Certification Report

EAL 3 Evaluation of Thales Communications S. A.

External Communications Management System (ECMS)

Version 4.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-24-CR
Version: 1.0
Date: 19 August 2004
Pagination: i to iv, 1 to 10

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, have been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for IT 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.

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 Laboratories, 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 19 August 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 which is a registered trademark of Microsoft Corporation; JDK (Java Development Toolkit) which is a trademark of Sun Microsystems Inc.; EXCEED which is a registered trademark of Hummingbird Ltd.; INGRESS which is a registered trademark of Computer Associates International Inc.; and Rational ClearCase which is a registered trademark of IBM.

TABLE OF CONTENTS

Executive Summary

The External Communications Management System Version 4.1, from Thales Communications S.A., is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 evaluation.

The External Communications Management System (ECMS) Version 4.1, together with the Internal Communications Management System (ICMS) Version 3.7.1.0, form the Communications Control and Monitoring System (CCMS) which manages all internal and external communications equipment on shipboard communications systems.

The ECMS is a software application that runs on CCMS workstations. It manages the following aspects of the communications system:

- Radio equipment such as HF transmitters, HF receivers, V/UHF transceivers and modems; and
- Radio services supported by this equipment offering voice and data communication services.

DOMUS IT Security Laboratories is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 12 August 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 ECMS, 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 ECMS 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 3 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 1.0* (with applicable final interpretations), for conformance to the *Common Criteria for IT Security Evaluation, version 2.1*.

[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.

The Communications Security Establishment, as the CCS Certification Body, declares that the ECMS 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) 3 evaluation is the External Communications Management System Version 4.1, from Thales Communications S.A.

2 TOE Description

The External Communications Management System (ECMS) Version 4.1, together with the Internal Communications Management System (ICMS) Version 3.7.1.0, form the Communications Control and Monitoring System (CCMS) which manages all internal and external communications equipment on shipboard communications systems.

The ECMS is a software application that runs on CCMS workstations. It manages the following aspects of the communications system:

- Radio equipment such as HF transmitters, HF receivers, V/UHF transceivers and modems; and

- Radio services supported by this equipment offering voice and data communication services.

The ECMS security services enforce the ECMS Security Policy (identified in Chapter 6 of this report).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the ECMS is identified in Section 5.1 of the security target (ST).

4 Security Target

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

Title: Security Target External Communications Management System
Version: Issue 1.2
Date: January 15, 2004

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for IT Security Evaluation, version 2.1* incorporating all final interpretations issued prior to 23 May 2003. The ECMS 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 the security assurance requirements in the EAL 3 package.

6 Security Policy

The ECMS Security Policy states the rules by which the ECMS manages communications resources. The complete ECMS Security Policy is identified in the ST. The following statements are representative of the ECMS Security Policy:

Identification and Authentication. Users of the ECMS are required to successfully identify and authenticate before they are granted access to the functional aspects of the software.

Access Control. The ECMS implements and enforces a discretionary access control environment. Within this environment, each user's access to controlled peripherals and components within the application is determined by the user's assigned role. The ECMS controls access to radio equipment such as HF transmitters, HF receivers, V/UHF transceivers and modems and the radio services supported by this equipment offering voice and data communication services.

Audit. The audit component of the ECMS generates audit logs upon use of the identification and authentication mechanisms, upon performance of an operation on an object covered by the ECMS Security Policy and upon performance of preset actions taken due to exceeding of a set threshold, e.g. audit log exceeding 80% capacity. The audit records are protected by ensuring that only authorized users have access to the audit records. The audit records are protected from deletion, modification and system failures.

7 Assumptions and Clarification of Scope

Consumers of the ECMS 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 ECMS.

7.1 Secure Usage Assumptions

For purposes of this evaluation, the users are assumed to be trusted and to understand the correct usage of the system. The users must operate the ECMS following the guidance in the *ECMS Operating Instructions*.

7.2 Environmental Assumptions

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

a) The components of the ECMS will be located within controlled access facilities which will prevent unauthorised physical access;

b) Administrators are non-hostile and will not attempt to compromise the ECMS functionality; and

c) Logical and physical protection will be provided for the communications with peripheral devices.

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

7.3 Clarification of Scope

The ECMS 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.

8 Architectural Information

The ECMS is a software application that resides on a PC running the Windows NT® operating system. Users interface with the application via the PC's keyboard and display.

The Target of Evaluation (TOE) is denoted in figure 2.1 of the ST as the ECMS Core, and comprises the following subsystems:

a) *HOST*, that provides management of security and other basic services for other subsystems;

b) *Service Manager*, that is used to manage a set of communication services using the resources and services managed by the lower level subsystems;

c) *Delegation Manager*, that delegates the remote control of remote controllable equipment to Delegate Managers; and

d) *Agent Manager XXX*, that manages remote controllable equipment.

9 Evaluated Configuration

The TOE is evaluated under the same configuration as indicated in the ST, except that no radio equipment which the TOE is designed to command was available due to transportation constraints.

The ECMS Host application runs on a Microsoft® Windows NT4® PC. The following software is used by the ECMS Host application:

- JDK™ 1.2.2
- EXCEED®
- Microsoft® Windows NT® 4 Service Pack 6a
- INGRES® II.

10 Documentation

The documentation for the ECMS consists of *ECMS Operating Instructions (Issue 06/2004)* which is described in Section 11 below.

11 Evaluation Analysis Activities

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

Configuration management: An analysis of the ECMS development environment and associated documentation was performed. The evaluators found that the ECMS configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system (Rational® ClearCase®) was observed during a site visit, and was found to be mature and well developed. In particular, the developer uses an integrated suite of commercial tools to perform software configuration management and problem tracking.

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 ECMS during distribution to the consumer. The evaluators examined 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 ECMS 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 *ECMS Operating Instructions* document 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. The *ECMS Operating Instructions* document includes both the user and administrator manuals.

Life-cycle support: The evaluators assessed the development security procedures during a site visit and determined that the procedures detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the ECMS design and implementation.

Vulnerability assessment: The ECMS Security Target's claims for the strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis, and found that it sufficiently described each of the potential vulnerabilities along with 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 had considered all potential vulnerabilities.

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

12 ITS Product Testing

Testing at EAL3 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing independent vulnerability tests.

12.1 Assessing Developer's Tests

The evaluators verified that the developer had met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Technical Report (ETR)[2].

The evaluators analyzed the developer's test coverage analysis and test depth analysis, and found it to be complete and accurate. The correspondence between tests identified in the

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

developer's test documentation and the functional specification and high-level design was complete.

12.2 Independent Functional Testing

During this evaluation, the evaluators developed independent functional tests by examining the 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.

Independent functional testing focused on the ECMS Security Policy, specifically:

a) Testing that User Interfaces and User Roles corresponded;

b) Access control testing;

c) Testing of audit;

d) Abstract machine testing; and

e) Consequence of successive failed login attempts.

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 ECMS in the anticipated, restrictive operating environment.

12.4 Conduct of Testing

The ECMS was subjected to a comprehensive suite of formally-documented, independent functional tests. The testing took place at the DOMUS IT Security Laboratories 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 tests and independent functional tests yielded the expected results, giving assurance that the ECMS behaves as specified in its ST and functional specification.

13 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.

14 Evaluator Comments, Observations and Recommendations

The ECMS must be operated in accordance with the *ECMS Operating Instructions* and must be installed within a non-hostile and well-managed user community.

15 Acronyms and Abbreviations

Acronym/Abbreviation/Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCRA	Common Criteria Recognition Arrangement
CCS	Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CR	Certification Report
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
ECMS	External Communications Management System
ICMS	Internal Communications Management System
PALCAN	Program for the Accreditation of Laboratories Canada
ST	Security Target

16 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 External Communications Management System, Version 4.1, Issue 1.2, 15 January 2004.

e) Evaluation Technical Report (ETR) External Communications Management System, Version 1.0, 11 August 2004.