSER that limits the number of possible address spaces to only the count that is specified in the CMD entries.
3. The COMMNDxx member(s) specified in IEASYSxx must start only administrator-approved tasks for operating in FIPS mode. In addition, the DASD device that contains the parmfile/accessfile on other LPAR systems in the complex must be inaccessible. This can be accomplished with a particular system generation configuration, or with VARY commands on each non-FIPS system such that at IPL time the device is made inaccessible.

Secure Delivery

The Crypto-Officer makes a purchase request for the module online. They can request to receive the product via standard delivery services (i.e. Fedex or UPS) or to download directly from vendor's website. To download from the Sterling website, the CO is given user ID and password via email by Sterling. During the download the Crypto-Officer must use the provided user ID and password to authenticate themselves. Downloaded modules include a digital signature to check the integrity of the software, which is checked during power up. The Crypto-Officer should monitor the product download for any irregularity.

The Crypto-Officer may also fill out the Order Fulfillment Process form in order to have the product shipped to them. Sterling ships the module in a sealed box. Upon receipt of the module, the Crypto-Officer must examine the package for evidence of tampering. Tamper-evidence includes tears, scratches, and other irregularities in the packaging.

With the delivered software, the Crypto-Officer also receives a complete documentation library which includes the Getting Started Guide, Release Notes, and Secure+ Implementation Guide.

Crypto-Officer Guidance

The Crypto-Officer is responsible for installation and initialization, configuration, management, and removal of the module.

Installation

Before installing the modules, Crypto-Officer must check that *Initial Setup* has been performed as described above. Installation procedures are described in the Installation Guide that accompanies the module software.

Configuration and Management

The Crypto-Officer should monitor the module's status by regularly checking the Statistics log information. For guidance on configuring and monitoring the modules, please refer to the Secure+ Implementation Guide. If any irregular activity is noticed or the module is consistently having errors, then Sterling Commerce customer support should be contacted. Procedure to maintain the modules in FIPS mode of operation is specified below.

1. The Connect:Direct modules provide numerous configuration options for TLS to ensure its versatility. The TLS channel protocol is stored in the Parmfile, which is created and maintained by the Crypto-Officer via the SPADMIN interface. A TLS transfer logs the following protocol specification into the Statistics file along with the cipher suites that has been used in the session:

   Secure+ Protocol => TLS

To conform to the FIPS 140-2 standard, a secure session must be configured with one of the following cipher suites on mainframe:

i. SSL_RSA_WITH_3DES_EDE_CBC_SHA

On UNIX platform, a secure session must be configured with one of the following cipher suites:

i. TLS_RSA_WITH_AES_256_CBC_SHA
ii. TLS_RSA_WITH_AES_128_CBC_SHA
iii. TLS_RSA_WITH_3DES_EDE_CBC_SHA

Statistics for a plaintext session (Bypass mode) does not specify the protocol specification and associated cipher suite. Only the indication of a created tunnel is mentioned with the message below.

"Secure+ Protocol => TLS"

To activate the plaintext session NULL cipher suite need to be added in the Parmfile instead of "AES_128," "AES_256," or "TDES_EDE" suites for the specific session; and also the remote node needs to be configured with NULL cipher suite, too. The decision of encryption algorithm to use for a TLS connection is made from the cipher suite. Activating a session with NULL cipher suite sets the modules in alternating bypass mode.

2. To maintain the FIPS mode of operation, the Crypto-Officer shall not allow any SSL or STS session to be defined in the Secure+ Parmfile.

3. Also, the CO must check that there are no Netmap entries that are not listed in the Secure+ Parmfile.

4. The FIPS parameter in Initfile must be set to "HALT" level.

5. The Operating System must be set to single user mode to maintain FIPS mode of operation of the modules.

6. For the mainframe platform, the Crypto-Officer must ensure that the IBM eServer zSeries 900 CMOS Cryptographic Coprocessor is installed and active.

7. Crypto-Officer should check Statistics log file regularly for self-test status. The following table contains status indicator messages that are logged for each self-tests performed by the modules.

Platform	Self-Test Occurrence	Status	Indicator Message
UNIX	Power-up	Success	msgid=XFST002I subst=FIPS Software Integrity Test Successful
			msgid=XFST011I subst=FIPS Self Test Successful
		Failure	msgid=XFST003E subst=FIPS Software Integrity Test Failed
			msgid=XFST012E subst=FIPS Self Test Failed
	Conditional	Failure	msgid=CSPA202E stext=SSL handshake failure, reason=<reason code>
z/OS	Power-up	Success	SITA903I FIPS Self-test Operation successful.

Platform	Self-Test Occurrence	Status	Indicator Message
		Failure	SITA904E FIPS Self-test Operation failed.
	Conditional	Failure	msgid=CSPA202E stext=SSL handshake failure, reason=<reason code>

Table 7 - Self-Test Status Indicator Messages

There is no separate success status message for Conditional self-tests. Establishing a TLS connection indicates that Conditional self-test passed.

User Guidance

Users access the module's file transfer functionality as a remote node, however remote login is not permitted. Although the User does not have any ability to modify the configuration of the modules, care should be taken not to provide authentication information and access codes to other parties.

ACRONYMS

AES	Advanced Encryption Standard
APF	Authorized Program Facility
API	Application Programming Interface
CBC	Cipher Block Chaining
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CSP	Critical Security Parameter
CVS	Concurrent Versioning System
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
ECDSA	Ecliptic Curve DSA
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
HMAC	(Keyed-) Hash MAC
IP	Internet Protocol
ISPF	Interactive System Productivity Facility
KAT	Known Answer Test
MAC	Message Authentication Code
MD5	Message Digest Algorithm 5
NIST	National Institute of Standards and Technology
OS	Operating System
PKCS	Public-Key Cryptography Standard
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
STS	Station To Station (custom protocol)
TCP	Transmission Control Protocol
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
VSS	Visual Source Safe

