Security Target

NetMotion Mobility XE® 9.5

Document Version 0.12

June 19, 2012

Prepared For:

NetMotion Wireless, Inc.
701 N 34th Street, Suite 250,
Seattle, WA 98103
www.netmotionwireless.com

Prepared By:

Apex Assurance Group, LLC
530 Lytton Avenue, Suite 200
Palo Alto, CA 94301
www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Mobility XE 9.5. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	Security Target: NetMotion Mobility XE 9.5
ST Revision	0.12
ST Publication Date	June 19, 2012
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	NetMotion Mobility XE 9.5
TOE Type	VPN

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *italicized* text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

When not embedded in a Security Functional Requirement, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table describes the acronyms used in this document:

TERM	DEFINITION
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CC	Common Criteria version 3.1
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
OSP	Organizational Security Policy
RFC	Request for Comment
RSA	Rivest Shamir Adelman
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security

TERM	DEFINITION
TSF	TOE Security Function
VPN	Virtual Private Network

Table 2 – Acronyms Used in Security Target

1.6 TOE Overview

The TOE is NetMotion Mobility XE 9.5, which is a standards-compliant, client/server-based software VPN that securely extends the enterprise network to the mobile environment. Using Mobility XE™, TCP/IP network applications 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 server relays data to the new location, even if it is on a different subnet or a different network. Mobility XE addresses the problems of slow, unreliable, insecure links over IP-based wireless wide area networks, adding features that include bandwidth optimizations, compression, and encryption.

Mobility XE also extends the centralized system management capabilities of wired networks to wireless connections, integrating with existing network security. It provides console applications and metrics that a system administrator can use to configure and manage remote connections, and troubleshoot remote connection problems.

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.

1.7 TOE Description

1.7.1 Physical Boundary

The TOE is a software TOE and is defined as the Mobility XE 9.5. In order to comply with the evaluated configuration, the following components must be used:

COMPONENT	VERSION/MODEL NUMBER
Software	Version 9.5 (Client and Server) Build Number 42566
Hardware (IT Environment)	• Table 4 – Server Component Requirements • Table 5 – Client Platform Hardware Requirements

Table 3 – Evaluated Configuration for the TOE

The TOE interfaces comprise the following:

1. Network interfaces that pass traffic and enforce flow control policy

2. Management interface through which to handle administrative actions

The TOE boundary is shown below:

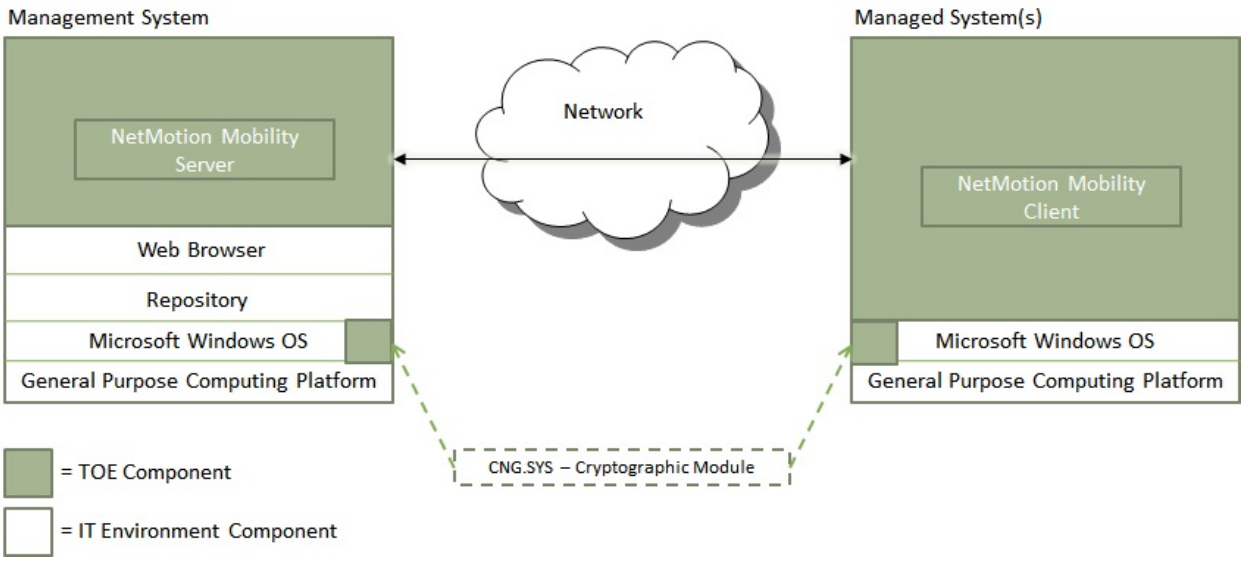

Figure 1 – TOE Boundary

The TOE is comprised of the base NetMotion Mobility Server and the CNG.SYS cryptographic module from the Microsoft operating systems. Add-on functionality such as the Policy Management Module, Network Access Control Module, and Analytics Module is not included in the scope of the evaluation. Please note that use of these add-on modules are allowed in the evaluated configuration and do not impact the evaluated features, but the features of those add-ons is not evaluated.

1.7.2 Hardware and Software Supplied by the IT Environment

The TOE consists of a set of software applications. The hardware, operating systems and all third-party support software (e.g., DBMS) on the systems on which the TOE executes are excluded from the TOE boundary.

The TOE requires the following hardware and software configuration on the management platform (i.e., server).

COMPONENT	MINIMUM REQUIREMENTS
Processor	x64-compatible dual-core processor, 2.0 GHz
Memory	4 GB RAM
Free Disk Space	20 GB
Monitor	1024x768, 256-color, VGA monitor or higher
Operating System	Windows Server 2008 R2 SP1 Windows Server 2008 R2

COMPONENT	MINIMUM REQUIREMENTS
DBMS	Oracle Directory Server Enterprise Edition 11g Release 1 (11.1.1)
Additional Software	• Internet Explorer® 8 or 9 • Firefox® 3.5 or later
Network Card	Ethernet, 100Mb or higher
Disk Partition Formats	NTFS

Table 4 – Server Component Requirements

The minimum hardware requirements for the Mobility Client platforms are specified in the following table:

COMPONENT	MINIMUM HARDWARE REQUIREMENTS
Processor	x64 processors supported by the operating system
Memory	At least the minimum supported by the Operating System
Free Disk Space	30 MB
Monitor	1024x768, 256-color, VGA monitor or higher
Operating System	Windows 7 (64-bit Ultimate Edition) SP1 Windows 7 (64-bit Ultimate Edition)
Additional Software	• Internet Explorer® 8 or 9 • Firefox® 3.5 or later

Table 5 – Client Platform Hardware Requirements

1.7.3 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

TSF	DESCRIPTION
Security Audit	The TOE generates audit records for security events. The administrator and read-only operator are the only roles with access to the audit trail and have the ability to view the audit trail.
Cryptographic Support	The TOE supports secure communications between TOE components. This encrypted traffic prevents modification and disclosure of user information. The cryptographic module fulfills the requirements of FIPS 140-2 Overall Level 1.
User Data Protection	The TOE provides an information flow security policy. The security policy limits traffic to resource types to specific user roles.
Identification	All users are required to perform identification before any information flows are permitted. Additionally, administrators must be identified before performing any administrative functions.
Security Management	The TOE provides a wide range of security management functions. Administrators can configure the TOE, manage users, the information flow policy, and audit among other routine maintenance activities.
Protection of the TSF	The TOE provides a secure connection between users and peer devices. Traffic is protected from disclosure and modification. Audit data is timestamped.

Table 6 – Logical Boundary Descriptions

1.7.3.1 TOE Guidance

The following guidance documentation will be provided as part of the TOE:

- *Operational User Guidance and Preparative Procedures Supplement: NetMotion Mobility XE 9.5.*

1.7.3.2 Excluded Functionality

In the evaluated configuration, the Event Viewer is excluded from the TOE for both the Client and Server.

2 Conformance Claims

2.1 CC Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 conformant and Part 3 conformant at Evaluation Assurance Level 4 and augmented by ALC_FLR.1 – Basic Flaw Remediation.

2.2 PP Claim

The TOE does not claim conformance to any registered Protection Profile.

2.3 Package Claim

The TOE claims conformance to the EAL4 assurance package defined in Part 3 of the Common Criteria Version 3.1 Revision 3 (July 2009). The TOE does not claim conformance to any functional package.

2.4 Conformance Rationale

No conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to modify the behavior of TSF data without being detected.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.OLDINF	An unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information or information properties sent between distributed components of the TOE.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.

Table 7 – Threats Addressed by the TOE

The IT Environment addresses the following threat:

THREAT	DESCRIPTION
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

Table 8 – Threats Addressed by the IT Environment

3.2 Organizational Security Policies

The TOE is not required to meet any organizational security policies.

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.PHYSEC	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.PUBLIC	The TOE does not host public data.
A.TIME	The TOE can receive time data from a reliable source.
A.SECCOMM	The communications between the TOE and external IT services is secured.

Table 9 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes.
O.ENCRYP	The TOE must protect the confidentiality of its dialogue between distributed components.
O.IDENTIFY	The TOE must be able to identify users prior to allowing access to TOE functions and data on the management system.
O.MEDIAT	The TOE must mediate the flow of all information from users on an external network to resources on an internal network, and must ensure that residual information from a previous information flow is protected and not transmitted in any way.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.SECKEY	The TOE must provide the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt traffic flows.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.

Table 10 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.ADMTRA	Authorized administrators are trained to appropriately install, configure, and maintain the TOE within its evaluated configuration according to the installation and guidance documents for the TOE.
OE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
OE.PHYSEC	Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from any physical attack.
OE.PUBLIC	The TOE does not host public data.

OBJECTIVE	DESCRIPTION
OE.IDAUTH	The Operational Environment must be able to identify and authenticate users prior to them gaining access to TOE functionality on the managed system. It must also be able to authenticate user credentials on the management system when requested by the TOE.
OE.TIME	The Operational Environment will provide reliable timestamps for the TOE.
OE.SECCOMM	The Operational Environment will protect the communications between the TOE and IT servers.
OE.NOEVENT	The Operational Environment will prohibit the use of the Event Viewer.

Table 11 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

THREATS/ ASSUMPTIONS / OBJECTIVES	T.AUDACC	T.MEDIAT	T.NOAUTH	T.OLDINF	T.PROCOM	T.SELPRO	A.NOEVIL	A.PHYSEC	A.TIME	A.PUBLIC	A.SECCOMM
O.ACCOUN	✓										
O.AUDREC	✓										
O.ENCRYP					✓						
O.IDENTIFY			✓								
O.MEDIAT		✓		✓							
O.SECFUN			✓								
O.SECKEY					✓						
O.SECSTA						✓					
OE.ADMTRA							✓				
OE.GUIDAN							✓				
OE.PHYSEC								✓			
OE.PUBLIC										✓	
OE.IDAUTH			✓								
OE.TIME									✓		
OE.SECCOMM											✓
OE.NOEVENT	✓										

Table 12 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

4.3.1.1 Rationale for Security Threats to the TOE

THREAT	RATIONALE
T.AUDACC	This threat is completely countered by • O.ACCOUN which ensures the TOE provides user accountability for information flows through the TOE and for Administrator use of security functions related to audit. • O.AUDREC which ensures The TOE provides a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes
T.MEDIAT	This threat is completely countered by • O.MEDIAT which ensures the TOE mediates the flow of all information from users on an external network to resources on an internal network
T.NOAUTH	This threat is completely countered by • O.IDENTIFY which ensures the TOE uniquely identifies the claimed identity of all users before granting a user access to TOE functions. • O.SECFUN which provide functionality that enables an authorized administrator to use the TOE security functions, and ensures that only authorized administrators are able to access this functionality. • OE.IDAUTH which provides for authentication of users prior to any TOE data access.
T.OLDINF	This threat is completely countered by • O.MEDIAT which ensures that residual information from a previous information flow is protected and not transmitted
T.PROCOM	This threat is completely countered by • O.ENCRYP which ensures the TOE protects the confidentiality of its dialogue between distributed TOE components • O.SECKEY which ensures the TOE provides the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt traffic flows
T.SELPRO	This threat is completely countered by • O.SECSTA which ensures the TOE does not compromise its resources or those of any connected network upon initial start-up or recovery from an interruption in TOE service

Table 13 – Mapping of Objectives to Threats

4.3.1.2 Rationale for Security Objectives of the TOE

OBJECTIVE	RATIONALE
O.ACCOUN	This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows as well as management function.
O.AUDREC	This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search the information contained in the audit trail.

OBJECTIVE	RATIONALE
O.ENCRYP	This security objective is necessary to counter the threat T.PROCOM by requiring the TOE to protect the confidentiality of communications between distributed TOE components.
O.IDENTIFY	This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.
O.MEDIAT	This security objective is necessary to counter the threats: T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.
O.SECFUN	This security objective is necessary to counter the threat T.NOAUTH by requiring that the TOE provides functionality that ensures that only authorized users have access to the TOE security functions.
O.SECKEY	The objective mitigates the threat of data modification or disclosure by ensuring that cryptographic keys are generated sufficiently, kept confidential, and destroyed property (T.PROCOM)
O.SECSTA	This security objective ensures that no information is comprised by the TOE upon startup or recovery and thus counters the threat T.SELPRO.
OE.ADMTRA	This non-IT security objective is necessary to counter the threat T.TUSAGE and support the assumption A.NOEVIL because it ensures that authorized administrators receive the proper training in the correct configuration, installation and usage of the TOE.
OE.GUIDAN	The objective to deliver, install, administer, and operate the TOE in a manner that maintains security.(A.NOEVIL)
OE.PHYSEC	The objective to provide physical protection for the TOE supports the assumption that the TOE will be located within controlled access facilities, which will prevent unauthorized physical access (A.PHYSEC).
OE.PUBLIC	The TOE does not host public data. (A.PUBLIC)
OE.IDAUTH	The objective to identify and authenticate users prior to them gaining access to TOE functionality on the managed system. It must also be able to authenticate user credentials on the management system when requested by the TOE. (T.NOAUTH)
OE.TIME	The Operational Environment provides a reliable time source to the TOE (A.TIME).
OE.SECCOMM	The Opearational Environment provides secured communications between the TOE and IT servers.
OE.NOEVENT	The Operational Environment provides protection against access to audit records.

Table 14 – Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

5.1 Definition of Extended Components

There are no extended components in this Security Target.

6 Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1	Cryptographic Operation
User Data Protection	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
Identification and Authentication	FIA_UID.2	User identification before any action
Security Management	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection

Table 15 – TOE Security Functional Requirements

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 – Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [*not specified*] level of audit; and

c) [The events in column two of Table 16 – Auditable Events]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column two of Table 16 – Auditable Events].

SFR	EVENT	DETAILS
FIA_UID.2	All use of the user identification mechanism	None
FCS_COP.1	When an encrypted session is established	The identity of the User performing the action
FDP_IFF.1	All decisions on requests for information flow	The presumed addresses of the source and destination subject

Table 16 – Auditable Events

6.1.1.2 FAU_SAR.1 – Audit Review

FAU_SAR.1.1 The TSF shall provide [an Administrator and Operator] with the capability to read [all audit information] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1 – Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [NIST Special Publication 800-56a] and specified cryptographic key sizes [128-, 192-, or 256-bit AES key] that meet the following: [FIPS 197 for AES].

6.1.2.2 FCS_CKM.4 – Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite] that meets the following: [Federal Information Processing Standard 140 requirements for key zeroization].

6.1.2.3 FCS_COP.1 – Cryptographic Operation

FCS_COP.1.1 The TSF shall perform [the operations described below] in accordance with a specified cryptographic algorithm [multiple algorithms in the modes of

operation described below] and cryptographic key sizes [multiple key sizes described below] that meet the following: [multiple standards described below].

OPERATION	ALGORITHM (MODE)	KEY SIZE IN BITS	CAVP CERTIFICATE	STANDARDS
Encryption and Decryption	AES	128, 192, 256	1168, 1178, 1187	FIPS 197
Hashing	SHA-1 SHA-256 SHA-384 SHA-512	160 256 384 512	1081	FIPS 180-3
Random Number Generation	FIPS 186-2	Not Applicable	649	Digital Signature Standard (DSS), Appendix 3.1

Table 17 – Cryptographic Operations

6.1.3 Information Flow Control (FDP)

6.1.3.1 FDP_IFC.1 – Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [Secure Flow Control SFP] on [

Subjects: unauthenticated external IT entities that send and receive packets over a protected network through the TOE,

Information: connection state

Operations: tunnel, bypass, not connected].

6.1.3.2 FDP_IFF.1 – Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [Secure Flow Control SFP] based on the following types of subject and information security attributes: [

Subject security attributes:

- identity

Information security attributes:

- Connect, disconnect, unreachable, reachable, roaming].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:[

- The client successfully identifies and has permission].

FDP_IFF.1.3 The TSF shall enforce the [No additional rules].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [No additional rules].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [

- If a client does not support the encryption method set on the server, it cannot connect and posts a message in the client event log OR
- If a client accepts the requested encryption method, but then tries to establish an unencrypted connection or a connection using a different encryption method, the Mobility Client will be disconnected automatically and posts a warning in the server event log.
- If the administrator changes the server setting to add a new version of CNG.SYS to the list of certified modules, the new setting will not be effective until Clients reconnect. The administrator can then disconnect of all Clients and force them reconnect using the new setting.

].

6.1.4 Identification and Authentication (FIA)

6.1.4.1 FIA_UID.2 – User Identification before Any Action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.5 Security Management (FMT)

6.1.5.1 FMT_MTD.1 – Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to **control** the [data described in the table below] to [the roles specified]:

DATA	CHANGE DEFAULT	QUERY	MODIFY	DELETE	CLEAR
Secure Flow Control SFP	A	A O	A	A	
Audit Logs		A O			A
User Account Attributes		A O	A	A	

Table 18 – Management of TSF data (A = Admin O = Operator)

6.1.5.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

a) Start-up and shutdown;

b) Create, delete, modify, and view information flow security policy rules that permit or deny information flows;

c) Query, modify, and delete users and user account attributes;

d) Review the audit trail].

6.1.5.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Administrator, Operator and End User].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.6 Protection of the TSF (FPT)

6.1.6.1 FPT_ITT.1 – Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure* **and** *modification* when it is transmitted between separate parts of the TOE.

6.2 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon, and any necessary rationale.

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_GEN.1	No other components	FPT_STM.1	Satisfied (FPT_STM.1 dependency satisfied by IT Environment's provision of time)
FAU_SAR.1	No other components	FAU_GEN.1	Satisfied
FCS_CKM.1	No other components	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Satisfied by FCS_COP.1 and FCS_CKM.4
FCS_CKM.4	No other components	FDP_ITC.1 or FDP_IDC.2 or FCS_CKM.1	Satisfied by FCS_CKM.1
FCS_COP.1	No other components	FDP_ITC.1 or FDP_IDC.2 or FCS_CKM.1 FCS_CKM.4	Satisfied by FCS_CKM.1 and FCS_CKM.4
FDP_IFC.1	No other components	FDP_IFF.1	Satisfied
FDP_IFF.1	No other components	FDP_IFC.1 FMT_MSA.3	Satisfied[1]
FIA_UID.2	FIA_UID.1	None	n/a
FMT_MTD.1	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied
FMT_SMF.1	No other components	None	n/a
FMT_SMR.1	No other components	FIA_UID.1	Satisfied by FIA_UID.2, which is hierarchical
FPT_ITT.1	No other components	None	n/a

Table 19 – TOE SFR Dependency Rationale

6.3 Security Assurance Requirements

The Security Assurance Requirements for this evaluation are listed in Table 23 – Security Assurance Measures.

[1] FMT_MSA.3 does not impact the security required by FDP_IFF.1 for this particular TOE because there are no configurable security attributes.

6.4 Security Requirements Rationale

6.4.1 Security Functional Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

SFR \ OBJECTIVE	O.IDENTIFY	O.MEDIAT	O.SECSTA	O.SECKEY	O.ENCRYP	O.AUDREC	O.ACCOUN	O.SECFUN
FAU_GEN.1						✓	✓	
FAU_SAR.1						✓		
FCS_CKM.1				✓				
FCS_CKM.4				✓				
FCS_COP.1					✓			
FDP_IFC.1		✓						
FDP_IFF.1		✓						
FIA_UID.2	✓						✓	
FMT_MTD.1	✓	✓	✓		✓			✓
FMT_SMF.1								✓
FMT_SMR.1								✓
FPT_ITT.1					✓			

Table 20 – Mapping of TOE Security Functional Requirements and Objectives

6.4.2 Sufficiency of Security Requirements

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

SFR	RATIONALE
FAU_GEN.1	This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.
FAU_SAR.1	This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.
FCS_CKM.1	This component ensures that cryptographic keys and parameters are generated with standards-based algorithms (O.SECKEY).
FCS_CKM.4	This component ensures that the cryptographic keys and parameters are safely destroyed when their lifetime ends or when the Administrator forces generation of new keys. Keys are zeroized in accordance with FIPS 140-2 specifications (O.SECKEY).

SFR	RATIONALE
FCS_COP.1	This component ensures that when all users communicate with the TOE remotely from an internal or external network, robust algorithms are used to encrypt such traffic. This component traces back to and aids in meeting the following objective: O.ENCRYP.
FDP_IFC.1	This component identifies the entities involved in the Secure Information Flow SFP. This component traces back to and aids in meeting the following objective: O.MEDIAT.
FDP_IFF.1	This component identifies the attributes of the users sending and receiving the information in the Secure Information Flow SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.
FIA_UID.2	This component requires successful identification of a role before having access to the TSF and as such aids in meeting O.IDENTIFY and O.ACCOUN.
FMT_MTD.1	This component restricts the ability to modify the Secure Information Flow SFP, and as such aids in meeting O.ENCRYP, O.MEDIAT, O.SECSTA, and O.SECFUN. This component restricts the ability to modify identification and authentication data, and as such aids in meeting O.IDENTIFY, O.MEDIAT, O.SECSTA, and O.SECFUN. This component restricts the ability to modify the data relating to TOE access locations, and as such contributes to meeting O.MEDIAT, O.SECSTA, and O.SECFUN.
FMT_SMF.1	This component was chosen in an attempt to consolidate all TOE management/administration/security functions. This component traces back to and aids in meeting the following objective: O.SECFUN.
FMT_SMR.1	This component ensures that roles are available to allow for varying levels of administration capabilities and restricts access to perform TSF-relevant functionality depending on the role assigned to an authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.
FPT_ITT.1	This component works with the encryption provided in the FCS_COP.1 requirement to ensure that traffic transmitted between the server and client are protected from disclosure and modification. This component traces back to and aids in meeting the following objective: O.ENCRYP.

Table 21 – Rationale for TOE SFRs to Objectives

The following table presents a mapping of the rationale of TOE Objectives to Security Requirements:

OBJECTIVE	RATIONALE
O.ACCOUN	This objective is completely satisfied by • FAU_GEN.1 which outlines what events must be audited. • FIA_UID.2 ensures that users are identified to the TOE.
O.AUDREC	This objective is completely satisfied by • FAU_GEN.1 which outlines what events must be audited. • FAU_SAR.1 which requires that the audit trail can be read.

OBJECTIVE	RATIONALE
O.ENCRYP	This objective is completely satisfied by • FCS_COP.1 which ensures robust algorithms are used to support encrypted communications between users and the TOE. • FMT_MTD.1 which restricts the ability to change default, query, modify, delete the Secure Flow Control SFP, restricts the ability to query audit logs, and restricts the ability to query, modify, or delete user account attributes. All restrictions apply to unauthenticated or unauthorized users. • FPT_ITT.1 which ensures all communications between TOE components is encrypted via a secure connection using encryption & decryption algorithms.
O.IDENTIFY	This objective is completely satisfied by • FIA_UID.2 which ensures that users are identified to the TOE. • FMT_MTD.1 which restricts the ability to change default, query, modify, delete the Secure Flow Control SFP, restricts the ability to query audit logs, and restricts the ability to query, modify, or delete user account attributes. All restrictions apply to unauthenticated or unauthorized users.
O.MEDIAT	This objective is completely satisfied by • FDP_IFC.1 which ensures the TOE supports an information flow policy that controls who can send and receive network traffic. • FDP_IFF.1 which ensures Secure Information Flow SFP limits information flow based on user roles and resource types. • FMT_MTD.1 which restricts the ability to change default, query, modify, delete the Secure Flow Control SFP, restricts the ability to query audit logs, and restricts the ability to query, modify, or delete user account attributes. All restrictions apply to unauthenticated or unauthorized users.
O.SECFUN	This objective is completely satisfied by • FMT_MTD.1 which restricts the ability to modify the Secure Information Flow SFP. • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based.
O.SECKEY	This objective is completely satisfied by • FCS_CKM.1 which ensures that cryptographic keys and parameters are generated with standards-based algorithms. • FCS_CKM.4 which ensures that the cryptographic keys and parameters are safely destroyed.
O.SECSTA	This objective is completely satisfied by • FMT_MTD.1 which restricts the ability to change default, query, modify, delete the Secure Flow Control SFP, restricts the ability to query audit logs, and restricts the ability to query, modify, or delete user account attributes. All restrictions apply to unauthenticated or unauthorized users.

Table 22 – Rationale for TOE Objectives to SFRs

6.4.3 Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 4 augmented with ALC_FLR.1: Basic Flaw Remediation. EAL4 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL4 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited and purpose-built interface.

6.4.4 Security Assurance Requirements and Associated Evidence

This section identifies the measures applied to satisfy CC assurance requirements. There are no explicitly defined assurance components.

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_ARC.1 Security Architecture Description	Security Architecture: NetMotion Mobility XE 9.5
ADV_FSP.4 Complete Functional Specification	Functional Specification: NetMotion Mobility XE 9.5
ADV_IMP.1 Implementation Representation of the TSF	Basic Modular Design: NetMotion Mobility XE 9.5
ADV_TDS.3 Basic Modular Design	Basic Modular Design: NetMotion Mobility XE 9.5
AGD_OPE.1 Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: NetMotion Mobility XE 9.5
AGD_PRE.1 Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: NetMotion Mobility XE 9.5
ALC_CMC.4 Production support, acceptance procedures and automation	Configuration Management Processes and Procedures: NetMotion Mobility XE 9.5
ALC_CMS.4 Problem tracking CM coverage	Configuration Management Processes and Procedures: NetMotion Mobility XE 9.5
ALC_DEL.1 Delivery Procedures	Secure Delivery Processes and Procedures: NetMotion Mobility XE 9.5
ALC_DVS.1 Identification of security measures	Security Measures: NetMotion Mobility XE 9.5
ALC_LCD.1 Developer defined life-cycle model	Product Development Lifecycle Model: NetMotion Mobility XE 9.5
ALC_FLR.1 Basic Flaw Remediation	Basic Flaw Remediation: NetMotion Mobility XE 9.5
ALC_TAT.1 Well-defined development tools	Configuration Management Processes and Procedures: NetMotion Mobility XE 9.5
ATE_COV.2 Analysis of Coverage	Testing Evidence Supplement: NetMotion Mobility XE 9.5
ATE_DPT.1 Testing: Basic Design	Testing Evidence Supplement: NetMotion Mobility XE 9.5
ATE_FUN.1 Functional Testing	Testing Evidence Supplement: NetMotion Mobility XE 9.5

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ATE_IND.2 independent Testing – Sample	Produced by Common Criteria Testing Laboratory
AVA_VAN.3 Focused Vulnerability Analysis	Produced by Common Criteria Testing Laboratory

Table 23 – Security Assurance Measures

7 TOE Summary Specification

This section presents the Security Functions implemented by the TOE.

7.1 TOE Security Functions

The security functions performed by the TOE are as follows:

- Security Audit
- Cryptographic Operations
- User Data Protection
- Identification
- Security Management
- Protection of the TSF

7.2 Security Audit

The TOE generates a fine-grained set of audit logs, as described in the table below:

STATE	DESCRIPTION
Connect	A Mobility client connected to the Mobility server. Displays the date and time the connection was made, unique device identifier, user name, virtual IP address, and point-of-presence IP address of the network interface that established the connection.
Disconnect	A Mobility client bypassed the Mobility server, the system administrator disconnected the client from the Mobility console, or a user logged off or shut down the client operating system. If the **Activity Logging - Statistics** setting is enabled, a statistics event follows. Displays the date and time the disconnect occurred, unique device identifier, user name, and reason for disconnect.

STATE	DESCRIPTION
Unreachable	The Mobility server could not reach a client device that was connected to the server. An unreachable state occurs when a client's network connection fails or the device goes out of coverage and no other network is available, the device goes into standby or hibernation, or the server receives no confirmation from the client device that it must disconnect from the server. The **Timeout - Client Unreachable** setting determines the amount of time the server allows to elapse before it logs the client as unreachable. Displays the date and time the server determined the client was unavailable, the unique device identifier, and the user name.
Reachable	A Mobility client that was unreachable resumes communication. Displays the date and time the communication was reestablished, unique device identifier, and user name.
Roaming	A Mobility client's point-of-presence IP address changes. Examples include changes to network type (Ethernet, 802.11, WWAN) or subnet. Displays the date and time the connection change was made, unique device identifier, user name, virtual IP address, point-of-presence address of the network interface to which the client roamed, and the cumulative byte count since authentication up to the time the client roamed.
Statistics	When the **Activity Logging - Statistics** setting is enabled, logs the number of inbound and outbound bytes transmitted between a client's connect event and disconnect event. Displays the date and time the event was posted, unique device identifier, user name, connection length in dd:hh:mm, and the number of bytes sent and received during that connection period.

Table 24 – Audit Log: States and Descriptions

The TOE generates Local Logs for the following list of events:

- All use of the user identification mechanism.
- All decisions on requests for information flow.
- When an encrypted session is established.
- Startup and shutdown of audit function (instantiated through startup/shutdown of TOE).

The logs are accessible through the web-based administrative interface, which only authorized operators can access. The log files are also physically available on the disk environment. The web-based administrative interface is on the same PC.

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE generates all the audit events identified in this requirement. Within each event is the information listed above which addresses all required details.
- FAU_SAR.1: The Administrator has the ability to read all of the audit logs. Each log is presented to the administrator in a human-readable format.

7.3 Cryptographic Support

The TOE provides an encrypted path between separate components (i.e., Client and Server). The client and server communicate via a secure connection using the AES encryption algorithm implemented by the TOE. The secure connection ensures that user data are protected from modification and disclosure when transmitted between separate parts of the TOE (client and server). A FIPS 140-2 Level 1 validated cryptographic module performs cryptographic operations. The following table details the applicable FIPS 140-2 validations.

CMVP Cert #	Platform	Description	Cert Date
1328	Microsoft Windows 7 Ultimate Edition (x64 version)	Microsoft Windows 7 Kernel Mode Crypto Library (cng.sys)	6/1/2011
1335	Microsoft Windows Server 2008 R2 SP1 (x64 version)	Microsoft Windows Server 2008 R2 Kernel Mode Cryptographic Primitives Library (cng.sys)	6/21/2011

The Cryptographic Support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1: This component ensures that cryptographic keys and parameters are generated with standards-based algorithms.
- FCS_CKM.4: This component ensures that the cryptographic keys and parameters are safely destroyed when their lifetime ends or when the Administrator forces generation of new keys.
- FCS_COP.1: Robust algorithms are used to support encrypted communications between users and the TOE.

7.4 User Data Protection

The TOE enforces an information flow policy between TOE components. These policies determine whether the Mobility Client can access data and resources on an internal, protected network.

Once the client is successfully identified and authenticated, a secure tunnel is established to the server. There are two other client connection states:

1. Loopback traffic need not be sent through the Mobility server. To accommodate this, traffic on any interface for remote address 127.0.0.1 is passed directly to the local IP stack.
2. The Mobility client sends traffic destined for local applications simultaneously through Mobility XE and in local passthrough mode. If the Mobility client is running a server application, like a local web server, local application traffic is passed through Mobility XE to connect to the local server.

These implicit rules (pass through loopback, split local traffic, allow everything else) can be considered default Mobility XE behavior. Client connection to the server will be denied if a client does not support the encryption method set on the server or if a client accepts the requested encryption method but then tries to establish an unencrypted connection or a connection using a different encryption method, the Mobility server disconnects the session.

The User Data Protection function is designed to satisfy the following security functional requirements:

- FDP_IFC.1: The TOE supports a secure information flow policy that controls who can send and receive network traffic.
- FDP_IFF.1: The Secure Information Flow SFP limits information flow based on policy compliance. Administrators have the ability to establish rules that permit or deny information flows based on the combination of attributes listed.

7.5 Identification

The TOE performs identification of all operators and administrators accessing the TOE. The TOE accepts a username and password combination and forwards these credentials to a remote authentication mechanism (i.e., NTLM, ActiveDirectory, smart cards) within the IT Environment.

The Identification function is designed to satisfy the following security functional requirement:

- FIA_UID.2: The TOE requires a user name during the identification and authentication process. The username is entered, then a password. If the password is validated by the IT Environment, the user will be associated with a role and set of privileges based on the username.

7.6 Security Management

The TOE provides security management functions via a browser interface. The Administrator logs onto the TOE locally and performs all management functions through the browser interface. The Administrator has the ability to control all aspects of the TOE configuration including: user management, information flow policy management, audit management, and system start-up and shutdown.

The following account types are available on the Mobility console.

- Administrator group—Members of the group selected as an Administrator group have full access to the Mobility console, and can perform such administrative tasks as changing server and client settings, creating and applying client policies, or creating and applying network access control rule sets. By default, this is set to the Administrators group. Note that the ST refers to this user role as Administrator.
- Operator group—Members of the group selected as an Operator group can connect to the Mobility console and perform management tasks, such as monitoring server and client status, generating reports, or reviewing activity logs. They cannot modify server or client settings, client policies, or network access control rule sets. To restrict Mobility console access to administrators, set the Operator group to None.

The table below further describes the options available to the Administrator role:

OPTION	DESCRIPTION
Configure	Adds the selected user to the Client Settings page, where you can configure user settings. The user appears with the icon in the user list.
Clear Settings	Removes any user-specific settings for the selected user (but not global settings), and removes the user from the Client Settings page.
Quarantine	Changes status of selected users to the quarantined state. The Mobility server quarantines users the next time they attempt to connect. The server does not terminate existing connections but the quarantined device cannot establish a new connection. The device appears with an icon on the Users page. To immediately terminate an existing connection and prevent a device from reconnecting, apply quarantine from the Connection List page.
Clear Quarantine	Removes the selected user from quarantine and allows him or her to connect to a Mobility server.
Add Users	Opens the Add Users page, where you can add users to the User page display. This lets you configure user settings or assign users to user groups before the user connects to a Mobility server for the first time. Adding a user to the Mobility console does not allow the user to authenticate to a Mobility server and establish a connection. To allow new users access to Mobility XE services, add them to the appropriate global domain user group, the local NetMotion Users group, or to the RADIUS authentication database.
Remove Users	Removes a user from the User page display. It does not terminate any existing connections and does not prevent the user from connecting to a Mobility server.

OPTION	DESCRIPTION
Join group	This drop-down list shows the names of existing user groups. Selecting a user from the list and clicking OK adds the selected user to the group.

Table 25 – Administrator Privileges

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MTD.1: The TOE restricts the ability to change default, query, modify, delete the Secure Flow Control SFP, restricts the ability to query and clear audit logs, and restricts the ability to query, modify, or delete user account attributes. All restrictions apply to unauthenticated or unauthorized users.
- FMT_SMF.1: The TOE supports the following security management functions:

  a) start-up and shutdown of The TOE;
  b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;
  c) query, modify, and delete users and user account attributes;
  d) archive, clear, and review the audit trail.

- FMT_SMR.1: The TOE supports the roles administrator and operator. The administrator role can perform all management functionalities available from within the administrator console. An operator can monitor server and client status, generate reports, or review activity log

7.7 Protection of the TSF

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_ITT.1: All communications between TOE components is encrypted via a secure connection using encryption & decryption algorithms defined in FCS_COP.1. This protects the traffic from disclosure and modification.