Certification Report

EAL 2+ Evaluation of Sterling Commerce Inc.,

Connect:Direct® with Secure+ Option

v4.5 on IBM OS/390 and z/OS

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-48a-CR
Version: 1.0
Date: 3 October 2006
Pagination: i to v, 1 to 10

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, have been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment (CSE), or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the CSE, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment (CSE).

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is Electronic Warfare Associates-Canada, Ltd. located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 3 October 2006, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at: http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html

This certification report makes reference to the following trademarked names:

- Connect:Direct and Secure+ are either trademarks or registered trademarks of Sterling Commerce Incorporated in the United States and other countries; and
- IBM is registered trademark of IBM Corporation in the United States and other countries.

TABLE OF CONTENTS

Executive Summary

The Connect:Direct® with Secure+ Option v4.5 on IBM OS/390 and z/OS, from Sterling Commerce Incorporated, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

Connect:Direct® with Secure+ Option is a software application that enables secure peer-to-peer file transfer over a non-secure network. The Connect:Direct® with Secure+ Option provides server-based software file transfer solutions for high volume applications. Connect:Direct® with Secure+ Option installations perform periodic high capacity file transfers between specific servers. 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.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 18 September 2006, and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for the Connect:Direct with Secure+ Option, the security requirements, and the level of confidence (evaluation assurance level) to which the product is intended to satisfy the security requirements. Consumers of the Connect:Direct with Secure+ Option are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product indicate that it meets the EAL 2+ assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 2.3 August 2005* (with applicable final interpretations), for conformance to the *Common Criteria for IT Security Evaluation, version 2.3 August 2005*. The following augmentation is claimed:

- ALC_FLR.2 - Flaw Reporting Procedures.

The Communications Security Establishment, as the CCS Certification Body, declares that the Connect:Direct® with Secure+ Option v4.5 on IBM OS/390 and z/OS evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list.

[1] The evaluation technical report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2+ evaluation is the Connect:Direct® with Secure+ Option v4.5 on IBM OS/390 and z/OS, from Sterling Commerce Incorporated.

2 TOE Description

Connect:Direct® with Secure+ Option is a software application that enables secure peer-to-peer file transfer over a non-secure network. The Connect:Direct® with Secure+ Option provides server-based software file transfer solutions for high volume applications. Connect:Direct® with Secure+ Option installations perform periodic high capacity file transfers between specific servers. 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.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the Connect:Direct® with Secure+ Option is identified in Section 5 of the ST.

The TOE performs encryption, decryption, digital signing, digital signature verification, and hashes in accordance with FIPS standards. The keys are created by the environment and imported to the TOE securely. The TOE ensures that only secure values are accepted for cryptographic keys. The TOE provides key destruction by zeroizing keys in accordance with the Key Zeroization requirements in FIPS 140-2. TOE cryptographic functionality is provided using the following algorithms:

Cryptographic Algorithm	Key Size	Standard	Certificate Numbers
Digital Signature Algorithm (DSA)	1024	FIPS 186-2	129, 130, 131
Rivest, Shamir, Adleman (RSA)	1024, 2048	PKCS#1	55, 56
Triple DES (ECB, CBC modes)	168	FIPS 46-3	319, 320, 321, 322, 323, 325, 326
Advanced Encryption Algorithm (AES) (ECB, CBD modes)	128, 192, 256	FIPS 917	229, 230, 231, 232, 233, 234, 235

Secure Hash 1 (SHA-1)	N/A	FIPS 180-2	308, 309, 310, 311, 312, 313, 314
Hashed Message Authentication Code (HMAC) with SHA-1	160	FIPS 198	41, 42, 44, 45

4 Security Target

The ST associated with this Certification Report (CR) is identified by the following nomenclature:

Title: Sterling Commerce Inc., Connect:Direct® with Secure+ Option v4.5 on IBM OS/390 and z/OS Security Target
Version: 0.1
Date: 5 September 2006

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 2.3 August 2005*, for conformance to the *Common Criteria for IT Security Evaluation, version 2.3 August 2005*. The Connect:Direct with Secure+ Option v4.5 on IBM OS/390 and z/OS is:

a) Common Criteria Part 2 extended, with security functional requirements based upon functional components from Part 2 except for one explicitly stated requirement TOE_SEP_(EXP).1;
b) Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and
c) Common Criteria EAL 2 augmented, containing all security assurance requirements from EAL 2, as well as ALC_FLR.2.

6 Security Policy

The Connect:Direct® with Secure+ Option implements a secure file transfer policy that governs the transfer of files between instances of the TOE. File transfers are allowed or disallowed based upon whether the user requesting the transfer is able to establish a valid connection (login) with both nodes involved in the transfer, and has the appropriate read/write access permissions for the files involved in the transfer. Connect:Direct® with Secure+ Option security policy detail can be found in Section 5.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the Connect:Direct® with Secure+ Option should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the Connect:Direct® with Secure+ Option.

7.1 Secure Usage Assumptions

There are one or more competent individuals assigned to manage the Connect:Direct® with Secure+ Option and the security of the information that it contains.

Administrators of the Connect:Direct® with Secure+ Option are non-hostile, appropriately trained and follow all relevant guidance instructions.

7.2 Environmental Assumptions

Physical security is provided for the Connect:Direct® with Secure+ Option and the server on which it resides.

7.3 Clarification of Scope

The Connect:Direct® with Secure+ Option provides a level of protection that is appropriate for an assumed non-hostile and well-managed user community. It is designed to protect its user community against inadvertent or casual attempts to breach system security, by attackers possessing a low attack potential. It is not intended for situations in which determined attempts by hostile and well-funded attackers use sophisticated attacks from within the physical zone.

8 Architectural Information

The Connect:Direct® with Secure+ Option is a software application comprising several subsystems.

The primary subsystem, the Process Manager (PMGR), listens for both local (client) file transfer requests and remote file transfer requests.

When a client request is received, the PMGR spawns the Client Manager (CMGR). The CMGR services the request, and enters the request into the Transport Control Queue (TCQ). The PMGR monitors the TCQ, and when the client request reaches the top of the TCQ, the PMGR spawns the Session Manager (SMGR) to perform the file transfer.

As mentioned, the PMGR also listens for incoming sessions from remote nodes. When an incoming request from a remote node is received, the PMGR spawns the SMGR to handle the file transfer.

If a file transfer is to be performed securely, the SMGR invokes the Crypto Module Subsystem that provides encryption and decryption services.

Each of the subsystems send relevant audit information to the Statistics Manager subsystem that writes the audit information to the audit log.

A separate stand-alone system called the Secure+ Admin Tool is used by administrators to configure the parameters used by the subsystems for the secure transfer of files.

9 Evaluated Configuration

The evaluated configuration for the Connect:Direct® with Secure+ Option comprises:

- Connect:Direct® with Secure+ Option v4.5 on IBM OS/390 and z/OS.

10 Documentation

The documents provided to the consumer are:

- Connect:Direct OS/390 Installation Guide, Version 4.5, First Edition;
- Connect:Direct OS/390 Administration Guide, Version 4.5, First Edition; and
- Connect:Direct Secure+ Option OS/390 Implementation Guide, Version 4.5, First Edition.

These documents also apply to z/OS.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the Connect:Direct® with Secure+ Option, including the following areas:

Configuration management: An analysis of the Connect:Direct® with Secure+ Option development environment and associated documentation was performed. The evaluators found that the Connect:Direct® with Secure+ Option configuration items were clearly marked, and could be modified and controlled. The use of the configuration management systems was observed during a site visit, and was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the

Connect:Direct® with Secure+ Option during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the Connect:Direct® with Secure+ Option functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the Connect:Direct® with Secure+ Option user and administrator guidance documentation and determined that they sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators carefully reviewed the flaw remediation process and the evidence generated by adherence to the process. The evaluators concluded that adequate procedures are in place to track and correct security flaws, and distribute the flaw information and corrections.

Vulnerability assessment: The Connect:Direct® with Secure+ Option strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the Connect:Direct® with Secure+ Option and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing independent penetration tests.

12.1 Assessing Developer Tests

The evaluators verified that the developer had met their testing responsibilities by reviewing the developer's test plan, test approach, test procedure and test results, and examining their test evidence, as documented in the Evaluation Technical Report (ETR)[2].

The evaluators analyzed the developer's test coverage analysis, and found that the correspondence between tests identified in the developer's test documentation and the functional specification was complete and accurate.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The tests focused on:

- Audit;
- User data protection;
- Security management; and
- Resource utilization.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis and the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. Penetration testing did not uncover any exploitable vulnerabilities for the Connect:Direct® with Secure+ Option in the anticipated operating environment.

12.4 Conduct of Testing

The Connect:Direct® with Secure+ Option was subjected to a comprehensive suite of formally documented, independent functional tests. The testing took place both at the

[2] The Evaluation Technical Report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

Developer's site in Irving, Texas, USA and at the Information Technology Security Evaluation and Test (ITSET) Facility at Electronic Warfare Associates-Canada The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in the ETR.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the Connect:Direct® with Secure+ Option behaves as specified in its ST and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 2+** level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

Documentation for the Connect:Direct® with Secure+ Option product includes comprehensive platform specific Installation Guides for the secure configuration of the product.

The Connect:Direct® with Secure+ Option is straightforward to configure, use and integrate into a network.

15 Glossary

This section expands any acronyms, abbreviations and initializations used in this report

Acronym/Abbreviation/Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCRA	Common Criteria Recognition Arrangement
CCS	Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CMGR	Client Manager
CR	Certification Report
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ISO	International Organisation for Standardisation

IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
PMGR	Process Manager
SMGR	Session Manager
ST	Security Target
TCQ	Transport Control Queue
TOE	Target of Evaluation
TLS	Transport Layer Security

16 References

This section lists all documentation used as source material for this report:

a) Common Criteria for Information Technology Security Evaluation, CCIMB-2005-08-001/002/003, Version 2.3 August 2005.

b) Common Methodology for Information Technology Security Evaluation, CCIMB-2005-08-004, Version 2.3 August 2005.

c) CCS #4: Technical Oversight for TOE Evaluation, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 1.0, 3 October 2002.

d) Sterling Commerce, Inc., Connect:Direct® with Secure+ Option v4.5 on IBM OS/390 and z/OS, Security Target, Document Version 0.1, 5 September 2006.

e) Evaluation Technical Report (ETR), Sterling Commerce Incorporated Connect:Direct® with Secure+ Option, v4.5 on IBM OS/390 and z/OS, EAL 2+ Evaluation, Document Number 1525-001-D002, Version 1.0, 18 September 2006.