Swedish Certification Body for IT Security

Certification Report - NetMotion Mobility 11.0

Issue: 1.0, 2017-dec-04

Authorisation: Imre Juhász, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is the NetMotion Mobility version 11.0. The TOE is software only and consists of a client/server based software, Virtual Private Network (VPN), that secures communications between the enterprise network and the mobile environment.

The TOE consists of the following parts:

- NetMotion Mobility 11.0 NetMotion Mobility 11.0 Server (11.04.21384)
- NetMotion Mobility 11.0 Client for Windows 8.1 (11.04.21384)
- NetMotion Mobility 11.0 Client for Windows 10 (11.04.21384)
- NetMotion Mobility 11.0 Client for Android (11.04.21376)
- NetMotion Mobility 11.0 Client for macOS (11.04.21579)
- NetMotion Mobility 11.0 Client for iOS (11.04.21379)

The NetMotion Mobility Server and Windows client software is delivered via a secure download from the NetMotion Wireless website via a SSL connection. The Android, macOS and iOS applications can be downloaded through Google Play and the Apple App store.

The TOE is dependent on the cryptographic modules implemented within the server (Windows Server 2012 R2) and client platforms (Windows 8.1, Windows 10, iOS 10, macOS 10.12 and Android 6.0) to perform cryptographic operations. The implementation of the cryptographic primitives and related key management are not covered in the evaluation. These cryptographic modules have been Federal Information Processing Standards (FIPS) 140-2 validated by the National Institute of Standards and Technology (NIST) in the United States of America (USA) and Communications Security Establishment (CSE) in Canada.

There are eight assumptions made in the ST regarding the secure usage and environment of the TOE. The TOE relies on these being met in order to be able to counter the four threats in the ST. The assumptions and the threats are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by Combitech AB and EWA-Canada. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT security Evaluation, version 3.1, release 5. The evaluation was performed at the evaluation assurance level EAL4, augmented by ALC_FLR.1.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation. EWA-Canada operates as a Foreign location for Combitech AB within scope of the Swedish Common Criteria Evaluation and Certification Scheme.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

EAL 4 + ALC_FLR.1.

The evaluation was completed on 2017-11-09. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 3.1 release *5*.

The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced by Combitech AB

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met. This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2015008
Name and version of the certified IT product	NetMotion Mobility 11.0, consisting of: - Server (11.04.21384) - Client for Windows 8.1 (11.04.21384) - Client for Windows 10 (11.04.21384) - Client for Android (11.04.21376) - Client for macOS (11.04.21579) - Client for iOS (11.04.21379)
Security Target Identification	NetMotion Mobility 11.0 Security Target, version 1.8
EAL	EAL 4 + augmented with ALC_FLR.1
Sponsor	NetMotion Wireless Incorporated
Developer	NetMotion Wireless Incorporated
ITSEF	Combitech AB and EWA-Canada
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	1.20.5
Recognition Scope	CCRA: EAL2 + ALC_FLR.1, SOGIS-MRA: EAL4 EA-MLA: EAL4 + ALC_FLR.1
Certification date	2017-12-07

3 Security Policy

The TOE consists of six security functions. Below is a short description of each of them. For more information, see Security Target [ST]:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF

3.1 Security Audit

The TOE generates audit records for security events. Only those roles that have been granted specific access to the audit trail have the ability to view the audit trail. For the purpose of this evaluation, only users in the Administrator role have been granted this access.

3.2 Cryptographic Support

The TOE supports secure communications between TOE components. This encrypted traffic prevents modification and disclosure of user information. Cryptographic functionality is provided by FIPS 140-2 validated modules in the operating systems of the server and client components. Cryptography also supports the authentication of users.

3.3 User Data Protection

The TOE provides an information flow security policy. The security policy limits access to internal protected resources based on policy settings. The TOE provides a secure connection between mobile users and the internal network. Traffic is protected from disclosure and modification.

3.4 Identification and Authentication

The TOE verifies that users are identified and authenticated before permitting access. Additionally, administrators must be identified and authenticated before access to administrative functions is permitted.

3.5 Security Management

The TOE provides security management functions through the Mobility Console. Administrators manage users, information flow policy, and audit.

3.6 Protection of the TSF

Reliable timestamps are provided in support of TOE functions, including the generation of audit records.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target makes eight assumptions on the operational environment of the TOE.

A.NOEVIL: Authorized administrators are non-hostile and follow all administrator guidance.

A.PHYSEC: The server resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

A.SECCOM: The communications between the TOE (Mobility server) and the authentication services and between the TOE (Mobility server) and the management console computer are secured on an internal network.

4.2 Environmental Assumptions

A.AUTH: The operational environment provides authentication services to the TOE.

A.CERTIFICATE: A Public Key Infrastructure is available to issue certificates to users and servers. Root trust exists for the certificated chain.

A.INTERNAL: The internal network and its assets are protected from unauthorized access. A firewall must be in place to ensure that only authorized connections from Mobility Clients to the Mobility Server are permitted.

A.MANAGE: A management console computer is available on the internal protected network for the purposes of managing the TOE. Administrators will access the Mobility Console only from a management console computer on the internal network.

A.OS: The services, including cryptographic services, provided by the underlying operating system work correctly, and the operating system does not introduce any negative side effects to the TSF.

4.3 Clarification of Scope

The Security Target contains four threats, which have been considered during the evaluation.

T.ACCESS: An unauthorized individual on an external network may access and exploit protected application data resources on an internal network.

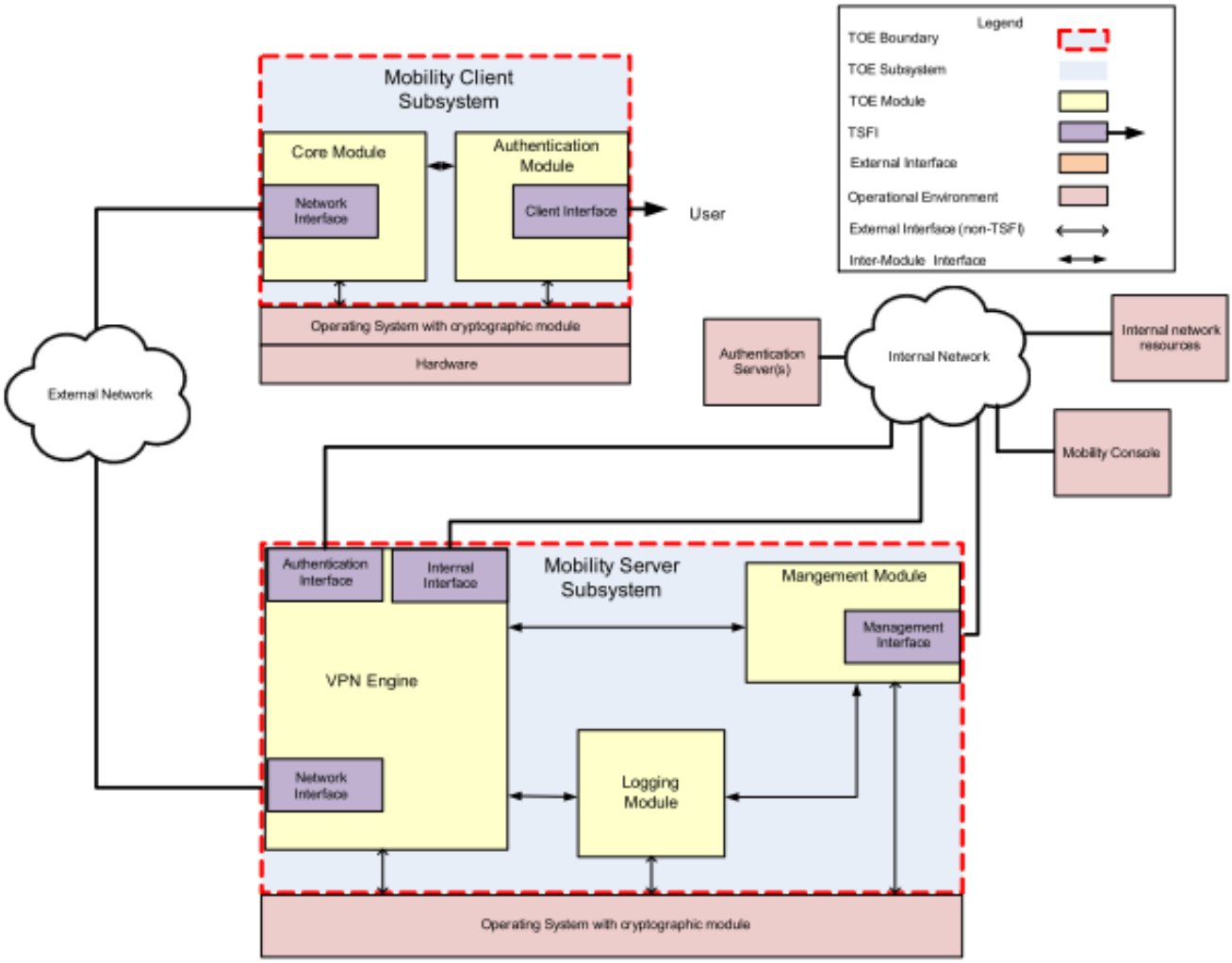
T.NOAUTH: An unauthorized individual may gain access to the TOE security management functions and use this to allow unauthorized access to application data protected by the TOE.

T.SENSDATA: An unauthorized individual may be able to view or alter sensitive application data passed between a client and a server.

T.UNAUTH: An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and application data.

5 Architectural Information

A TOE system overview is given in the figure below:



The subsystems are divided into the following parts:

5.1 Mobility Server Subsystem

Virtual Private Network (VPN) Engine

The VPN Engine ensures that Mobility client users are identified before allowing connections to the internal network resources protected by the Mobility Server. When a Mobility Client attempts to access the Mobility Server, the VPN Engine calls the external authentication server to validate the user credentials. The VPN Engine can allow or refuse information flow depending on the results of authentication and policy settings.

Management Module

The Management Module provides authorized administrators access to audit log information and security management functionality of the TOE.

Logging Module

The Logging Module records connection events in the activity log. The Management Module writes audit log messages to the event log for console events. The Logging Module records information on events that occur on the Mobility Server.

5.2 Mobility Client Subsystem

Authentication Module

The Authentication Module collects user identification and password information when a user attempts to log into the Mobility Client. The Authentication Module then passes the user credentials to the Core Module which launches the request to connect to the Mobility Server.

Core Module

The Core Module receives user credentials from the Authentication Module and attempts to connect with the Mobility Server. The Mobility Server requires that all users and devices first authenticate and establish an encrypted tunnel. Depending on the server configuration, authentication is performed using either PEAP MS-CHAPv2 or EAP-TLS.

6 Documentation

The physical scope of the TOE also includes the following guidance documentation:

- http://www.netmotionwireless.com/support/docs/MobilityXG/1100/help/mobilityhelp.htm#page/Mobility%20Server/intro.01.02.html
- NetMotion Mobility 11.0 Common Criteria Guidance Supplement

7 IT Product Testing

7.1 Developer Testing

The test configuration set up follows the information provided by the TOE boundary, function and evaluated configuration as stated in the [ST]. All clients were run in a virtual environment. The developer tests are well described and broken down into step by step descriptions with clear definition of the test criteria's for pass/fail. The tests set have consistent and adequate mapping between both TSFIs and the TSF-subsystems. The developer testing shows a complete pass verdict for every executed test. The developer testing activities are complemented by the evaluator independent testing as described below.

7.2 Evaluator Testing

The evaluator conducted the independent and penetration testing using the TOE installed on physical devices, thus minimizing the possible discrepancies from a real world configuration. The evaluator testing effort included both re-testing of the developer tests and the additional evaluator testing. The testing performed was divided into the following test groups:

- TOE Installation
- Access from Clients (EAP-TLS and PEAP-MsCHAPv2)
- Security Audit and Management function (change_default)
- User and Client Access
- Crypto Verification
- Repetition of Developer Testing

The following independent testing complemented the developer testing:

- Negative test of audit review permissions
- Cryptographic verification
- Key destruction source code inspection
- Test Quarantine on other than Android based devices
- Negative tests using invalid certificates and wrong passwords
- Test to change_default TSF data

The cryptographic functionality tests included verification against independent reference implementations of both cryptographic primitives and protocols.

7.3 Penetration Testing

Three types of penetration tests were performed:

- Port scan
- Vulnerability scan
- Network resilience

Port scans were run on the Mobility Server IP address after initial configuration according to the guidance documentation. The purpose was to check that no unused ports were opened and no unused IP services available by default. The Nmap port scan tool was used. Four different modes were used: TCP Connect, TCP SYN, UDP, and IP protocol scans. All possible 65535 ports were scanned.

Nessus vulnerability scans were run on the on the Mobility Server IP address. All Nessus scan modules available at the time were used.

The SSLyze scanner was run on the Mobility Server IP address to analyse the TOE TLS abilities.

The wireless connection between clients and the server were disrupted and connected again to verify the TOE network resilience and resistance to security breaches.

All penetration testing had negative outcome, i.e. no vulnerabilities were found.

8 Evaluated Configuration

The following software and hardware components are required for operation of the TOE in the evaluated configuration.

- NetMotion Mobility 11.0 Server:
  - Windows Server 2012 R2,
  - General Purpose Computing Platform with x64-compatible dual-core processor, 2.0 GHz, 4 GB RAM
- NetMotion Mobility 11.0 Windows Client
  - Windows 8.1
- NetMotion Mobility 11.0 Windows Client
  - Windows 10
- NetMotion Mobility 11.0 Android Client
  - Android version 6.0
- NetMotion Mobility 11.0 iOS Client
  - iOS 10
  - iPad, iPhone (Apple device with A7 to A9X hardware)
- NetMotion Mobility 11.0 macOS Client
  - macOS 10.12
  - Mac mini, iMac, MacPro or MacBook hardware

Operational Environment Components required

- Management Console Computer
  - Windows 10 Microsoft Edge 38
- RADUIS Authentication server(s) (provided as a service to the TOE)
  - Software supporting PEAP MS-CHAPv2 and EAP-TLS
- Public Key Infrastructure (provided as a service to the TOE)
- Firewall (General Purpose Firewall appliance)

In the evaluated configuration, the use of RC4 and MD5 must be disabled in the RADIUS server. However, it should be noted that even without this configuration, Mobility will default to PEAP authentication using a cipher-suite with RSA, AES 256 and SHA 384.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of enhanced-basic.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class Name / Assurance Family Name	Short name	Verdict
Security Target Evaluation	ASE	
ST Introduction	ASE_INT.1	Pass
Conformance claims	ASE_CCL.1	Pass
Security Problem Definition	ASE_SPD.1	Pass
Security objectives	ASE_OBJ.2	Pass
Extended components definition	ASE_ECD.1	Pass
Derived security requirements	ASE_REQ.2	Pass
TOE summary specification	ASE_TSS.1	Pass
Life-cycle support	ALC	
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Well-defined development tools	ALC_TAT.1	Pass
Basic flaw remediation	ALC_FLR.1	Pass
Development	ADV	
Security Architecure description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Basic modular design	ADV_TDS.3	Pass
Guidance documents	AGD	
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Tests	ATE	
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass

Functional testing	ATE_FUN.1	Pass
Independent testing - Sampling	ATE_IND.2	Pass
Vulnerability assessment	AVA	
Focused vulnerability analysis	AVA_VAN.3	Pass

10 Evaluator Comments and Recommendations

The evaluators have no remaining comments, observations, or recommendations.

10.1 Certifier comments and Recommendations

The TOE relies on cryptographic functions implemented in cryptographic modules, the internals of which has not been covered by this evaluation as permitted by SP-188 Scheme Crypto Policy. These cryptographic modules have been FIPS 140-2 validated as stated in the ST.

Full testing of the cryptographic functionality as used by the TOE has been done through the external interfaces. Code review of the calls to the cryptographic modules has been performed as part of the evaluation.

11 Glossary

CC	Common Criteria
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
EAL	Evaluation Assurance Level
FER	Final Evaluation Report
FIPS	Federal Information Processing Standards
FLR	Flaw Remediation
HTTPS	Hypertext Transfer Protocol Secure
iOS	Apple iPhone Operating System
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
PEAP	Protected Extensible Authentication Protocol
SSL	Secure Sockets Layer
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TLS	Transport Layer Security
TOE	Target of Evaluation
VPN	Virtual Private Network

12 Bibliography

[CCp1] Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 5, September 2012, CCMB-2012-09-001

[CCp2] Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 5, September 2012, CCMB-2012-09-002

[CCp3] Common Criteria for Information Technology Security Evaluation, Part 3:, version 3.1, revision 5, September 2012, CCMB-2012-09-003

[CEM] Common Methodology for Information Technology Security Evaluation, version 3.1, revision 5, September 2012, CCMB-2012-09-004

[SP-002] Evaluation and Certification, SP-002, Issue: 26.0, 2017-06-27, FMV/CSEC

[ST] NetMotion Mobility® 11.0 Security Target, Doc No: 1905-000-D102, NetMotion Wireless Incorporated, document Version 1.8, 2017-09-29

[AGDWIN] http://www.netmotionwireless.com/support/docs/MobilityXG/1100/help/mobilityhelp.htm#page/Mobility%20Server/intro.01.02.html, NetMotion Wireless Incorporated, 2017-05-17

[CCADM] NetMotion Mobility 11.0 Common Criteria Guidance Supplement, Doc No: 1905-000-D105, NetMotion Wireless Incorporated, Version 1.4, 2017-06-08

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme has been used.

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
1.21	2017-11-15	*None*
1.20.5	2017-06-26	*None*
1.20.4	2017-05-11	*None*
1.20.3	2017-04-24	*None*
1.20.2	2017-02-27	*None*
1.20.1	2017-01-12	*None*
1.20	2016-10-20	*None*
1.19.3	2016-06-02	Original version

A.2 Scheme Notes

Scheme Note	Title	Applicability
SN-15	Demonstration of test coverage	ATE
SN-18	Highlighted Requirements on the Security Target	ASE