Certification Report

EAL 2+ Evaluation of SecureLogix Corporation®

ETM® (Enterprise Telephony Management) System

Version 5.0.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-38
Version: 1.0
Date: 04 November 2005
Pagination: i to iv, 1 to 15

DISCLAIMER

The Information Technology (IT) product identified in this certification report has been evaluated using the *Common Methodology for Information Technology Security Evaluation, Version 2.2 r256*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.2 r256*. The evaluation was conducted by an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS). 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 04 November 2005, 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/en/services/common_criteria/trusted_products. html

This certification report makes reference to the following trademarked names: Windows NT®, Windows XP®, Windows 2000®, and Windows Server 2003® which are registered trademarks of Microsoft® Corporation; ETM®, SecureLogix®, and SecureLogix Corporation® are registered trademarks of SecureLogix Corporation in the U.S.A. and other countries; and Solaris® which is a registered trademark of Sun Microsystems Inc.

TABLE OF CONTENTS

Executive Summary

The ETM® (Enterprise Telephony Management) System, Version 5.0.1, from SecureLogix Corporation, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) EAL 2+ evaluation.

The ETM® System is designed to protect telecommunications lines from abuse and provide extensive auditing capabilities on all telecommunications line traffic. The ETM® System acts as a traffic firewall to protect internal telecommunication resources (telephones, modems, faxes, etc.) from abuse, fraud, and attack. The system is capable of operating in conjunction with a Private Branch Exchange, but is not required to do so. The system can encrypt network communications between components using Triple DES cryptography.

Electronic Warfare Associates-Canada, Ltd. is the CCEF that conducted the evaluation. This evaluation was completed in October 2005 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 ETM® System Version 5.0.1, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in 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[1] for this product provide sufficient evidence that it meets the EAL EAL 2+ assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.2 r256* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.2 r256*. The following augmentations are claimed:

a. ACM_CAP.3 – Configuration management authorization controls;
b. ACM_SCP.1 – TOE configuration management coverage; and
c. ALC_DVS.1 – Identification of security measures.

CSE, as the CCS Certification Body, declares that the ETM® System Version 5.0.1 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) EAL 2+ evaluation is the ETM® (Enterprise Telephony Management) System Version 5.0.1, from SecureLogix Corporation.

This report pertains to the TOE, which is comprised of the following main components:
1. ETM® System Software;
2. ETM® System Applications;
3. ETM® Platform Appliances; and
4. Windows/Solaris Operating System.

2 TOE Description

The ETM® System is an enterprise voice firewall, a class of technology that protects voice services much like data firewalls protect data networks. The ETM® System protects the backdoors into data networks created by poorly secured voice networks. The ETM® System addresses vulnerabilities associated with TDM (Time Division Multiplexing) voice networks and addresses many of the challenges inherent in introducing VoIP technologies. The ETM® System also provides enterprise wide visibility into telecom resource utilization, phone network usage, abusive and costly calling patterns, and incidence of toll fraud. The ETM® System can manage both Voice over Internet Protocol (VoIP) and TDM traffic simultaneously, enabling enterprise voice networks to be managed by a common ETM® Platform.

The ETM® System is designed to protect telecommunications lines from abuse and provide extensive auditing capabilities on all telecommunications line traffic. The ETM® System acts as a voice traffic firewall to protect internal telecommunication resources (telephones, modems, faxes, etc.) from abuse, fraud, and attack. The system is capable of operating in conjunction with a Private Branch Exchange (PBX), but is not required to do so.

The ETM® System mediates access between local telecommunication users and external telecommunication users based on rules defined by the administrator. Rule sets are created on the ETM® Management Server, which are then pushed to the appliances. The appliances allow or deny calls based on their respective rule sets.

The ETM® System provides the same type of visibility and control over the use of the telephone network that traditional firewalls provide for Transmission Control Protocol/ Internet Protocol (TCP/IP) networks. It physically interfaces with each telephone voice or data line in the enterprise and enforces a user-defined security policy based on calling number, called number, time of day, call direction (inbound, outbound), call duration, and call type (voice, fax, modem, modem energy, STU III, busy, unanswered, data, or undetermined). The ETM® System also provides an enterprise with the ability to counter the threat of unauthorized access to the data network through user-connected modems.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the ETM® System Version 5.0.1 is identified in Section 5 of the Security Target (ST).

4 Security Target

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

Title: Security Target for the SecureLogix Corporation® ETM®
(Enterprise Telephony Management) System, Version 5.0.1
Version: v1.1
Date: 11 October 2005

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.2 r256*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.2 r256*.

The ETM® System Version 5.0.1 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, containing all security assurance requirements from EAL 2, as well as the following:
   - ACM_CAP.3 – Configuration management authorization controls;
   - ACM_SCP.1 – TOE configuration management coverage; and
   - ALC_DVS.1 – Identification of security measures.

6 Security Policy

The TOE Security Policy is comprised of the TELCO, NETWORK, FILE and CRYPTO Security Function Policies (SFPs) that define the rules by which the TOE governs access to its telecommunication, network, and file resources, and the export/import of cryptographic keys respectively.

6.1 Telecommunications SFP (TELCO_SFP)

The ETM® System is required to mediate access between local and external telephony users based on rules defined by the administrator. Rule sets are created on the ETM® Management

Server, then pushed down to the appliances. The appliances are required to allow or deny calls based on their respective rule sets.

The default telecommunications information flow security policy for ETM® System telecommunications users is "telecommunications that are not explicitly denied, are allowed". The rule set is traversed from top to bottom, triggering on the first applicable rule. A default rule, which cannot be removed, exists at the top of the rule set to always allow calls to emergency services (e.g. 911).

There is a capability for access control to an Authorisation, Authentication, and Accounting (AAA) appliance based on user ID and PIN.

Rule-based policies to identify, monitor, and control telecom network usage, access, security, and costs include:

a. Voice firewall application policies, used to monitor and control individual VoIP and TDM calls according to defined call criteria; and

b. Voice IPS (Intrusion Prevention System) application policies, used to identify and control calling patterns that might indicate toll fraud, war dialing attempts, misuse of resources, and other undesired events. IPS policies monitor and protect telecom resources against calling patterns over time, according to the criteria specified and thresholds set.

A recording policy consists of a set of rules that define specific calls to be recorded. Calls can be identified for recording by any combination of call direction, called and/or calling phone numbers, call time, and call type. When a call matches both a rule in a recording policy and a rule in a firewall or IPS policy, the action field of the IPS or firewall policy determines the outcome of the call.

6.2 Network SFP (NETWORK_SFP)

User ID, password, source IP address, cryptographic algorithm and cryptographic key phrase are used as security attributes to enforce the NETWORK_SFP. Administrators are authenticated to the TOE using user ID/password enforcing access control. There are information flow control restrictions on client-to-server, appliance-to-server and appliance-to-appliance network communications. This is accomplished by validating the IP address, username and password, by authenticating communications with a variable handshake and by encrypting the data with a valid cryptographic key.

6.3 File Access SFP (FILE_SFP)

Only one administrator can be granted access to edit an object at a time. Access to the TOE objects (i.e., data in the database) is controlled by user accounts that restrict who is allowed to access the system and which features they are permitted to modify. User permissions

provide granular control of the features available to users and limit displayed features to those for which a user has permissions.

6.4 Cryptographic SFP (CRYPTO_SFP)

The import of pass phrases is restricted to authorised administrators and processes. Pass phrases are manually entered by authorized administrators through the ETM® System Console, overwriting any existing pass phrases.

The TOE can encrypt network communications between components using Triple DES cryptography. Cryptographic keys are entered directly into the cryptographic modules.

7 Assumptions and Clarification of Scope

Consumers of the ETM® System Version 5.0.1 product 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 TOE.

7.1 Secure Usage Assumptions

For the purposes of this evaluation, the ETM® System administrators are assumed to be trusted and to understand the correct usage of the system within the context of TCP/IP networking and telecommunications systems. The ETM® System must be installed and configured using the guidance specified in the SecureLogix® document entitled *ETM® System Installation Guide*.

7.2 Environmental Assumptions

The following assumptions are made about the operating environment of the TOE:

a. the components of the ETM® System Version 5.0.1 are located within controlled access facilities that will prevent unauthorized physical access;

b. administrators are non-hostile and do not attempt to compromise the TOE functionality; and

c. communications between the management server and the database server are protected by the environment.

For more information about the TOE security environment, refer to Section 3 of the ST.

7.3 Clarification of Scope

The administrator responsible for the TOE must ensure that the TOE is delivered, installed, configured, administered, and operated in a manner that maintains its security by following proper security procedures. Compromise of the integrity and/or availability of the TOE may

occur as a result of an administrator not following proper security procedures or unwittingly introducing malicious code (e.g., virus, Trojan horse) into the system.

The product should be operated within the intended operating environment as specified in the ST and guidance documentation.

In order to ensure that the ETM® System properly enforces the security policy without leaving vulnerabilities due to rule set processing logic, it is important that administrators carefully read and understand the applicable administrative guidance information published by SecureLogix Corporation.

8 Architectural Information

The TOE is comprised of the following subsystems:

1. ETM® System Software;
2. ETM® Platform Appliances;
3. ETM® Client Interface; and
4. Operating System.

The ETM® System Software includes:

1. ETM® System Console v5.0.1, Build 011;
2. ETM® Management Server v5.0.1, Build 011;
3. ETM® Report Server v5.0.1, Build 011;
4. ETM® Database v5.0.1, Build 011;
5. ETM® Call Recorder v5.0.1, Build 011; and
6. Collection Server v2.0, Build 011;

The ETM® Platform Appliances fall into 2 categories:

1. ETM® communications appliances:
   (a) ETM® Model 1010-Analog Appliance version 5.0.54 with 12 lines;
   (b) ETM® Model 1012-Hybrid Analog & VoIP Appliance version 5.0.54 with 12 lines;
   (c) ETM® Model 1024-Hybrid Analog & VoIP Appliance version 5.0.54 with 24 lines;
   (d) ETM® Model 1090-Hybrid Digital & VoIP Appliance version 5.0.54 (supporting 1 Span configurable for T1 CAS, T1 PRI, Euro (E1) CAS, E1 PRI, SS7, or VoIP);

(e) ETM® Model 2100-Digitial Appliance version 5.0.54 (supporting 4 Spans configurable for T1 CAS, T1 PRI, E1 CAS, E1 PRI, or SS7); and

(f) ETM® Model 3200-Digital Appliance version 5.0.54 (supporting 16 Spans configurable for T1 CAS, T1 PRI, E1 CAS, E1 PRI, or SS7).

2. ETM® application appliances:

   (a) ETM® Model 1050-AAA Services Appliance version 5.0.54 with 2 IVR ports; and

   (b) ETM® Model 1060-Call Caching Appliance version 5.0.54 for call recording.

Interfaces to the ETM® System include:

1. Graphical User Interface – Infrastructure Manager (Console) I/O;
2. ASCII window (ETM® System Commands) I/O;
3. Telnet[2] (ETM® System Commands) I/O; and
4. RS-232 serial (ETM® System Commands) I/O.

The ETM® System Software and ETM® System Applications run on Windows® NT 4 SP6a, Windows® 2000 SP4, Windows server 2003® SP1, and Solaris™ 7/8 as the operating systems. The ETM® System Console and ETM® System Applications also run on Windows® XP SP2. These operating systems are included in the TOE.

The administrator uses the ETM® System Console to communicate with the ETM® Management Server, and through it, to communicate with an appliance. The administrator may also directly communicate to an appliance through a Telnet server or a serial port on the appliance.

The ETM® System Components (ETM® Platform Appliances, ETM® System Software, and ETM® System Applications) can be distributed across an Ethernet network. ETM® Management Servers maintain a file of approved Appliance IP addresses and a file of approved remote ETM® System Console IP addresses and only allow communications from these addresses.

The Performance Manager, running within an ETM® System Console, allows the administrator to manage one or more ETM® Systems using graphical windows. The administrator can configure appliances by creating a configuration file on the ETM® Management Server that, in turn, gets pushed to the appliances.

[2] Optional remote admin method - Telnet is only allowed when appliance security level is set to LOW.

SecureLogix Corporation has added an extensive set of appliance command line instructions called ETM® System Commands. The ETM® System Command set can be accessed through a Telnet connection, an ASCII command line window opened in the ETM® System Console, or an RS-232 serial (console) link. However, a small subset of the ETM® System Commands can only be performed locally at the appliance through the serial link.

The AAA Services Appliance is used by a user to temporarily enable an ETM® Communications Appliance rule allowing a specific voice/data circuit to be enabled. The telecom user is required to enter a user ID, PIN and destination telephone number to be called.

The ETM® Call Recorder also adds functionality to the ETM® Communications Appliances (1012, 1024, 1090, 2100 & 3200) allowing them to record calls into temporary storage. The ETM® Communications Appliances forward the recorded calls to a Call Caching Appliance. The Call Caching Appliance then forwards the recorded calls to a Collection Server where the calls are stored on disk. The Collection Server can be installed on the same system as an ETM® Management Server or on a separate system.

Audit records concerning telecommunication information flow and appliance status are generated at the ETM® Communication Appliances and are uploaded to the ETM® Management Server. Each appliance, except the AAA Appliance, contains a memory card that can store the audit records temporarily if the ETM® Management Server is unavailable.

The system can encrypt communications between components using Triple DES cryptography. The ETM® System implementations of Triple DES are based on the specifications of FIPS 46-3 and ANSI X9.52-1998 and have been awarded certificate numbers 373, 374, and 375 on the Triple DES Validated Implementations list. Assessment of the cryptographic algorithm implementations does not form part of the CC evaluation but is separately validated under the Cryptographic Module Validation Program.

Most of the data produced during the operation of the ETM® System is stored in the ETM® Database, which is part of the ETM® Management Server. The ETM® Database supports both Oracle® 8i and 9i Database Management Systems (DBMS) on both Windows® and Solaris™. The DBMS used for the ETM® Database can be installed on the same system as an ETM® Management Server or on a separate system.

9 Evaluated Configuration

The evaluated configuration for the ETM® System v5.0.1 consists of:

ETM® Communications/ Application Appliance Package Version 5.0.54:

a. ETM® Communications/ Application Linux 2.6 operating system.

b. ETM® Management Server Build 11;

c. ETM® Report Server Build 11;

d. ETM® Collection Server, Version 2.0-011;

e. ETM® System Console, Build 11:

f. Java® Virtual Machine software, version 1.4.2_03 on both the ETM® Management Server and the ETM® System Console hosts;

g. ETM® Database Oracle RDBMS for the ETM® Database, one of the following versions: Oracle 8i, version 8.1.7.4 and Oracle 9i, version 9.2.0.6; and

h. Supported operating systems: Windows® NT 4 SP6a, Windows® 2000 SP4, Windows Server 2003® SP1, Windows® XP SP2 (console only), and Solaris™ 7/8.

10 Documentation

The complete documentation for the ETM® System consists of a set of printed guides and in-depth, context-sensitive online Help. The SecureLogix® documents provided to the consumer are as follows:

a. document set: DOC-ETM412-2004-015, consisting of:

- ETM® System User Guide;
- ETM® System Installation Guide;
- ETM® System Technical Reference;
- Voice Firewall User Guide;
- Voice IPS User Guide;
- Usage Manager User Guide;
- ETM® System Administration and Maintenance Guide;
- ETM® Database Schema; and

- ETM® Safety and Regulatory Compliance Information.

b. Knowledge Base Article #ETM991 ETM® (Enterprise Telephony Management) System v5.0.1 Release Notes; and

c. Other Knowledge Base Articles available from SecureLogix® Support Services.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the ETM® System Version 5.0.1, including the following areas:

Configuration management: An analysis of the ETM® System Version 5.0.1 development environment and associated documentation was performed. The evaluators found that the ETM® System Version 5.0.1 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 ETM® System Version 5.0.1 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 ETM® System Version 5.0.1 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 ETM® System Version 5.0.1 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 assessed the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the ETM® System Version 5.0.1 design and implementation.

Vulnerability assessment: The ETM® System Version 5.0.1 ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the ETM® System Version 5.0.1 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. Penetration testing was conducted by evaluators, which did not expose any residual vulnerabilities that would be exploitable in the intended operating environment for the TOE.

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

12 ITS Product Testing

Testing (coverage, functional tests, independent testing): The evaluators examined the developer's testing activities and verified that the developer has met their testing responsibilities.

12.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Technical Report (ETR)[3].

SecureLogix employs a rigorous testing cycle process that tests the changes and fixes in each release of the ETM® System. Certification Acceptance Test procedures are also carried out at the start of each test cycle. Comprehensive regression testing is conducted for all releases.

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

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. Resulting from this test coverage approach was the following list of EWA-Canada test goals:

a. Security Policy Execution;

b. Access Control testing;

[3] 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.

c. Events, Reports and Usage Manager testing;

d. VOIP testing;

e. Call Recording;

f. Telecom Anomaly Detection;

g. Penetration testing; and

h. AAA testing.

Evaluator testing (executing a sample of the developer's test cases) was carried out on 22-28 July 2005 in San Antonio, Texas on ETM® System v5.0.1.

Independent evaluator tests (functional) were conducted using the ETM® System Demo Unit at the EWA-Canada's Information Technology Security Evaluation and Testing (ITSET) Facility, Ottawa, Ontario.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis, limited independent evaluator penetration testing was conducted. This testing confirmed that no exploitable vulnerabilities exist for the TOE given the anticipated, restrictive operating environment for the TOE, and the high level of sophistication and specialized tools that would be required to exploit any of the residual vulnerabilities identified by the developer.

12.4 Conduct of Testing

The ETM® System Version 5.0.1 was subjected to a comprehensive suite of formally documented, independent functional tests. The testing took place at the SecureLogix Corporation facility in San Antonio Texas, and the ITSET facility at Electronic Warfare Associates-Canada, Ltd. 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 and in a separate Test Results document.

12.5 Testing Results

The developer’s tests and the independent functional tests yielded the expected results, giving assurance that the ETM® System Version 5.0.1 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

The complete documentation for the ETM® System Version 5.0.1 includes comprehensive Installation and User Guides.

The ETM® System Version 5.0.1 is straightforward to configure, use and integrate into a corporate network.

The ETM® System Version 5.0.1 graphical user interface provided by the ETM® System Console is intuitive and easy to use.

SecureLogix Corporation Configuration Management (CM) and Quality Assurance (QA) provide the requisite controls for managing all CM/QA activities.

15 Glossary

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

15.1 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/Initialization	Description
AAA	Authorisation, Authentication, and Accounting
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CM	Configuration Management
CSE	Communications Security Establishment
DBMS	Database Management System
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ETM®	Enterprise Telephony Management
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
IP	Internet Protocol
IPS	Intrusion Prevention System
ISDN	Integrated Services Digital Network
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
JRE	Java Runtime Environment
PBX	Private Branch Exchange
PIN	Personal Identification Number
PRI	Primary Rate Interface
QA	Quality Assurance
SS7	Signaling System 7
SFP	Security Function Policy
ST	Security Target
TCP/IP	Transmission Control Protocol/ Internet Protocol
TDM	Time Division Multiplexing
TOE	Target of Evaluation
VOIP	Voice Over Internet Protocol

References

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

a. Common Criteria for Information Technology Security Evaluation, Version 2.2 r256, January 2004, CCIMB-2004-01-001/002/003.

b. Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.2 r256, January 2004, CEM-2004-01-004.

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

d. Security Target for the SecureLogix Corporation® ETM® (Enterprise Telephony Management) System, Version 5.0.1, 1495-011-D001, Version v1.1, 11 October 2005; and

e. Evaluation Technical Report (ETR) SecureLogix Corporation® ETM® (Enterprise Telephony Management) System V5.0.1, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-38, Document No. 1495-000-D002, Version 1.1, 18 October 2005.