Certification Report

EAL 2+ Evaluation of Sterling Commerce Gentran Integration Suite v4.2

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-53-CR
Version: 1.0
Date: 15 May 2007
Pagination: i to iv, 1 to 11

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, applies 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.

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 EWA-Canada 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 15 May 2007, 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 and on the official Common Criteria Program website at http://www.commoncriteriaportal.org

This certification report makes reference to the following trademarked names:

- Gentran Integration Suite (GIS) which is a registered trademark of Sterling Commerce Incorporated;
- Security Builder which is a registered trademark of Certicom Incorporated; and
- Solaris and SPARC which are registered trademarks of Sun Microsystems Incorporated.

TABLE OF CONTENTS

Executive Summary

The Gentran Integration Suite, v4.2, from Sterling Commerce Incorporated, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

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

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

EWA-Canada is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 15 May 2007, 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 GIS, 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 GIS 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 provide sufficient evidence that it meets the EAL 2 augmented assurance requirements for the evaluated security functionality. 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 following augmentations are claimed:

[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.

ALC_FLR.1 – Basic Flaw Remediation

The Communications Security Establishment, as the CCS Certification Body, declares that the Gentran Integration Suite v4.2 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 (CPL) at http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and on the official International Common Criteria Program website at http://www.commoncriteriaportal.org.

.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2+ evaluation is the Gentran Integration Suite, v4.2, from Sterling Commerce.

2 TOE Description

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

- tie together applications, processes, data and people, both within and outside the organization;
- offer flexible options for deployment, configuration and customization, including the ability to add capabilities one at a time;
- include innovative visual management tools for easy configuration and visibility into work flows, system and trading partner activity, translation maps, and business process implementation; and
- work with existing and emerging business and communication standards.

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

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the GIS is identified in Section 5 of the Security Target (ST).

As part of the CC evaluation effort, the evaluators made use of the results generated under the Cryptographic Module Validation Program (CMVP). Refer to section 5 of the ST for a complete list of the cryptographic algorithms employed by the TOE.

4 Security Target

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

Title:	Sterling Commerce, Inc., Gentran Integration Suite v4.2, Security Target
Version:	0.7
Date:	22 January 2007

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 Gentran Integration Suite v4.2 is:

a) Common Criteria Part 2 conformant, with security functional requirements based only upon functional components in Part 2;

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, with all the security assurance requirements in the EAL 2 package, as well as the following:

ALC_FLR.1 – Basic Flaw Remediation

6 Security Policy

The TOE implements a classic discretionary access control policy (called the GIS Access Control Security Functional Policy) whereby the access of users to objects (data files) controlled by the TOE is based upon access permissions on the objects granted either to the users individually or to groups of which the user is a member.

In addition, the TOE implements an information flow control policy (called the Adapter Security Functional Policy) which uses the concept of a Trading Partner to determine whether or not a business process transaction is allowed to proceed. An administrator of the TOE defines specific business partners for the TOE. Security parameters for the business partner determine the type of authentication required, the transaction types which are permitted and the permitted transaction protocols. An information flow request to the TOE with parameters which match the required security parameters for one of the TOE's business partners is allowed to proceed.

7 Assumptions and Clarification of Scope

Consumers of the GIS should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will help to ensure the proper and secure operation of the product.

7.1 Secure Usage Assumptions

The following Secure Usage assumptions are listed in the ST:

- Administrators of the underlying operating system are also administrators of the TOE; and

- Administrators of the TOE are non-hostile, appropriately trained and follow all relevant guidance instructions.

7.2 Environmental Assumptions

The following Environmental assumptions are listed in the ST:

- The database used by the TOE is installed on the same server as the TOE itself and is not used for any other purpose but support of the TOE;
- There are no general purpose computing capabilities hosted on the server which hosts the TOE;
- The TOE is physically located in a secure area which protects it from unauthorized physical access;
- The TOE and any remote management consoles used for the TOE are located on a private network protected by a firewall; and
- Information flows between internal and external business partners must pass through the TOE.

7.3 Clarification of Scope

The GIS provides a level of protection that is appropriate for low robustness environments processing unclassified information. It offers protection against inadvertent or casual attempts to breach system security, by unsophisticated attackers possessing a low attack potential. It is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Architectural Information

The core of the GIS product is the Integration Broker subsystem which determines authorization, destination, and services needed for each information exchange. The GIS product includes multiple adapters to enable information exchanges with the Integration Broker. Adapters provide an interface for sending information using GIS-supported communication protocols.

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

profile is a record which describes the parameters of a contract made with a trading partner. The profile contains identity information about the trading partner, including a unique identifier, name, address, telephone, and other related information. It also contains information about protocols available to the trading partner, including the protocol type. A trading partner profile may contain other information such as destination information such as IP addresses, URLs and port numbers. For the FTP, HTTP, and Connect:Direct Server adapters, a user name and password are also supplied. The profile also describes the business processes a trading partner is allowed to use. The message or data (payload) may provide other specific instructions as to what should be done with the data When an input adapter receives data from a B2B system, the Integration Broker locates the appropriate business process or processes to call, and starts the process or delivers the incoming data to the appropriate already-running process.

The data translation and manipulation services provided by the Integration Broker are complex and as such GIS also includes a tool called the Graphical Process Modeler to aid an administrator in defining these services. The Graphical Process Modeler is used to define business process models which in turn define how the GIS Integration Broker executes the activities in a business process. Creating business process models for the system to follow is the central operational activity required for configuration and administration of the product. The Graphical Process Modeler is a tool that enables creation of business process models using drag-and-drop technology. The modeler depicts the services included in business process models using icons.

9 Evaluated Configuration

The evaluated configuration of the TOE consists of the Gentran Integration Suite v4.2, along with a MySQL v4.0.18 database and the Certicom Security Builder FIPS Java Module v2.0, all of which are hosted on a SUN Solaris 10 / SPARC 32 server/operating system.

10 Documentation

The documentation set for the GIS product consists of several hundred electronic documents all of which are provided to the customer. For the purposes of this evaluation the documents listed below were relevant:

- Checklist - System Performance and Tuning v4.2, GIS42_Checklist_Tuning.pdf
- Gentran Integration Suite - Digital Certificates v4.2, GIS42_Certificates.pdf
- Gentran Integration Suite - Encryption Method v4.2, GIS42_Encryption.pdf
- Gentran Integration Suite - Implementing SSL v4.2, GIS42_SSL.pdf
- Gentran Integration Suite - Installation Guide v4.2, GIS42_Installation.pdf
- Gentran Integration Suite - Managing Services and Adapters v4.2, GIS42_ManagingServicesAdapters.pdf
- Gentran Integration Suite - Overview Guide v4.2, GIS42_OverviewGuide_NoCover.pdf

- Gentran Integration Suite - Performance and Tuning Guide v4.2, GIS42_Performance_and_Tuning.pdf
- Gentran Integration Suite - Perimeter Server Guide v4.2, GIS42_Perimeter_Server.pdf
- Gentran Integration Suite - Resource Management Guide v4.2, GIS42_ManagingResources.pdf
- Gentran Integration Suite - Role-Based Security v4.2, GIS42_RoleBasedSecuirty.pdf
- Gentran Integration Suite - System Administration Guide v4.2, GIS42_SystemAdministration.pdf
- Gentran Integration Suite - System Requirements v4.2, GIS42_SystemRequirements.pdf
- Gentran Integration Suite - Upgrade Guide v4.2, GIS42_Upgrade.pdf
- Issues and Resolutions for Gentran Integration Suite Version 4.2, GIS42_ReleaseNotes.pdf
- Setup Checklist - Gentran Integration Suite Implementation v4.2, GIS42_Checklist_GIS_Implementation.pdf
- Setup Checklist - UNIX or Linux Preinstallation v4.2, GIS42_Checklist_UNIX_Preinstall.pdf
- Setup Checklist - Windows Preinstallation v4.2, GIS42_Checklist_Windows_Preinstall.pdf

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the GIS, including the following areas:

Configuration management: An analysis of the GIS development environment and associated documentation was performed. The evaluators found that the GIS configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it 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 GIS 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 GIS 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 GIS user and administrator guidance documentation and determined that it 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 reviewed the flaw remediation procedures used by Sterling Commerce for the GIS. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability assessment: The strength of function claims in the ST were validated through independent evaluator analysis. The evaluators also validated the developer's vulnerability analysis. In addition, the evaluators performed an independent vulnerability analysis and developed tests that focused on potential vulnerabilities in the GIS.

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.

[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.

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;
- Identification and authentication; and
- Security management.

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. The penetration tests focused on:

- Bypass attempts;
- Tampering;
- Direct Attacks; and
- Generic Vulnerabilities.

The evaluator conducted a port scan of the GIS server and perimeter server. Only the ports listed in the installation instructions were found to be open. The evaluator used a publicly available tool to scan the GIS server for generic vulnerabilities, and none were found. The evaluator also used a publicly available packet capture tool to examine output from the GIS server during startup, shutdown and normal operations. The evaluator searched the captured results in an attempt to extract information which might be useful to a potential attacker; no useful information was uncovered. In addition, the evaluator performed direct attacks on the GIS server, attempting to bypass or break the TOE's role-based security mechanisms.

The independent penetration testing did not uncover any exploitable vulnerabilities for the GIS in the anticipated operating environment.

12.4 Conduct of Testing

The GIS was subjected to a comprehensive suite of formally-documented, independent, functional and penetration tests. The testing took place at the ITSET facility at EWA-Canada located in Ottawa, Ontario. 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 independent functional tests yielded the expected results, giving assurance that the GIS behaves as specified in its ST and functional specification. The penetration testing resulted in a **PASS** verdict, as the evaluators were unable to exploit any of the identified potential vulnerabilities in the GIS in its intended operating environment.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 2+ level of assurance, including the augmentations identified in Section 5 of this report. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The Gentran Integration Suite v4.2 is a large and complex software product. Much of the product's complexity derives from the large number of adapters which are available to accommodate a large variety of business processes and protocols. Despite the product complexity, the evaluators found the product documentation to be well-written and easy to understand. The high quality of the documentation was complemented by a knowledgeable and highly responsive customer support organization.

15 Glossary

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

15.1 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/Initialization	Description
B2B	Business to Business
CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation
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
CMVP	Cryptographic Module Validation Program
CR	Certification Report
CSE	Communications Security Establishment

EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GIS	Gentran Integration Suite
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
JVM	Java Virtual Machine
PALCAN	Program for the Accreditation of Laboratories Canada
ST	Security Target
TOE	Target of Evaluation

16 References

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

a) Common Criteria for Information Technology Security Evaluation, CCIMB-2004-01-001/002/003, Version 2.3, August 2005

b) Common Methodology for Information Technology Security Evaluation, CCIMB-2004-01-004, Part 2: Evaluation and Methodology, 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.