Certification Report

EAL 3 Evaluation of Thales Systems Canada

Message Handling System (MHS)

MHS Server Version 5.1, MHS Client Version 1.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-19
Version: 1.0
Date: 30 April 2004
Pagination: i to iv, 1 to 12

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 30 April 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 registered trademark of Microsoft Corporation; Java which is registered trademark of Sun Microsystems Inc.; Intel and Pentium which are registered trademarks of Intel Corporation; and Interbase which is a registered trademark of Borland Software Corporation.

TABLE OF CONTENTS

Executive Summary

The Thales Message Handling System (MHS), MHS Server Version 5.1 and MHS Client Version 1.0, from Thales Systems Canada, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 evaluation.

The Thales MHS is a multi-user, network based, Commercial-Off-The-Shelf (COTS), configurable application which prepares, transmits, receives, and distributes radio teletype messages. The system provides the user with the ability to create, modify, store, distribute, send, and receive messages simultaneously over all channels in the communication system.

The Thales MHS is a message handling system based on the Allied Communication Publication (ACP) 127 message format, a radio teletype standard, which is widely used in naval systems. However, the MHS does not support industry-standard email protocols. It is designed to protect its user community against inadvertent or casual attempts to breach system security, and is appropriate for an assumed non-hostile and well-managed user community.

DOMUS IT Security Laboratories is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 16 April 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 Thales MHS, 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 Thales MHS 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*.

The Communications Security Establishment, as the CCS Certification Body, declares that the Thales MHS evaluation meets all the conditions of the *Arrangement on the Recognition*

[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.

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 Thales Message Handling System (MHS), MHS Server Version 5.1 and MHS Client Version 1.0, from Thales Systems Canada.

The TOE consists of the following distributed software components:

- MHS Server, Version 5.1; and
- MHS Client, Version 1.0.

2 TOE Description

The Thales MHS is a multi-user, network based, Commercial-Off-The-Shelf (COTS), configurable application which prepares, transmits, receives, and distributes radio teletype messages. The Thales MHS provides the user with the ability to create, modify, store, distribute, send, and receive messages simultaneously over all channels in the communication system. It is based on the Allied Communication Publication (ACP) 127 message format, a radio teletype standard, which is widely used in naval systems.

Figure 2-1 in the Security Target (ST) shows the environment in which the Thales MHS operates. The Thales MHS Server software component resides on the Master Server and the Thales MHS Client software component resides on the User Terminals.

The Thales MHS security services enforce the Thales MHS Security Policy (identified in Chapter 6 of this report) for all outgoing and incoming messages.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the Thales MHS is identified in Section 5.1 of the ST.

4 Security Target

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

Title: Thales Message Handling System Security Target
Version: Version 3.0
Thales Systems Canada Document No: 1165C.011-ST REV.07
Date: April 16, 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 22 May 2003. The Thales MHS 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 Thales MHS Security Policy states the rules by which the Thales MHS handles messages. The complete Thales MHS Security Policy is identified in the ST. The following statements are representative of the Thales MHS Security Policy:

Outgoing Messages. Every outgoing message has, at any given time after creation and prior to release, a unique owner user who has sole read-access, write-access and delete-access to the message. Every owner of an outgoing message may forward the message for review to any other user having read clearance for the classification of the message, in which case the owner's access privileges are transferred to the recipient of the outgoing message. For each classification of outgoing message, there may exist a release authority based on external organizational policy. If defined, only that release authority has release privilege for an outgoing message of the classification. Prior to release, an outgoing message may be re-classified by the current owner of the message to a classification of equal or less sensitivity to the release privilege of the owner.

Incoming Messages. The Thales MHS grants a user read-access to all incoming messages containing a classification level of equal or less sensitivity to the classification attribute of that specific user.

General. Read-access to a message is denied to any user whose read clearance is less than the classification of the message.

Message Export. Only the release authority having release permission for an outgoing message can transfer release permission for the message to a supervisor. Only a supervisor can execute the export of an outgoing message. Message classification is time-invariant for all Thales MHS operations after sending of an outgoing message.

Message Import. The Thales MHS preserves the time-invariance of the classification and all non-security attributes and content of every incoming message.

Audit. The Thales MHS records all commands/responses to/from users, events that pertain to message import, export and reading by a user and other key events within the Thales MHS Server (e.g., Server Startup and Shutdown).

7 Assumptions and Clarification of Scope

Consumers of the Thales MHS 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 Thales MHS.

7.1 Secure Usage Assumptions

For purposes of this evaluation, the system administrators are assumed to be trusted and to understand the correct usage of the system. The Thales MHS must be installed and configured using the guidance specified in *Thales Message Handling System (MHS) Belgium E71 Frigate Installation Instructions*; *Thales Message Handling System (MHS) Supervisor Manua*l; and *Thales Message Handling System (MHS) Administrator Manual*.

7.2 Environmental Assumptions

The following assumptions are made about the operating environment of the Thales MHS:

a) the components of the Thales MHS are located within controlled access facilities, that will prevent unauthorized physical access;

b) administrators are non-hostile and do not attempt to compromise the Thales MHS functionality; and

c) logical and physical protection must be provided for the communications between the Thales MHS Server and the Thales MHS Client.

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

7.3 Clarification of Scope

The Thales MHS 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 Thales MHS architecture comprises two software components, the Thales MHS Server and the Thales MHS Client.

8.1 Thales MHS Server

The Thales MHS Server is written in Ada95 and resides on a Windows NT based platform.

The Thales MHS Server is a single executable with multiple tasks running within a single memory space. The server's source code is made up from several logical components called packages. The Thales MHS Server package comprises two parts. One part contains the packages that process user commands (e.g., view message) and the other part contains the server supporting packages (e.g. input/output).

The Thales MHS Server displays three windows. One window is for starting the server via username and password, the second is a runtime window, and the third is a shutdown window for shutting down the server via username and password.

8.2 Thales MHS Client

The Thales MHS Client is written in Java2 and resides on a Windows NT based platform running Java2.

The Thales MHS Client has three different types of windows displayed, the type displayed depending on the type of user logged in. There are Administrator, Supervisor and User windows, each corresponding to the three roles a user can be assigned to.

The Thales MHS Client does not have direct access to data. To access data, the client issues commands on behalf of a user request (e.g., view message) to the server. The results of the commands are displayed within the client's window. Each Thales MHS Client runs as a separate executable and communicates with the Thales MHS Server using the TCP/IP protocol.

9 Evaluated Configuration

The minimum evaluated configuration for the Thales MHS comprises:

1. Thales MHS Server Version 5.1 running on an Intel Pentium PC with Microsoft Windows NT Server 4.0 Service Pack 6 (configured as per Microsoft C2 Administrator's and user's security guide 1.1 document), and Borland's Interbase 6 database software.

2. Thales MHS Client version 1.0 running on an Intel Pentium PC with Microsoft Windows NT Server 4.0 Service Pack 6 (configured as per Microsoft C2 Administrator's and user's security guide 1.1 document), and Sun's Java 2 runtime environment standard edition version 1.3.0_02.

Correct configuration is described in *Thales Message Handling System (MHS) Belgium E71 Frigate Installation Instructions,* in *Thales Message Handling System (MHS) Supervisor Manual*, and in *Thales Message Handling System (MHS) Administrator Manual.*

10 Documentation

The documentation for the Thales MHS consists of:

1. Thales Message Handling System (MHS) Belgium E71 Frigate Installation Instructions;
2. Thales Message Handling System (MHS) Supervisor Manual;
3. Thales Message Handling System (MHS) Administrator Manual; and
4. Thales Message Handling System (MHS) User Manual.

11 Evaluation Analysis Activities

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

Configuration management: An analysis of the Thales MHS development environment and associated documentation was performed. The evaluators found that the Thales MHS 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. In particular, the developer uses an integrated suite of commercial tools to perform software configuration management and problem tracking. The problem tracking tool is MKS Integrity Manager, and the software configuration management tool is MKS Source Integrity. The evaluators witnessed demonstration of MKS Integrity Manager and MKS Source Integrity.

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 Thales MHS 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 Thales MHS 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 Thales MHS 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 the procedures detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the Thales MHS design and implementation.

Vulnerability assessment: The Thales MHS 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. Limited penetration testing was conducted by evaluators, which exposed residual vulnerabilities not exploitable in the intended operating environment of the Thales MHS.

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 focussed on the Thales MHS Security Policy, specifically:

a) Creation of Roles by the Administrator;

b) Creation of Users by the Administrator;

c) Testing that User Interfaces and User Roles corresponded;

d) Testing of Role and User attributes management by the Administrator;

e) Testing of message ownership;

f) Testing transfer of message and message ownership;

g) Testing of the Release Authority Role;

h) Testing of re-classification of an outgoing message;

i) Testing that the classification of an outgoing message after transmission is time-invariant;

j) Testing access to an incoming message;

k) Testing that the classification of an incoming message is time-invariant;

l) Testing of the message queue;

m) Testing correctness of the ACP127 message formatter;

n) Testing of audit;

o) Abstract machine testing;

p) Password testing;

q) Testing of authentication before startup and shutdown; and

r) 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 Thales MHS in the anticipated, restrictive operating environment.

12.4 Conduct of Testing

The Thales MHS 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 Thales MHS 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 Thales MHS must be configured in accordance with the Thales MHS Installation Instructions and must be installed within a non-hostile and well-managed user community.

15 Acronyms and Abbreviations

Acronym/Abbreviation/Initialization	Description
ACP 127	Allied Communication Publication 127

CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation
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
MHS	Message Handling System
PALCAN	Program for the Accreditation of Laboratories Canada
RATT	Radio Teletype
ST	Security Target
TOE	Target of Evaluation

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) Thales Message Handling System Security Target, Version 3.0, 1165C.011-ST REV 07, 16 April 2004.

e) Evaluation Technical Report (ETR) Thales Systems Canada Message Handling System (MHS), Version 1.1, 16 April 2004.