Certification Report

EAL 4+ Evaluation of NetMotion Mobility XE® 9.5

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-185-CR
Version:	1.0
Date:	10 August 2012
Pagination:	i to iii, 1 to 10

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, the 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 10 August 2012, 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 registered trademarks:

- NetMotion Mobility and Mobility XE are registered trademarks of NetMotion Wireless, Inc.

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

TABLE OF CONTENTS

Executive Summary

NetMotion Mobility® XE™ 9.5 (hereafter referred to as Mobility XE™), from NetMotion Wireless, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

The TOE is a client/server-based software Virtual Private Network (VPN) which securely extends the enterprise network to the mobile environment enabling TCP/IP network applications to operate reliably, without modification, over wireless connections.

The TOE is managed via the Mobility console, which is a web-based configuration and management utility that an administrator can use to configure settings, monitor server status and client connections, monitor activity or event logs, and troubleshoot problems.

The TOE includes a FIPS 140-2 validated module, which performs cryptographic operations.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 19 July 2012 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 Mobility XE™, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its 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 4 *augmented* 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.* The following augmentation is claimed: ALC_FLR.1 – Basic Flaw Remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Mobility XE™ 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

[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.

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) 4 augmented evaluation is NetMotion Mobility XE® 9.5 (hereafter referred to as Mobility XE®), from NetMotion Wireless, Inc.

2 TOE Description

The TOE is a client/server-based software Virtual Private Network (VPN) which securely extends the enterprise network to the mobile environment enabling TCP/IP network applications to operate reliably, without modification, over wireless connections. When a mobile device goes out of range or suspends operation, Mobility XE® maintains the session status and resumes the session when the device returns to service. If the mobile device returns to service at a different point on the network or connects from a new location, the Mobility XE® server relays data to the new location, even if it is on a different subnet or a different network.

The TOE is managed via the Mobility console, which is a web-based configuration and management utility that an administrator can use to configure settings, monitor server status and client connections, monitor activity or event logs, and troubleshoot problems.

The TOE includes a FIPS 140-2 validated module, which performs cryptographic operations.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Mobility XE® is identified in Section 6 of the ST.

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

Cryptographic Module	**Certificate #**
Microsoft Windows 7 Kernel Mode Crypto Library (CNG.SYS)	1328
Microsoft Windows Server 2008 R2 Kernel Mode Cryptographic Primitives Library (CNG.SYS)	1335

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in Mobility XE®:

Cryptographic Algorithm	**Standard**	**Certificate #**
Advanced Encryption Standard (AES)	FIPS 197	1168, 1178, 1187
Secure Hash Algorithm (SHA-1), SHA-256, SHA-384, SHA-512	FIPS 180-3	1081
Random Number Generator	Digital Signature Standard Appendix 3.1	649

4 Security Target

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

Title: Security Target: NetMotion Mobility XE® 9.5
Version: 0.12
Date: 19 June 2012

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.*

Mobility XE® 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 4 augmented*, containing all security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.1 – Basic Flaw Remediation.

6 Security Policy

Mobility XE® implements a Secure Flow Control policy between TOE components which determines whether the Mobility Client can access data and resources on an internal, protected network. Details of this security policy can be found in Section 6 of the ST.

In addition, Mobility XE® implements policies pertaining to security audit, cryptographic support, identification and authentication, security management, and protection of the TOE

Security Functionality (TSF). Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Mobility XE® 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 Assumption is listed in the ST:

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

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- The TOE can receive time data from a reliable source.
- The communications between the TOE and external IT services is secured.
- The TOE does not host public data.

7.3 Clarification of Scope

Mobility XE® offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing enhanced-basic attack potential. Mobility XE is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The evaluated configuration for Mobility XE® comprises the NetMotion Mobility server software version 9.5 build 42566 running on Windows Server 2008 R2 SP1 and Windows Server 2008 R2; and the NetMotion Mobility client software version 9.5 build 42566 running on Windows 7 (64-bit Ultimate Edition) SP1 and Windows 7 (64-bit Ultimate Edition). The TOE also includes the CNG.SYS cryptographic module.

The publication *Operational User Guidance and Preparative Procedures Supplement NetMotion Wireless Mobility XE 9.5, Version 0.4* describes the procedures necessary to install and operate Mobility XE® in its evaluated configuration.

9 Documentation

The NetMotion Wireless, Inc. documents provided to the consumer are as follows:

a. Mobility XE System Administrator Guide, Version 9.5, January 2012; and

b. Operational User Guidance and Preparative Procedures Supplement NetMotion Wireless Mobility XE 9.5, Version 0.4, June 19, 2012.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Mobility XE®, including the following areas:

Development: The evaluators analyzed the Mobility XE® functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TSF interfaces and the TSF subsystems and modules, and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Mobility XE® security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Mobility XE® 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 are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the Mobility XE® configuration management system and associated documentation was performed. The evaluators found that the Mobility XE® configuration items were clearly marked and could be modified and controlled by automated tools. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed and operated in accordance with the CM plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorised access to the configuration items.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Mobility XE® during distribution to the consumer.

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 the Mobility XE® design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by NetMotion Wireless, Inc. for Mobility XE®. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of Mobility XE®. Additionally, the evaluators conducted a review of public domain vulnerability databases and a focused search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to Mobility XE® in its operational environment.

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

11 ITS Product Testing

Testing at EAL 4 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[2].

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, TOE design and security architecture description 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.

[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.

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 is the following list of EWA-Canada test goals:

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

b. Remote access to the administrator console: The purpose of this test case is to verify that the administrator console can only be accessed from the NetMotion Mobility server;

c. Create and delete security policy: The purpose of this test case is to verify that an administrative user can create and delete a security policy; and

d. Clear audit log: The purpose of this test case is to verify that only an administrative user can clear the audit log.

11.3 Independent Penetration Testing

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

a. Port scanning: The objective of this test goal is to scan the TOE using a port scanner to determine what ports were open and what services were running;

b. Vulnerability scanning: The objective of this test goal is to scan the TOE using a vulnerability scanner to determine if the TOE is susceptible to any particular attacks;

c. Information Leakage Verification: The objective of this test goal is to monitor the TOE for leakage during start-up, shutdown, and login; and

d. Session Management: The objective of this test goal is to verify that browser sessions were successfully destroyed.

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

11.4 Conduct of Testing

Mobility XE® 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 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 Results document.

11.5 Testing Results

The developer’s tests and the independent functional tests yielded the expected results, giving assurance that Mobility XE® 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 4+ 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 evaluator strongly recommends that the TOE administrator ensures that the FIPS 140-2 validated cryptographic module (CNG.SYS) is configured in accordance with the instructions contained within the *Operational User Guidance and Preparative Procedures Supplement NetMotion Wireless Mobility XE 9.5, Version 0.4*.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VPN	Virtual Private Network

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: NetMotion Mobility XE® 9.5, 0.12, 19 June 2012.

e. Evaluation Technical Report for EAL 4+ Common Criteria Evaluation of NetMotion Wireless, Inc. NetMotion Mobility XE 9.5, Document No. 1713-000-D002, Version 1.1, 19 July 2012.