Certification Report

EAL 3 Evaluation of Concepteers Teleconsole™ Version 2.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-177-CR
Version: 1.0
Date: 18 July 2011
Pagination: i to iii, 1 to 9

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 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 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 Canada, 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 Communications Security Establishment Canada, 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 Canada.

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/IEC 17025:2005, General requirements for the Competence of Testing and Calibration 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, Canada.

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 18 July 2011, 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 (CPL) and the Common Criteria Portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarked or registered trademark:

- *Teleconsole is a registered trademark of Concepteers LLC in the United States and other countries.*

TABLE OF CONTENTS

Executive Summary

The Concepteers Teleconsole™ Version 2.0 (hereafter referred to as the Teleconsole Version 2.0), from Concepteers LLC, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 3 evaluation.

Teleconsole Version 2.0 is a software product which acts as a secure application-layer gateway to intermediate all requests between remote computers and internal resources. All requests from remote computers to the Teleconsole Version 2.0 and from the Teleconsole Version 2.0 to remote computers are encrypted using TLS1.0/HTTPS encryption. All unencrypted requests (e.g. HTTP) are redirected to HTTPS, which ensures the connection is encrypted. Users gain authenticated access to authorized resources via an extranet session hosted by the product. Each request is subject to administratively defined access control and authorization policies before the request is forwarded to an internal resource.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 13 July 2011 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 Teleconsole Version 2.0, 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 (ETR)[1] for this product provide sufficient evidence that it meets the EAL 3 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 3.*

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Teleconsole™ Version 2.0 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) and the Common Criteria portal (the official website of the Common Criteria Project).

[1] The ETR 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) 3 evaluation is Concepteers Teleconsole™ Version 2.0 (hereafter referred to as Teleconsole Version 2.0), from Concepteers LLC.

2 TOE Description

Teleconsole Version 2.0 is a software TOE which acts as a secure application-layer gateway to intermediate all requests between remote computers and internal resources. All requests from remote computers to the TOE and from the TOE to remote computers are encrypted using TLS1.0/HTTPS encryption. All unencrypted requests (e.g. HTTP) are redirected to HTTPS, which ensures the connection is encrypted. Users gain authenticated access to authorized resources via an extranet session hosted by the TOE. Each request is subject to administratively defined access control and authorization policies before the request is forwarded to an internal resource.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the Teleconsole Version 2.0 is identified in Section 6 of the Security Target (ST).

The following cryptographic modules were evaluated to FIPS 140-2 standard:

Cryptographic Modules	**Certificate #**
Concepteers Teleconsole TCS6U4W Firmware Version 2.0	*Pending*[2]
Concepteers Teleconsole E Firmware Version 2.0	*Pending*

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation:

Cryptographic Algorithm	**Standard**	**Certificate #**
Advanced Encryption Standard (AES)	FIPS 197	1554/1547
Triple-DES (3DES)	FIPS 46-3	1014/17
Secure Hash Algorithm (SHA-1)	FIPS 180-3	1369/1374
Digital Signature Algorithm (DSA)	FIPS 186-3	476/479
Rivest Shamir Adleman (RSA)	ANSI X9.31	747/752

[2] The cryptographic modules are in the process of FIPS 140-2 validation under the Cryptographic Module Validation Program (CMVP). Information regarding the status of the module validations can be found on the NIST website.

Cryptographic Algorithm	Standard	Certificate #
	PKCS #1 v1.5 RSASSA-PSS	
Random Number Generation (RNG)	ANSI x9.31	832/836

4 Security Target

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

Title: Security Target Concepteers Teleconsole Family Version 2.0
Version: 1.2
Date: 22 June 2011

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*.

The Teleconsole Version 2.0 is:

a. Common Criteria Part 2 conformant, with security functional requirements based on functional components in Part 2; and
b. Common Criteria Part 3 conformant, with security assurance requirements based on assurance components in Part 3.

6 Security Policy

The Teleconsole Version 2.0 implements an authenticated user policy to control all access requests between remote computers and internal resources. Each request is subject to administratively defined access control and authorization policies before the request is forwarded to an internal resource. Further details on this security policy may be found in Section 7.4 of the ST.

In addition, the Teleconsole Version 2.0 implements policies pertaining to security audit, cryptographic operations, identification and authentication, security management, and protection of the TOE Security Functionality (TSF). Further details on these policies may be found in Section 7.0 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the Teleconsole Version 2.0 product 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 TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

a. There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE;

b. Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error;

c. The TOE does not host public data; and

d. Information cannot flow among the internal and external networks unless it passes through the TOE.

7.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

a. The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

7.3 Clarification of Scope

Teleconsole Version 2.0 is not intended to be placed or operated in a hostile environment and should be protected by other products specifically designed to address sophisticated threats.

8 Evaluated Configuration

The evaluated configuration comprises Teleconsole Version 2.0 build 1407 running on Concepteers Teleconsole TCS6U4W or Teleconsole E hardware platforms.

The publications listed in section 9 below describe the procedures necessary to install and operate the Teleconsole Version 2.0 in its evaluated configuration.

9 Documentation

The Concepteers documents provided to the consumer are as follows:

a. Quick Install Guide Teleconsole S6U4W Secure Remote Diagnostic Access Gateway, 2010; or

b. Quick Install Guide Teleconsole E Secure Remote Diagnostic Access Gateway, 2011;

c. Administration Manual Teleconsole S6U4W Secure Remote Diagnostic Access Gateway, Revision v1.2.11, 2010; and

d. Operational User Guidance and Preparative Procedures Supplement Concepteers Teleconsole Family Version 2.0, February 7, 2011.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the Teleconsole Version 2.0, including the following areas:

Development: The evaluators analyzed the Teleconsole Version 2.0 functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements. The evaluators analyzed the Teleconsole Version 2.0 security architectural description and determined that the initialization process was secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance Documents: The evaluators examined the Teleconsole Version 2.0 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Life-Cycle Support: An analysis of the Teleconsole Version 2.0 configuration management system and associated documentation was performed. The evaluators found that the Teleconsole Version 2.0 configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was also observed during the site visit, and it was found to be mature and well developed.

During the site visit the evaluators examined the development security procedures and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the Teleconsole Version 2.0 design and implementation. The evaluators confirmed that the developer used a documented model of the TOE life-cycle and that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Teleconsole Version 2.0 during distribution to the consumer.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of Teleconsole Version 2.0. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables. The evaluators

identified potential vulnerabilities for testing applicable to the Teleconsole Version 2.0 in its operational environment.

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

11 ITS Product Testing

Testing at EAL 3 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 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 ETR[3].

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

11.2 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. Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration, as identified in the TOE Description of the Security Target, by following all instructions in the developer's Installation and Administrative guidance;

b. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests on the evaluator's TOE installation;

c. Independent Evaluator Testing: The objective of this test goal is to exercise the TOE's claimed functionality through evaluator independent testing and to augment any areas that were not covered during the repeat of developer testing;

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

d. Audit. The objective of this test goal is to exercise the TOE's claimed audit functionality. Evaluator testing focussed on the backup of TOE audit logs and startup and shutdown of the TOE's audit functionality; and

e. Password Policy. The objective of this test goal is to verify that the TOE enforces administrator configured password policies.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- Search for generic vulnerabilities: Vulnerability sites were searched for Teleconsole Version 2.0 vulnerabilities. No vulnerabilities were found;
- Bypassing by attempting to exploit the capabilities of TOE interfaces in an unexpected way which could result in a violation of a TOE security policy;
- Tampering to verify that the TOE is resistant to standard SQL injection attacks;
- Monitoring to verify that the TOE does not leak sensitive information; and
- Verification that the TOE continues to operate when a communications failure has occurred.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

11.4 Conduct of Testing

Teleconsole Version 2.0 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Testing (ITSET) Facility at EWA-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 a separate Test Procedures and Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the Teleconsole Version 2.0 behaves as specified in its ST, functional specification, TOE design, and security architecture description.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 3 level of assurance. The overall verdict for the evaluation is PASS. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

The Teleconsole Version 2.0 must be operated in accordance with the provided Installation and Administration Guides and must be installed within a non-hostile and well-managed operating environment.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CMVP	Cryptographic Module Validation Program
CPL	Certified Products list
CVE	Common Vulnerabilities and Exposures
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
SFP	Security Function Policy
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

15 References

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

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. Security Target Concepteers Teleconsole Family Version 2.0, Revision No. 1.2, 22 June 2011.

e. Evaluation Technical Report (ETR) for EAL 3 Common Criteria Evaluation of Concepteers LLC Concepteers Teleconsole™ Version 2.0, Document No. 1688-000-D002, Version 1.3, 13 July 2011, Common Criteria Evaluation Number: 383-4-177.