Certification Report

EAL 3 Evaluation of Clinicomp International, Inc.

Essentris Clinical Information System

Release 1.4

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-43-CR
Version: 1.0
Date: 11 April 2008
Pagination: i to iv, 1 to 11

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 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada (CSEC), 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 CSEC, 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 (CSEC).

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 DOMUS IT Security Laboratory, a division of NUVO Network Management, 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 11 April 2008, 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 http://www.commoncriteriaportal.org/

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

- Essentris is a registered trademark of Clinicomp, International.

TABLE OF CONTENTS

Executive Summary

The Essentris Clinical Information System Release 1.4, (hereafter referred to as Essentris 1.4), from Clinicomp International, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 3 evaluation

The Essentris 1.4 supports health care providers in the delivery of inpatient clinical care. The system consists of clinical information software that is deployed in a client-server open architecture and supports integration and use of industry standard hardware components. Essentris 1.4 supports the following types of patient care:

- Physician/nurse histories and physicals;
- Progress notes for all disciplines, including occupational therapists and social workers;
- Assessments;
- Vital sign monitoring;
- Critical paths;
- Plans of care;
- Orders;
- Admission data and laboratory and radiology values/results;
- Medications/treatments; and
- Discharge summaries.

Essentris also provides for graphical trending of patient parameters, a reference library, patient care educational materials, and various integrated ambulatory and imaging systems.

DOMUS IT Security Laboratory, a division of NUVO Network Management, is the CCEF that conducted the evaluation. This evaluation was completed on 28 March 2008 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 Essentris 1.4, 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

[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.

functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*.

CSEC, as the CCS Certification Body, declares that the Essentris 1.4 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 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 evaluation is the Essentris Clinical Information System Release 1.4, (hereafter referred to as Essentris 1.4), from Clinicomp International, Inc..

2 TOE Description

The Essentris 1.4 supports health care providers in the delivery of inpatient clinical care. The system consists of clinical information software that is deployed in a client-server open architecture and supports integration and use of industry standard hardware components. Essentris 1.4 supports the following types of patient care:

- Physician/nurse histories and physicals;
- Progress notes for all disciplines, including occupational therapists and social workers;
- Assessments;
- Vital sign monitoring;
- Critical paths;
- Plans of care;
- Orders;
- Admission data and laboratory and radiology values/results;
- Medications/treatments; and
- Discharge summaries.

Essentris also provides for graphical trending of patient parameters, a reference library, patient care educational materials, and various integrated ambulatory and imaging systems.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the Essentris 1.4 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: Essentris Release 1.4 Security Target
Version: Version 255-50042-A (3/08)
Date: 19 March 2008

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3.*

The Essentris 1.4 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 3 conformant, with all security the assurance requirements in the EAL 3 package.

6 Security Policy

The Essentris 1.4 implements a role-based access control policy to control user access to the system. Details of the security policy can be found in Section 5 of the ST.

In addition, the Essentris 1.4 implements policies pertaining to security audit, identification and authentication, and security management. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the Essentris 1.4 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:

- Systems administration functions are only performed by trained and trusted system administrators; and
- Authorized administrators and installers are non-hostile.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE will be installed in an IT environment built for complete system and data availability.
- All connections to peripheral devices reside within the controlled access facilities. TOE only addresses security concerns related to the manipulation of the TOE through its authorized access points. Internal communication paths to access points such as terminals are assumed to be adequately protected.
- The internal communication channel between the TOE Client and Server platforms is a LAN that resides within the controlled access facilities. Internal communication paths connecting TOE Client and Server Platforms are assumed to be adequately protected.

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

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

7.3 Clarification of Scope

The Essentris 1.4 provides a level of protection that is appropriate for an assumed non-hostile and well-managed user community. While it is designed to protect its user community against inadvertent or casual attempts to breach system security, it is not intended for situations in which determined attempts by hostile and well-funded attackers use sophisticated attacks to violate system security, particularly from within the physical zone or domain of deployment. The Essentris 1.4 is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, personnel and communications security.

8 Architectural Information

The Essentris 1.4 is a clinical information software that integrates with physiological monitoring and automated medical instruments. Sub-systems and modules are:

Discretionary Access Control (DAC) that restricts user access to system data and functions based upon the user's duties and responsibilities. Essentris 1.4 applications enforce access control through user privileges (e.g., read, write, and modify) restricting access to both sensitive patient data and system functions. Users must enter their assigned User Identification Code (UIC) and password to access the system and system functions (e.g. data store, order approval, order entry, etc.).

Essentris 1.4 also limits access to the functions that can be performed from an individual terminal. Essentris 1.4 can restrict access from a terminal to clinical units, subject to override within an individual user's permissions. This safeguard restricts users in one unit from obtaining information about a patient in another unit. In conjunction with user access controls, this is an effective tool to deter system users from performing unauthorized activities. If a terminal is inadvertently left unattended, Essentris 1.4 provides security features such as a terminal time out, terminal lock, and authentication to prevent unauthorized access to the application functions and sensitive patient data.

Access permissions are defined using the **Staff Configuration Tool** (SCT) and **Terminal Configuration Tool** (TCT) modules. Access to the SCT and TCT modules is restricted to the Clinical System Administrator (CSA) or individuals with equivalent permissions.

Identification and Authentication ensures that accountability is established and maintained for users. Access control decisions are based on user security attributes. Essentris 1.4 users must enter a unique UIC and password to access the system and system functions. The UIC

and password are assigned to users when their account is established. In CC mode, Essentris 1.4 is configured to lockout accounts after five (5) sequential failed login attempts.

Security Management by Essentris 1.4 includes management of user identification and authentication, terminal access, user access based on assigned permissions, and audit of user transactions. Essentris system security safeguards are configured and managed through the SCT and TCT modules. Access to the SCT and TCT modules is restricted to the MTF CSA. The CSA is responsible for establishing user accounts, granting user permissions based on their need-to-know, and controlling the system security configuration.

Audit tracks and records security relevant activity. Essentris 1.4 ensures accountability by associating each recorded event with a specific user based upon the unique staff identification code assigned to the user account. After entering their UIC and password to gain system access, users must again enter their UIC and password in order to complete transactions such as storing, modifying or deleting data. The **Audit Log Viewer** module allows CSAs to review user activity (e.g., access to a function or if access was denied, incorrect password attempts).

9 Evaluated Configuration

For evaluated configuration detail refer to Section 2.1 of the ST.

10 Documentation

The Essentris 1.4 documents provided to the consumer are as follows:

- Essentris User Manual, P/N 250-51049-C; and
- Essentris Clinical System Administrator Manual, P/N 250-51036-C.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the Essentris 1.4, including the following areas:

Configuration management: An analysis of the Essentris 1.4 configuration management system and associated documentation was performed. The evaluators found that the Essentris 1.4 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 Essentris 1.4 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 Essentris 1.4 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 Essentris 1.4 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 examined 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 Essentris 1.4 design and implementation.

Vulnerability assessment: The Essentris 1.4 ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the Essentris 1.4 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 at EAL 3 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

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 ETR[2].

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

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 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 DOMUS IT Security Laboratory, a division of NUVO Network Management test goals:

- Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;
- Audit: The objective of this test goal is to determine that audit data is stored, is protected, and can be accessed and searched;
- Authentication: The objective of this test goal is to determine the TOE's ability to authenticate users;
- Discretionary Access Control: The objective of this test goal is to determine the TOE's ability to provide access to system data and functions; and
- Security Management: The objective of this test goal is to determine the CSA's ability to manage security attributes.

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:

- Generic vulnerabilities;
- Port Scanning;
- Monitoring netwrk traffic; and
- SQL injection.

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

12.4 Conduct of Testing

The Essentris 1.4 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 Test (ITSET) Facility at DOMUS IT Security Laboratory, a division of NUVO Network Management. 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 Results document.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the Essentris 1.4 behaves as specified in its ST and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 3 **l**evel 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

Consumers of the Essentris Clinical Information System Release 1.4 should consider assumptions about usage and environmental settings, defined in the Section 3 of ST, and the TOE protection scope, clarified in the Section 7.3 of this document, as requirements for the product's installation and its operating environment.

15 Glossary

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

15.1 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CSA	Clinical System Administrator
CPL	Certified Products list
CM	Configuration Management
CSEC	Communications Security Establishment Canada
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
MTF	Medical Treatment Facility
PALCAN	Program for the Accreditation of Laboratories Canada
SCT	Staff Configuration Tool
ST	Security Target
TCT	Terminal Configuration Tool
TOE	Target of Evaluation
UIC	User Identification Code

16 References

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

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS) Publication #4, Technical Oversight, Version 1.0.

b. Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005.

c. Common Methodology for Information Technology Security Evaluation, CEM, version 2.3, August 2005.

d. Clinicomp, Intl. Essentris Release 1.4 Security Target, Version 255-50042-A (3/08), March 19 2008.

e. Evaluation Technical Report for EAL3 Evaluation of Essentris Clinical Information System Release 1.4, Version 1.2, March 26, 2008.