Certification Report

EAL 2+ Evaluation of SecureLogix Corporation® ETM® (Enterprise Telephony Management) System

Version 4.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number:	383-4-23
Version:	1.0
Date:	31 March 2004
Pagination:	i to iv, 1 to 16

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has 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 1.0*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.1*. 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 31 March 2004, 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, TeleAudit, TeleWall, TeleView, TeleVPN, SecureLogix, and SecureLogix Corporation which are trademarks or registered trademarks of SecureLogix Corporation; and Solaris® which is a registered trademark of Sun Microsystems Inc.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

The ETM® (Enterprise Telephony Management) System, Version 4.1, from SecureLogix Corporation, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (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 Data Encryption Standard (DES) or Triple DES cryptography. A TeleVPN® Call Shield option is available for the T1 and Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) versions of the ETM® Communication Appliances. This option allows the ETM® System to encrypt selected telecommunications channels using Triple DES cryptography.

Electronic Warfare Associates-Canada, Ltd. is the CCEF that conducted the evaluation. This evaluation was completed on 23 March 2004, 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 v4.1, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the ETM® System v4.1 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[1] for this product provide sufficient evidence that it meets the EAL 2+ assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 1.0* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.1*. The following augmentations are claimed:

a. ACM_CAP.3 – Configuration management authorization controls;

b. ACM_SCP.1 – TOE configuration management coverage; and

[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.

c. ALC_DVS.1 – Identification of security measures.

CSE, as the CCS Certification Body, declares that the ETM® System v4.1 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 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2+ evaluation is the ETM® System v4.1, from SecureLogix Corporation.

This report pertains to the TOE, which is comprised of the following main components:

a. ETM® Communication Appliances;

b. ETM® Management Server;

c. TeleAudit® Server;

d. Windows/Solaris Operating System; and

e. ETM® System Console.

2 TOE Description

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 ETM® System is also designed to protect telecommunications traffic from being disclosed by creating encrypted tunnels through the public switched telephone network (PSTN). 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 default behaviour is to allow calls that are not explicitly denied. Whether or not a call is encrypted is also enforced by the rules created on the ETM® Management Server. The default behaviour is that calls are not encrypted.

A TeleVPN® Call Shield option is available for the T1 and ISDN PRI versions of the ETM® Communication Appliances. This option allows the ETM® System to encrypt selected telecommunications channels using Triple DES cryptography.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the ETM® System v4.1 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 4.1
Version: v1.5
Date: 23 March 2004

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.1*, incorporating all final interpretations issued prior to 21 July 2003. The ETM® System v4.1 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 govern 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. Rulesets 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 rulesets. Whether or not a call is encrypted will also be enforced by the rules created on the ETM® Management Server.

The default telephony 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 one of the ETM® Communication Appliances, an AAA (Authorization, Authentication, and Accounting) appliance, based on security attributes of user ID and PIN. The AAA appliance can be used to temporarily and dynamically allow a specific voice/data circuit to be enabled based on user ID, PIN and destination telephone number to be called.

6.2 Network SFP (NETWORK_SFP)

User ID, password, source IP address, cryptographic algorithm and cryptographic key 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 valid a cryptographic key and algorithm.

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.

6.4 Cryptographic SFP (CRYPTO_SFP)

The export/import of cryptographic keys is restricted to authorised administrators and processes. The TOE applies encryption to telecommunications channels based on: call direction (inbound or outbound), call source and call destination. The TOE encrypts telecommunications using Triple DES cryptography. TeleVPN® Call Shield enabled ETM® Communication Appliances make use of RSA public/private key pairs to ensure the secure distribution of Triple DES session keys. The appliances exchange the RSA public keys during call setup. Session keys are generated by the TOE and are overwritten when no longer required.

The TOE can also encrypt network communications between components using DES or Triple DES cryptography. Cryptographic keys are manually entered by authorized administrators through the ETM® System Console, overwriting any existing keys.

7 Assumptions and Clarification of Scope

Consumers of the ETM® System v4.1 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 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 Transmission Control Protocol/ Internet Protocol (TCP/IP) networking and telecommunications systems. The ETM® System must be installed and configured using the guidance specified in the SecureLogix® document entitled *Installing the ETM® System v4.1*.

7.2 Environmental Assumptions

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

a. the components of the ETM® System v4.1 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. logical and physical protection must be provided for the communications between the management server and the database server.

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

8 Architectural Information

The ETM® System is a telecommunications firewall that provides the same type of visibility and control over the use of the telephone network that traditional firewalls provide for 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 is also designed to provide an enterprise with the ability to counter the threat of unauthorized access to the data network through user-connected modems.

Ethernet network links are used to implement communication channels between:

a. the appliances and the ETM® Management Server;

b. the TeleView® Infrastructure Manager (Console) and the ETM® Management Server; and

c. the administrator and appliances.

The administrator uses the ETM® System Console to communicate with the ETM® Management Server, and through it, 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 major components of the TOE consist of:

a. ETM® Communication Appliance subsystem, consisting of:

- Authorisation, Authentication, and Accounting (AAA) Appliance;
- Analog Appliance;
- T1 Appliance;
- ISDN-PRI Appliance;
- E1 Appliance;
- SS7 Appliance; and
- TeleVPN® Call Shield option (only available for T1 and ISDN-PRI 2100/3200-series Appliances).

b. ETM® Management Server Subsystem, consisting of:

- Audit Reports; and
- Appliance Manager/Security Policy Editor.

c. TeleAudit® Server

d. Supported operating systems:

- Windows® NT 4 SP6a;
- Windows® 2000 SP3 or SP4;
- Windows Server 2003;
- Windows® XP SP1 (console only); and
- Solaris™ 7/8.

e. ETM® System Console (Client Interface) Subsystem:

- Graphical User Interface – TeleView® Infrastructure Manager (Console) I/O;

- ASCII window (ETM® System Commands) I/O;

- Telnet[2] (ETM® System Commands) I/O; and

- RS-232 serial (ETM® System Commands) I/O.

9 Evaluated Configuration

The evaluated configuration for the ETM® System v4.1 consists of:

a. the ETM® Management Server Build 31;

b. the TeleAudit® Server Build 31;

c. the administrator ETM® System Console Build 31;

d. Java® Virtual Machine software, version 1.4.1_05 on both the ETM® Management Server and the ETM® System Console hosts;

e. ETM® 1000-series (ETM 1010) Appliance version 4.1.22 configured for Analog Services;

f. ETM® 1000-series (ETM 1020) Appliance version 4.1.22 configured for T1 Services;

g. ETM® 1000-series (ETM 1030) Appliance version 4.1.22 configured for North American ISDN PRI Services;

h. ETM® 1000-series (ETM 1040) Appliance version 4.1.22 configured for Euro (E1) ISDN PRI Services;

i. ETM® 1000-series (ETM 1050) Appliance version 4.1.22 configured for AAA Services;

j. ETM® 2100-series Appliance version 4.1.22 configured for T1 and/or North American ISDN PRI/SS7 Spans, or Euro (E1) ISDN PRI Spans and with optional TeleVPN® Call Shield module v1.0; and

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

k. ETM® 3200-series Appliance version 4.1.22 configured for T1 and/or North American ISDN PRI/SS7 Spans, or Euro (E1) ISDN PRI Spans and with optional TeleVPN® Call Shield module v1.0.

The ETM® Management Server, TeleAudit® Server, and ETM® System Console run on Windows® NT 4 SP6a, Windows® 2000 SP3 or SP4, Windows Server 2003, and Solaris™ 7/8 as the operating systems. The ETM® System Console also runs on Windows® XP SP1.

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:

- Installing the ETM® System v4.1;
- Using the ETM® System v4.1;
- Using the TeleAudit® Usage Manager v4.1;
- Using the TeleView® Infrastructure Manager v4.1;
- Using the TeleWall® Telecom Firewall v4.1;
- Using the TeleVPN® Call Shield v1.0;
- ETM® System v4.1 Technical Reference; and
- SecureLogix Published Schema Version 4.1.

b. ETM® (Enterprise Telephony Management) System v4.1, Release Notes; and

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

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the ETM® System v4.1, including the following areas:

Configuration management: An analysis of the ETM® System v4.1 development environment and associated documentation was performed. The evaluators found that the ETM® System v4.1 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 v4.1 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 v4.1 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 v4.1 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 v4.1 design and implementation.

Vulnerability assessment: The ETM® System v4.1 ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the ETM® System v4.1 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. Limited penetration testing was conducted by evaluators, which exposed a residual vulnerability that is not exploitable in the intended operating environment for the TOE.

Domain protection assessment: The evaluators also conducted an analysis of the Windows® and Solaris operating systems component of the TOE, as detailed in section 8, and determined that these operating systems will provide the required protected domain for the ETM® System (i.e.; ETM® Management Server, TeleAudit® Server and ETM® System Console components)

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. ETM® System Installation Procedures testing;

b. Security Policy Execution;

c. Access Control testing;

d. Reports and TeleAudit® Usage Manager testing;

e. AAA 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.

f. TeleVPN® Call Shield testing;

g. Signalling System 7 (SS7) testing;

h. Verification of Observation Reports (ORs) and SecureLogix Test Track Error Reports; and

i. Supplemental (Regression) testing.

Evaluator testing was carried out on 10-18 November 2003 in San Antonio, Texas on ETM® System release software v4.1-build 21, appliance build 4.1.19.

As a result of an updated product build, regression tests were conducted using the ETM® System Demo Unit with v4.1-build 31 system software and appliance build 4.1.22. The regression testing was conducted 24 Feb - 10 March 2004 at the EWA-Canada's Information Technology Security Evaluation and Testing (ITSET) Facility, Ottawa, Ontario.

The test philosophy for the regression testing was to use digital simulation test capabilities to test the TeleVPN® Call Shield capabilities of the v4.1-build 31 system software and appliance build 4.1.22 configuration of the product for the model 2100 ISDN-PRI appliance and to test the basic security functionality of the ETM® System with the management server and clients installed on Windows® platforms. Testing was completed to verify that none of the changes in the product affected the results of the evaluator testing conducted in November 2003 on a previous version of the ETM® System and that the product functioned as claimed in the functional specification.

A Regression Evaluation Test Procedures and Test Results document was developed by EWA-Canada.

Regression testing involved:

a. Security Policy Execution;

b. Access Control testing;

c. Reports and TeleAudit® Usage Manager testing; and

d. TeleVPN® Call Shield testing.

In addition to the regular suite of testing discussed above, additional analysis and tests were conducted to verify the correct operation of the cryptographic functionality provided by the ETM® System v4.1.

Cryptographic Operation (Network Communications)

The implementations of both the DES and Triple DES algorithms used in securing the network communications between ETM® System components have been previously validated. As part of the Common Criteria evaluation effort, the evaluator made use of the results generated under the Cryptographic Module Validation Program (CMVP). The cryptographic algorithms tested under the CMVP are:

a. Data Encryption Standard (DES), FIPS 46-3 CMVP Certificates #149 & #150; and

b. Triple-DES, FIPS 46-3 CMVP Certificates #89 and #90.

<u>Cryptographic Operation (Telephony Communications)</u>

The implementation of Triple DES cryptography in the TeleVPN® Call Shield has been previously validated. As part of the Common Criteria evaluation effort, the evaluator made use of the results generated under the CMVP. The cryptographic algorithm tested under the CMVP is Triple-DES, FIPS 46-3 CMVP Certificate #32.

The following Government of Canada approved algorithms were evaluated for correct implementation in the ETM® System v4.1 TeleVPN® Call Shield Version 1.0:

a. the RSAES-PKCS-v1_5 (1024-bit); and

b. ANSI X9.31: 1998-compliant Random Number Generator (RNG).

To verify the RSA implementation, test vectors were supplied by the Certification Body (CB) and were provided by EWA-Canada to SecureLogix Corporation for known-answer testing of the RSA Encryption (key wrapping) capability of the RSA engine within the TeleVPN® Call Shield Version 1.0. Output results were returned by SecureLogix Corporation, and found to match known correct results provided by CSE.

Statistical testing was also carried out by EWA-Canada on sample data from the X9.31-compliant RNG within the TeleVPN® Call Shield Version 1.0. This testing confirmed that the data produced by the TeleVPN® Call Shield v1.0 RNG is considered sufficiently random for the generation of cryptographic key material.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis and test activities, limited independent evaluator penetration testing was conducted. Penetration testing did not uncover any exploitable vulnerabilities for the TOE in the anticipated, restrictive operating environment.

12.4 Conduct of Testing

The ETM® System v4.1 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.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the ETM® System v4.1 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 v4.1 includes comprehensive Installation and User Guides.

The ETM® System v4.1 is straightforward to configure, use and integrate into a corporate network.

The ETM® System v4.1 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	Authorization, Authentication, and Accounting
CB	Certification Body
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CM	Configuration Management

CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ETM®	Enterprise Telephony Management
ETR	Evaluation Technical Report
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PBX	Private Branch Exchange
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
PKCS	Public-Key Cryptography Standards
PRI	Primary Rate Interface
QA	Quality Assurance
RNG	Random Number Generator
SS7	Signaling System 7
SFP	Security Function Policy
ST	Security Target
TCP/IP	Transmission Control Protocol/ Internet Protocol
TOE	Target of Evaluation

References

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

a. Common Criteria for Information Technology Security Evaluation, CCIMB-99-031/032/033, Version 2.1, August 1999.

b. Common Methodology for Information Technology Security Evaluation, CEM-99/045, Part 2: Evaluation and Methodology, Version 1.0, August 1999.

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 4.1, 1463-011-D001, Version v1.5, 23 March 2004; and

e. Evaluation Technical Report (ETR) SecureLogix Corporation® ETM® (Enterprise Telephony Management) System V4.1, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-23, Document No. 1463-000-D002, Version 0.3, 23 March 2004.