Windows Mobile 6.5

Security Target

EAL4 augmented with ALC_FLR.1

Version 1.0

January 2010

Document History

Version	Date	Author	Description
1.0	10-Jan-10	Ben Bromhead	Release version.

Table of Contents

List of Figures

List of Tables

1 ST Introduction

1.1 TOE type and usage

1 The Target of Evaluation (TOE), Windows Mobile 6.5, is a compact operating system for use on Pocket PCs and Smartphones, enabling users to securely extend their corporate Windows desktop to mobile devices.

2 Windows Mobile 6.5 provides the basis for establishing a secure enterprise mobile messaging solution that can securely synchronize and access Line of Business (LOB) applications and services, including Microsoft Exchange to access email, contacts, tasks and calendar and other corporate applications that may be only accessible from within the enterprise network.

3 Windows Mobile powered devices can be centrally managed through the System Center Mobile Device Manager (SCMDM). Windows Mobile 6.5 supports the standards needed to allow the client to establish an authenticated and encrypted communications channel to MDM Gateway Server for enterprise management.

4 The inclusion of the SCMDM client application in Windows Mobile 6.5 provides a security management platform for Windows Mobile phones with over 130 policies and settings and built-in mechanisms that help prevent the misuse of corporate data. Enterprise Administrators can lock down many areas of the Windows Mobile Smartphones, including certain communications and device functionality, while exercising significant control over the software to be installed on devices.

5 Windows Mobile 6.5 has a seamless user experience across cellular or Wi-Fi data connections to the enterprise network. SCMDM provides a single point for security–enhanced, behind-the-firewall access to corporate data and LOB applications for Windows Mobile. Enterprise Administrators can facilitate security over public wireless networks through a Mobile VPN link. The VPN link secures wireless communications between the Windows Mobile 6.5 powered mobile device and corporate servers through an SSL–encrypted tunnel.

6 Figure 1illustrates the claimed security functionality for Windows Mobile.

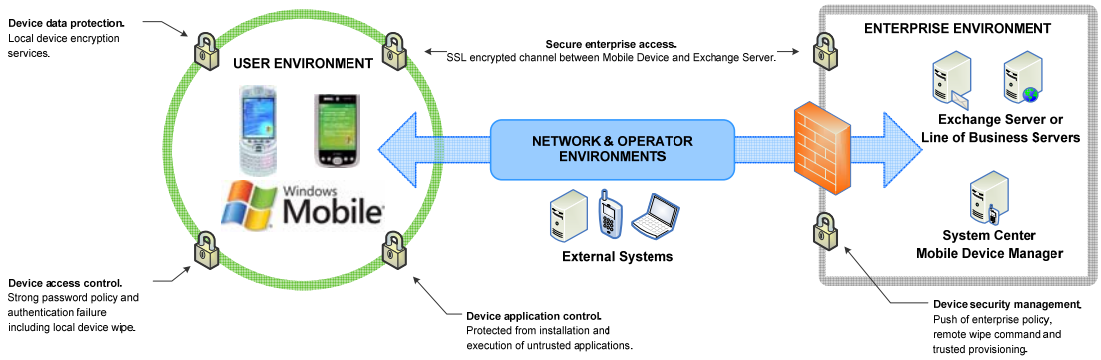

Figure 1– Windows Mobile 6.5 security architecture

1.2 TOE security features

7 Table 1 provides the set of claimed security features that are included within scope of the Common Criteria EAL4+ evaluation of Windows Mobile 6.5.

Table 1 – Windows Mobile security features

Security function	TOE security feature
Device data protection. The TOE provides the capability to protect data at rest.	**Sensitive Data Protection.** The TOE supports 128-bit AES encryption of data stored locally on the Mobile Device and also on removable storage cards.
	S/MIME support. The TOE provides additional protection features for e-mail messages, whether in transit between device and server or at rest.
	Certified cryptographic module. The TOE includes a FIPS validated cryptographic module enabling applications to make use of inbuilt cryptographic operations.
Secure enterprise access. The TOE provides the capability to securely connect trusted enterprise assets and facilitate secure data transfer.	**SSL/TLS channel encryption.** The TOE supports SSL/TLS encryption enabling sensitive data to be transmitted between the device and server, over-the-air or through a wired connection.
	Mobile VPN. Incorporating secure key exchange (IKEv2), an IPSec VPN tunnel can be established between the TOE and the enterprise gateway, providing protection for information communicated between the TOE and Line of Business (LOB) servers within the trusted enterprise.
	Enterprise Authentication. The TOE provides the capability to support enterprise authentication mechanisms.
Device application control. The TOE provides the capability to control the installation and execution of applications on the Mobile Device.	**Controlled application installation.** The TOE can be configured to only permit applications signed with a trusted certificate to be installed on the Mob le Device.
	Controlled application execution. The TOE implements code execution control to only permit applications signed with a trusted certificate to be executed on the Mobile Device.

Security function	TOE security feature
Device access control. The TOE has capability to provide controlled access to information and functionality of the Mobile Device.	**Device authentication and lock.** The TOE implements functionality that requires the Mobile User to enter a password to gain access to the Mobile Device.
	Local device wipe. The TOE can be configured to perform a local device wipe after a specified number of incorrect login attempts by the Mobile User on the Mobile Device.
	Trusted provisioning. The TOE implements protection mechanisms to ensure that provisioning and configuration data can only be accepted by the Mobile Device from a trusted source.
Device security management. The TOE has configurable security and management policies that enable enterprise management of the Mobile Device.	**Security roles and policies.** The TOE maintains multiple management roles and implements a suite of security policies which determine access to resources on the Mobile Device.
	Remote wipe. The TOE can be configured to accept a command from a management server to remotely wipe the Mobile Device.
	Device management policies. The TOE supports a range of mobile device management capabilities which can be instilled by the Enterprise Administrator through Server Center Mobile Device Manager (SCMDM) 2008.

1.3 ST and TOE identification

Table 2 – ST and TOE identification information

ST Title	Windows Mobile 6.5Security Target
ST Version	1.0, 10-JAN-10
TOE Software	Windows Mobile Version 6.5, which includes the following editions: Standard andProfessional. This evaluation includes the following Adaptation Kit Updates (AKUs): • Build 21849 (AKU 5.0.63) • Build 21854 (AKU 5.0.80)
Assurance Level	EAL4 augmented with ALC_FLR.1
CC Identification	Common Criteria for Information Technology (IT) Security Evaluation, Version 3.1, Revision 3, incorporating: • Part One – Introduction and General Model, Revision Three, July 2009; • Part Two – Security Functional Components, Revision Three, July 2009; and • Part Three – Security Assurance Components, Revision Three, July 2009. International Standard – International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 15408:1999.

1.4 Conformance claims

8 The following conformance claims are made for the TOE and ST:

a) **Part 2extended.**Extends Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1, Revision 3.

b) **Part 3 conformant, EAL4 augmented.** Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, Revision 3. Evaluation is EAL4 augmented with ALC_FLR.1.

1.5 Document conventions

9 Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

a) **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

b) **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

c) **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

d) **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

1.6 Terminology

Table 3 – Terminology

Term	Description
Active Directory	Active Directory is a Microsoft directory service. It supports a single unified view of objects on a network and allows locating and managing resources faster and easier.
Application Revocation List	The TOE maintains a list of applications that have been revoked. The Security Loader module will check this list before making a decision about permitting the install or execution of an application.
Applications	End-user applications that make use of either the voice or data services offered by the TOE.
Authenticated Channel	Assured identification of the end points of a communications channel.
Authentication	The process of determining whether someone or something is, in fact, who or what it is declared to be.

Term	Description
Authentication Data	Information used to verify the claimed identity of a user.
Credentials	Credentials include identifying attributes and associated authentication data that is used to validate requests authentication requests.
Device Identity	A unique identifier that exists for the Mobile Device.
Device Lock	The local lock of a device to end a session. Local device authentication is required to unlock the Mobile Device.
Device Manager	A term used within the Open Mobile Alliance to specify the server that can provide OMA-DM messages to the Mobile Device.
Device Resources	Those components of a mobile device that can be accessed and utilized by executable code to run processes and perform functions.
Enterprise Administrator	The role used to describe the enterprise IT administrator responsible for establishing security policies for Mobile Devices.
Enterprise Data	Data that resides in Line of Business (LOB) systems within the Enterprise Environment that can be communicated to Mobile Devices. Once communicated to and stored on Mobile Devices, enterprise data is considered user data.
Enterprise Exchange Server	The Microsoft Exchange Server used within the enterprise to communicate with Mobile Devices as a LOB Server.
Enterprise User Identifier	The alias used by the Mobile User to access the corporate network.
Exchange ActiveSync	Exchange ActiveSync is an Exchange synchronization protocol designed for keeping an Exchange mailbox synchronized with a Windows Mobile device. The protocol is based on HTTP, SSL/TLS, and XML and is a part of Exchange Server.
Executable Code	A file whose contents are meant to be interpreted as a program by the mobile device. Will contain the binary representation of machine instructions of the specific processor of the mobile device.

Term	Description
Local Device Wipe	The wipe of TOE Security Function (TSF) and user data in response to reaching the threshold for failed authentication attempts.
Mailbox Items	Items that can be synchronized through Exchange ActiveSync such as emails, contacts, tasks and calendar appointments.
Mobile Device	The physical device, either Smartphone or Pocket PC, that provides the hardware platform for the installation of the Windows Mobile 6.5 operating system and additional OEM applications and services.
Mobile Device Authentication	The local entry of a password by the user to gain access to the Mobile Device.
Mobile Operator	The entity that provides the network infrastructure for the Mobile Device to communicate with other devices and the enterprise network.
Mobile User	The authorized individual in control of the Mobile Device.
Object	An entity within the TSF Scope of Control (TSC) that contains or receives information and upon which subjects perform operations.
OMA-CP	Open Mobile Alliance Client Provisioning. A one way protocol that provides a WAP push and is typically used for bootstrapping.
OMA-DM	Open Mobile Alliance Device Management. A protocol designed for management of small mobile devices such as mobile phones, PDAs and palm top computers. OMA-DM provides continuous provisioning that modifies the device configuration settings when necessary and can be repeated on multiple occasions.
Provisioning	The act of configuring the Mobile Device including both enabling or disabling of features. Provisioning can be performed Over the Air (OTA) or locally via installation of an appropriately formed provisioning file.
Push Proxy Gateway	A WAP Push Proxy is a gateway intended to provide push connectivity between wired and wireless networks.

Term	Description
Remote Device Wipe	The wipe of TSF and user data in response to a command from System Center Mobile Device Manager.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
SystemCenter Mobile Device Manager (SCMDM)	An enterprise product for managing policies and device settings for mobile devices.
Secure Channel	Assured identification of the end points of a communication channel and protection of the channel data from modification or disclosure.
Secure Sockets Layer (SSL)	A protocol that supplies secure data communication through data encryption and decryption. SSL enables communications privacy over networks.
Security Policies	Used to configure security settings that are then enforced with the help of security roles and certificates. Security policies enforce security requirements for all OTA data messages that a Mobile Device receives.
Security Roles	Used to allow or restrict access to Windows Mobile powered device resources. The security role is based on the message origin and how the message is signed.
Sensitive Data Protection (SDP)	Used to protect information stored locally on the Mobile Device through the use of 128-bit AES encryption.
Service Indicator	An SI message can be sent by the Mobile Operator to notify users of new services, service updates, and provisioning services. The TOE can be configured to reject SI messages.
Service Loader	An SL message can be sent by the Mobile Operator to provision the Mobile Device. The TOE can be configured to reject SL messages.
Subject	An entity within the TSC that causes operations to be performed.
Trusted IT Product	A TOE that has been evaluated against the requirements of the Common Criteria.

Term	Description
Trusted Provisioning Server	The TPS is a source of provisioning information that can be trusted by a Mobile Device.

10

1.7 Document organization

11 This document is organized into the following sections:

a) Section 1 provides the introductory material for the ST.

b) Section 2 provides the TOE description and includes the physical and logical scope of the TOE.

c) Section 3 describes the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented within the TOE or through environmental controls.

d) Section 4 defines the security objectives for the TOE and environment.

e) Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively that must be satisfied by the TOE.

f) Section 6 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE and also the assurance measures designed to meet the assurance requirements.

g) Section 7 provides a rationale to explicitly demonstrate that security objectives have been satisfied by the TOE.

2 TOE Description

2.1 Physical scope of the TOE

12 Windows Mobile 6.5is a single user operating system designed for use with Smartphone and Pocket PC devices. The intended method of use of the TOE is as an operating system for integration into a mobile messaging device. The integrated operating system and device will provide a mobile messaging solution for mobile users that can be managed within the enterprise through Microsoft's System Center Mobile Device Manager 2008 (SCMDM 2008).

13 The TOE operates in a specific operational environment, the ***user environment***, and is supported by capabilities that exist within the ***network/operator***and ***enterprise environments***.The relationships between the TOE and relevant elements within each of the operating environments are depicted in Figure 2 below.

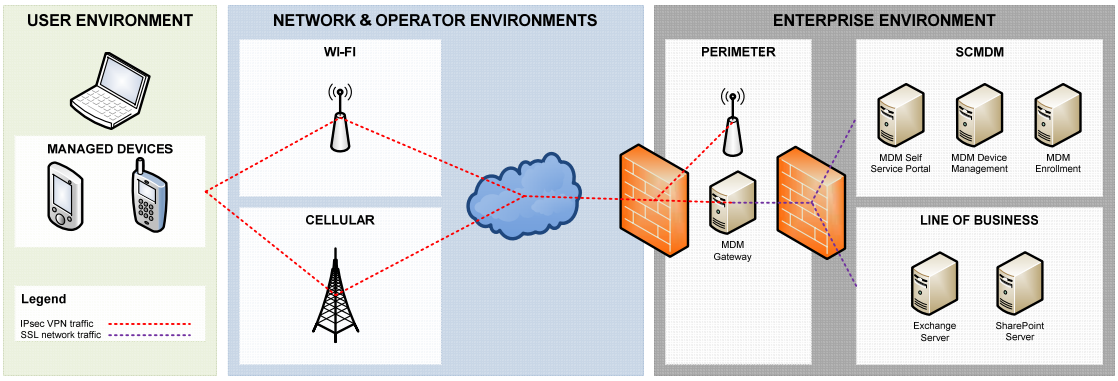

Figure 2 – The TOE operating environment

2.1.1 User environment

14 The Mobile Device is the hardware upon which the TOE operates. It is used for mobile communications in variable locations such as would be expected with a mobile phone.

15 Windows Mobile 6.5 provides the basis for the TOE. This is a single user operating system and includes a suite of services and functions that provides Window Mobile powered devices with a set of security functionality as specified in this ST.

16 The manufacturers of mobile devices that install and employ the Windows Mobile 6.5operating system for their devices, often include additional applications and services that are specific to their devices and service offerings.

17 Each Mobile Device also has specific hardware and drivers that have been developed for interfacing with the operator environment and general network infrastructure.

2.1.2 Operator & network environments

18 The operator environment is provided and controlled by the Mobile Operator. The Mobile Operator provides the cellular network connectivity and related services.

19 The Mobile Device is also capable of communicating with other devices and systems using a range of communication mechanisms, including WAP, Wi-Fi and voice. The Mobile Device is free to use general networking capabilities to communicate with external systems and the corporate network.

2.1.3 Enterprise environment

20 Users can use the TOE to gain access to resources residing on corporate networks through two secure communication methods; using an SSL/TLS encrypted channel, or a Mobile VPN. These provide communications security allowing for the following:

a) Policy data to be sent by an Enterprise Administrator to the TOE utilizing System Center Mobile Device Manager (SCMDM). SCMDM is outside of the scope of this evaluation, and is employed to provide the remote configuration and management of security and operational policies.

b) Communication between the TOE and Line of Business servers via an enterprise link established with the SCMDM.

21 Communication between the TOE and other components within the enterprise environment are mediated by another trusted IT product, a communications proxy, which provides the access point for the enterprise. The communications proxy does not form part of the TOE, however, it does provide the capability for the TOE to establish a trusted communications channel over which user and security policy data can be transferred.

22 The proxy is an integrated edge security gateway that can act as a cryptographic termination point and provide firewall functionality. The proxy also provides the Point of Presence at which the Mobile Device must have a URL so that connectivity can be provided back to the enterprise network.

23 Active Directory also plays a role in a managed Windows Mobile solution as it provides authentication services for supplied user credentials or digital certificates that are provided by the Mobile User through the Mobile Device.

2.2 Logical scope of the TOE

24 The TOE comprises the core software components of Windows Mobile 6.5operating system. Windows Mobile is an operating system that installs on a Mobile Device which incorporates hardware and firmware components. Additionally, mobile applications are installed on the Windows Mobile operating system and utilize the services of the TOE.

25 Windows Mobile 6.5 is available on a variety of devices from a variety of manufacturers and Mobile Operators. The claimed security functionality of the TOE is standard across all types of devices, from Pocket PCs to Smartphones, regardless of which model or device that the operating system is installed on.

26 The Mobile Device itself is not part of the TOE. The TOE communicates with several other physically separate components within the IT Environment, and these again do not form part of the TOE as they are within a trusted IT environment.

27 In the evaluated configuration, all communication between the TOE, System Center Mobile Device Manager and any LOB servers are mediated by the Communications Proxy or the Enterprise Gateway. Both of these mediation services are provided by trusted IT products that is used to establish a trusted path for the secure communication of both TSF and user data.

28 Figure 3illustrates the TOE boundary and the scope of the evaluation.

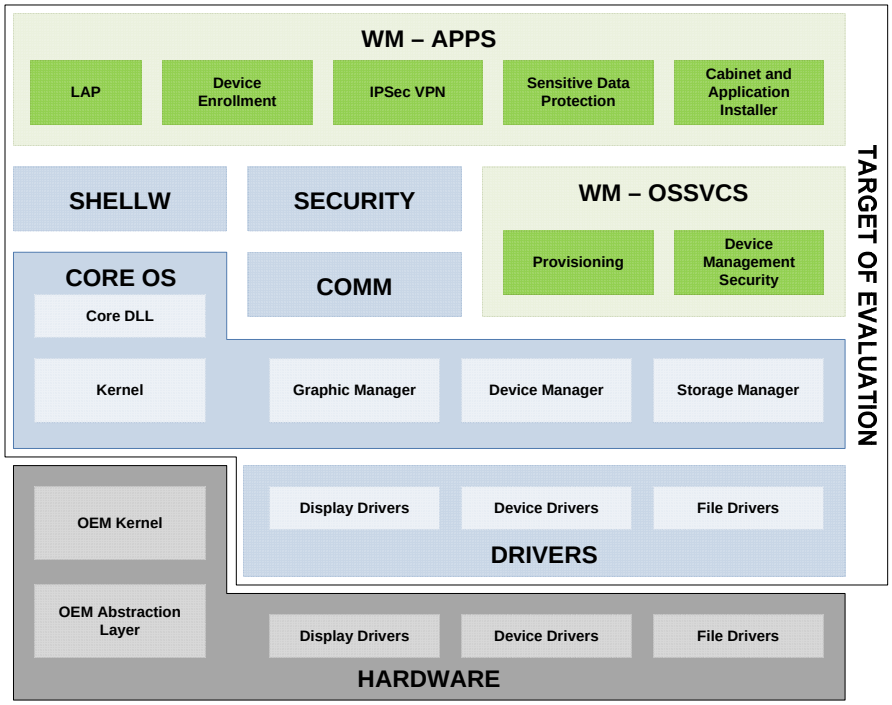

Figure 3 – TOE scope

3 Security Problem Definition

3.1 Overview

29 This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through assumptions about the security aspects of the environment and any threats to the assets that the TOE will be providing protection.

3.2 Assumptions

Table 4 – Assumptions

Identifier	Assumption statement
A.USAGE	Mobile Users are trusted to: a) follow user guidance, b) ensure that the TOE continues to operate in the evaluated configuration, c) only permit ActiveSync connections between the Mobile Device and trusted computing devices, and d) store the Mobile Device when not in use in a physically protected area that is appropriate for the information processed by the TOE.
A.DELIVERY	The security enforcing components of the TOE will not be modified by either the Mobile Operator or the manufacturer of the Mobile Device during the delivery process.
A.IT_ENTERPRISE	The Active Directory Server and all LOB Servers are located within the enterprise boundary and are protected from unauthorized logical/physical access.
A.ADMIN	The Enterprise Administrator is not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by administrator documentation.
A.I&A_ENTERPRISE	The IT environment will provide mechanisms for authenticating Mobile Users when accessing their mailbox and other resources within the corporate network.
A.COMMS_ENT	The IT environment will provide the server-side of a secure channel between the System Center Mobile Device Manager and LOB Servers and the Mobile Device.

Identifier	Assumption statement
A.SEC_POLICY	The IT environment will implement System Center Mobile Device Manager formanaging devices and establishing enterprise policy.

3.3 Threats

Table 5 – Threats to security

Identifier	Threat statement
T.EAVESDROPPING	An attacker may compromise the confidentiality of user, enterprise TSF data by monitoring communications between the TOE and SCMDM or LOB Servers.
T.INTERCEPT	An attacker may compromise the integrity of user, enterprise or TSF data by intercepting and altering communications between the TOE and andSCMDM or LOB Servers.
T.IMPORT	An administrator or user may inadvertently import malicious code to the TOE, resulting in a compromise of the confidentiality, integrity and/or availability of user, enterprise and/or TSF data.
T.MASQUERADE	An attacker may masquerade as the managing SCMDM instance and attempt to compromise the integrity of the TSF by sending malicious management messages to the TOE.
T.MISCONFIGURE	A user may inadvertently compromise the integrity of the TOE through the manipulation of Windows Mobile settings and configurations.
T.TOE_ACCESS	An attacker may gain direct access to a Mobile Device if it is not in the control of the Mobile User enabling compromise of the confidentiality of user or TSF data contained on the Mobile Device.
T.SC_ACCESS	An attacker may gain direct access to a Mobile Device if it is not in the control of the Mobile User enabling removal of any inserted removable storage card to compromise the confidentiality of stored user or TSF data.
T.WEAK_SECRET	A user may select a weak password thereby enabling an attacker to compromise the confidentiality of userdata.

4 Security Objectives

4.1 Overview

30 The security objectives are concise statements of the TOE's response to the security problem. Some objectives are to be achieved through the security functionality of the TOE and some elements of the problem will be addressed through the establishment of a secure environment in which the TOE must operate.

4.2 Security objectives for the TOE

Table 6 – Security objectives for the TOE

Identifier	Objective statement
O.COMMS_CONF	The TOE shall preserve the confidentiality of user, enterprise and TSF data transmitted between the TOE and SCMDM and LOB Servers.
O.COMMS_INT	The TOE shall preserve the integrity of user, enterprise and TSF data transmitted between the TOE and SCMDM and LOB Servers.
O.CODE_CTRL	The TOE shall prevent the installation and execution of code that has not been explicitly authorized.
O.MGMT_AUTH	The TOE shall ensure that management messages have originated from a trusted source.
O.USER_AUTH	The TOE shall prevent users from requesting access to applications or data prior to authentication.
O.REMOTE_ADMIN	The TOE shall perform administrative actions as directed by the Enterprise Administrator.
O.SECRET	The TOE shall be capable of not allowing the use of weak secrets.
O.REMOTE_WIPE	The TOE shall be capable of responding to a command from the administrator to wipe all TSF data and make user data inaccessible.
O.LOCAL_WIPE	The TOE shall be able to make user and TSF data inaccessible in response to a defined consecutive number of failed authentication attempts.
O.ROLES	The TOE will maintain a number of roles to distinguish access to functions of the TOE.

Identifier	Objective statement
O.DATA_ENCRYPT	The TOE shall be capable of securing user and/or TSF data stored on the mobile device, as well as on removable storage card media.
O.SESSION_LOCK	The TOE shall lock itself after an administrator defined period of inactivity, or in response to a user initiated request. The user shall be required to re-authenticate in order to request access to data or applications, however, users must be capable of using general phone features and making an emergency call.
O.MANAGEMENT	The TOE shall be capable of having security policy settings defined by an Enterprise Administrator, which cannot be modified or overwritten by Mobile Users.

4.3 Security objectives for the environment

Table 7 – Security objectives for the IT environment

Identifier	Objective statement
OE.I&A_ENTERPRISE	The IT environment must authenticate Mobile Users prior to providing access to enterprise resources.
OE.COMMS_ENT	The IT environment must authenticate the end-points and encrypt communications between the Mobile Device and SCMDM and LOB Servers
OE.SEC_POLICY	The IT environment must implement SCMDM for managing and securing mobile devices.

4.4 Security objectives for the non-IT environment

Table 8 – Security objectives for the non-IT environment

Identifier	Objective statement
OE.USAGE	The Enterprise Administrator shall ensure that Mobile Users are aware of the need to: a) follow user guidance relating to the operating system, installed applications and the Mobile Device; b) ensure that the TOE continues to operate in the evaluated configuration and that if their device is reset there may be a need to re-provision the Mobile Device into the evaluated configuration; c) only permit ActiveSync connections between their Mobile Device and computing devices that can be trusted; and d) store the Mobile Device when not in use in a physically protected area that is appropriate for the information processed by the TOE.
OE.DELIVERY	The Device Manufacturer and Mobile Operator shall not modify the security enforcing components of the TOE during the delivery process.
OE.IT_ENTERPRISE	The Enterprise Administrator shall ensure that the Active Directory Server and LOB Servers are protected from unauthorized logical and physical access.
OE.ADMIN	The Enterprise Administrator shall not be careless, willfully negligent, or hostile, and shall follow and abide by the instructions provided by the administrator documentation.

5 IT Security Requirements

5.1 Overview

31 This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

5.2 TOE security functional requirements

32 This section contains the security functional components from part 2 of the Common Criteria with the operations completed.

33 Standard Common Criteria text is in regular black font and the text inserted to perform an operation on the requirement is in accordance with the conventions specified in section 1.5 of this ST.

Table 9 – Summary of TOE Security Functional Requirements

Identifier	Title
FCS_CKM.1	Cryptographic key generation
FCS_COP.1a	Cryptographic operation (SSL/TLS)
FCS_COP.1b	Cryptographic operation (S/MIME)
FCS_COP.1c	Cryptographic operation (Removable storage card)
FCS_COP.1d	Cryptographic operation (Sensitive data protection)
FCS_COP.1e	Cryptographic operation (Mobile VPN)
FCS_CKM.4	Cryptographic key destruction
FDP_ACC.1a	Subset access control (Device Application Control SFP)
FDP_ACF.1a	Security attribute based access control (Device Application Control SFP)
FDP_IFC.1	Subset information flow control (Secure Enterprise Access SFP)
FDP_IFF.1	Simple security attributes (Secure Enterprise Access SFP)
FTP_ITC.1	Inter-TSF trusted channel
FDP_ACC.1b	Subset access control (Device Configuration Control SFP)

Identifier	Title
FDP_ACF.1b	Security attribute based access control (Device Configuration Control SFP)
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication
FIA_UAU.7	Protected authentication feedback
FTA_SSL.1.EX	TSF-initiated session lock
FTA_SSL.2.EX	User-initiated locking
FMT_MOF.1a	Management of security functions behaviour (Device Data Protection)
FMT_MSA.1a	Management of security attributes (Device Application Control SFP)
FMT_MSA.1b	Management of security attributes (Secure Enterprise Access SFP)
FMT_MSA.1c	Management of security attributes (Device Configuration Control SFP)
FMT_MOF.1b	Management of security functions behaviour (Device Access Control)
FMT_MSA.3a	Static attribute initialisation (Device Application Control SFP)
FMT_MSA.3b	Static attribute initialisation (Secure Enterprise Access SFP)
FMT_MSA.3c	Static attribute initialisation (Device Configuration Control SFP)
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles

5.2.1

5.2.2 FCS_CKM.1 Cryptographic key generation

Hierarchical to:	No other components.
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**a) RSA,** **b) 3DES, and** **c) AES**] and specified cryptographic key sizes [**a) 384through to a maximum 16384 bits (RSA)** **b) 168 bits (3DES), and** **c) 128 and 256 bits (AES)**] that meet the following: [**a) RFC 2437 "PKCS #1: RSA Cryptography Specifications Version 2.0", October 1998;** **b) Federal Information Processing Standard (FIPS) Publication 46-3, "Data Encryption Standard", 25 October 1999; and** **c) Federal Information Processing Standard (FIPS) Publication 197, "Advanced Encryption Standard (AES)", 26 November 2001**].
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.2.3 FCS_COP.1a Cryptographic operation (SSL/TLS)

Hierarchical to:	No other components.
FCS_COP.1a.1	The TSF shall perform [**encryption, decryption and digital signing for LOBand Trusted Provisioningcommunications**] in accordance with a specified cryptographic algorithm [**a) RSA,** **b) 3DES,** **c) AES, and** **d) SHA-1**] and cryptographic key sizes [**a) 384 through to a maximum of 16384 bits (RSA),** **b) 168 bits (3DES),** **c) 128 and 256 bits (AES), and** **d) N/A (SHA-1)**] that meet the following: [**a) RFC 2437 "PKCS #1: RSA Cryptography Specifications Version 2.0", October 1998;** **b) Federal Information Processing Standard (FIPS) Publication 46-3, "Data Encryption Standard", 25 October 1999;** **c) Federal Information Processing Standard (FIPS) Publication 197, "Advanced Encryption Standard (AES)", 26 November 2001, and** **d) Federal Information Processing Standard (FIPS) Publication 180-1, "Secure Hash Algorithm", 17 April 1995**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.2.4 FCS_COP.1b Cryptographic operation (S/MIME)

Hierarchical to:	No other components.
FCS_COP.1b.1	The TSF shall perform [**encryption, decryption and digital signing for securing email messages**] in accordance with a specified cryptographic algorithm [**a) RSA,** **b) 3DES, and** **c) SHA-1**] and cryptographic key sizes [**a) 384 through to a maximum of 16384 bits (RSA),** **b) 168 bits (3DES), and** **c) N/A (SHA-1)**] that meet the following:[**a) RFC 2437 "PKCS #1: RSA Cryptography Specifications Version 2.0", October 1998;** **b) Federal Information Processing Standard (FIPS) Publication 46-3, "Data Encryption Standard", 25 October 1999;** **c) Federal Information Processing Standard (FIPS) Publication 180-1, "Secure Hash Algorithm", 17 April 1995**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.2.5 FCS_COP.1c Cryptographic operation (Removable storage card)

Hierarchical to:	No other components.
FCS_COP.1c.1	The TSF shall perform [**encryption and decryption of data residing on removable storage card**] in accordance with a specified cryptographic algorithm [**AES**] and cryptographic key sizes [**128 bits**] that meet the following: [**Federal Information Processing Standard (FIPS) Publication 197, "Advanced Encryption Standard (AES)", 26 November 2001**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.2.6 FCS_COP.1d Cryptographic operation (Sensitive data protection)

Hierarchical to:	No other components.
FCS_COP.1d.1	The TSF shall perform [**encryption and decryption of data residing on the Mobile Device**] in accordance with a specified cryptographic algorithm [**AES**] and cryptographic key sizes [**128 bits**] that meet the following: [**Federal Information Processing Standard (FIPS) Publication 197, "Advanced Encryption Standard (AES)", 26 November 2001**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.2.7 FCS_COP.1e Cryptographic Operation (Mobile VPN)

Hierarchical to:	No other components.
FCS_COP.1e.1	The TSF shall perform [**encryption, decryption and digital signing for Mobile VPN**] in accordance with a specified cryptographic algorithm [**a) RSA,** **b) 3DES,** **c) AES, and** **d) SHA-1**] and cryptographic key sizes [**a) 384 through to a maximum of 16384 bits (RSA),** **b) 168 bits (3DES),** **c) 128 and 256 bits (AES), and** **d) N/A (SHA-1)**] that meet the following: [**a) RFC 2437 "PKCS #1: RSA Cryptography Specifications Version 2.0", October 1998;** **b) Federal Information Processing Standard (FIPS) Publication 46-3, "Data Encryption Standard", 25 October 1999;** **c) Federal Information Processing Standard (FIPS) Publication 197, "Advanced Encryption Standard (AES)", 26 November 2001, and** **d) Federal Information Processing Standard (FIPS) Publication 180-1, "Secure Hash Algorithm", 17 April 1995**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.2.8 FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**the CryptDestroyKey and CryptAcquireContext cryptographic key zeroization operation**] that meets the following: [**FIPS 140-1 or 140-2 Level 1**].
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Notes:	All keys are destroyed and their memory location zeroized when the CryptDestroyKey is called on the provided key handle. Private keys are destroyed when CryptAcquireContext is called.

5.2.9 FDP_ACC.1a Subset access control (Device Application Control SFP)

Hierarchical to:	No other components.
FDP_ACC.1a.1	The TSF shall enforce the [**Device Application Control SFP**] on [**a) Subjects:** **i. Cabinets (cab and cpffile extension),** **ii. Themes (hme and tsk file extensions),** **iii. Dynamic Link Libraries (dllfile extensions), and** **iv. Executables (exe file extensions).** **b) Objects:** **i. Device resources.** **c) Operations:** **i. Install an application (Cabinet or Theme) on the TOE, and** **ii. Execute an application (DLL or Executable) on the TOE**].
Dependencies:	FDP_ACF.1 Security attribute based access control
Notes:	The Device Application Control SFPspecifies the rules for implementing controls associated with installing and executing applications. This SFR identifies the four file types that are controlled under this policy, to include all files that can be executed on the TOE, executables and

	dynamic link libraries, and all files that can be used to install new applications or themes onto the Mobile Device.

5.2.10 FDP_ACF.1a Security attribute based access control (Device Application Control SFP)

Hierarchical to:	No other components
FDP_ACF.1a.1	The TSF shall enforce the [**Device Application Control SFP**] to objects based on the following: [**a) All subjects:** **i. Developer name, and** **ii. Digital signature.** **b) Device resources** **i. Object identifier**].
FDP_ACF.1a.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**a) All attempts to install an application (Cabinet or Theme) on the TOE:** **i. Cabinet or Theme files digitally signed with a certificate that exists in the SPC certificate store are permitted to access device resources and install on the TOE.** **ii. Unsigned Cabinet or Theme files require permission from the Mobile User to access devices resources and install on the TOE.** **iii. Cabinet or Themefilesdigitally signed with an invalid certificate require permission from the Mobile User to access device resources and install on the TOE.** **b) All attempts to execute an application (Executables or DLLs)on the TOE:** **i. Executables or DLLs digitally signed with a certificate that exists in the Privileged Execution Trust Authorities certificate store are permitted to access device resources and executeon the TOE.** **ii. Unsigned Executables or DLLs will require permission from the Mobile User to access device resources and executeon the TOE.** **iii. Executables or DLLs digitally signed with an invalid certificate will require permission from the Mobile User to access device resources and execute on the TOE.**].

FDP_ACF.1a.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**a) Executable code that resides in Read Only Memory (ROM) is permitted to execute without a digital signature**].
FDP_ACF.1a.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules[**a) If the application attempting to execute or install is listed in the Application Revocation List on the TOE**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Notes:	The Mobile Device must be configured correctly to implement the Device Application Control SFP as described above. To control the installation of applications on the TOE the following security policies must be appropriately applied: • Unsigned Themes Policy (SECPOLICY_UNSIGNEDTHEMES) • Unsigned CABS Policy (SECPOLICY_UNSIGNEDCABS) • Unsigned Prompt Policy (SECPOLICY_UNSIGNEDPROMPT) • Unsigned Applications Policy (SECPOLICY_UNSIGNEDAPPS) The correct application of these policies to enforce the Device Application Control SFP is described in the Windows Mobile 6.5 guidance documentation.

5.2.11 FDP_IFC.1Subset information flow control (Secure Enterprise Access SFP)

Hierarchical to:	No other components
FDP_IFC.1.1	The TSF shall enforce the [**Secure Enterprise Access SFP**] on [**a) Subjects:** **i. Mobile Device,** **ii. SCMDM, and** **iii. LOB Servers.** **b) Information:** **i. SCMDM policies,** **ii. Software Packages, and**

	iii. LOB Enterprise Data. **c) Operations:** **i. Access LOB Servers,** **ii. Receive Remote Wipe Command,** **iii. Receive SCMDM Policy, and** **iv. Receive Software Packages**].
Dependencies:	FDP_IFF.1 Simple security attributes
Notes:	The Secure Enterprise Access SFP demonstrates that the Mobile Device communicates securely with enterprise resources for a number of different types of information exchanges. The Mobile Device can synchronize data items contained in the Mobile Users enterprise mailbox, items such as email, calendar, tasks, contacts, and files. The Enterprise Administrator can also configure security and operational policies through SCMDM. The Mobile Device can connect to Line of Business servers within the organization to facilitate the transfer of data specific to applications residing on the Line of Business server.

5.2.12 FDP_IFF.1Simple security attributes (Secure Enterprise Access SFP)

Hierarchical to:	No other components
FDP_IFF.1.1	The TSF shall enforce the [**Secure Enterprise Access SFP**] based on the following types of subject and information security attributes: [**a) Mobile Device:** **i. the enterprise root CA certificate, and** **ii. Private key and the associated Mobile Device certificate.** **b) SCMDM:** **i. the enterprise root CA certificate, and** **ii. Private key and the associated SCMDM Server certificate.** **c) LOB Servers:** **i. User enterprise authentication data, and** **ii. Private key and the associated LOB Server certificate**].
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: [**a) Access by the Mobile Device to a LOB Server is permitted if:** **i. the Mobile Device and SCDMDM Gateway Server have mutually authenticated,** **ii. an active IPsec VPN session has been established between the SCMDM Gateway Server and the Mobile Device, and** **iii. an SSL session has been established between the Mobile Device and the LOB Server.** **b) Receipt of a Remote Wipe Command by the Mobile Device is permitted if:** **i. the Mobile Device and SCDMDM Gateway Server have mutually authenticated,** **ii. an active IPsec VPN session has been established between the SCMDM Gateway Server and the Mobile Device, and** **iii. an SSL session has been established between the Mobile Device and the MDM Device Management Server.** **c) Receipt of SCMDM Policy is permitted if:** **i. the Mobile Device and SCDMDM Gateway Server have mutually authenticated,** **ii. an active IPsec VPN session has been established between the SCMDM Gateway Server and the Mobile Device, and** **iii. an SSL session has been established between the Mobile Device and the MDM Device Management Server.** **d) Receipt of Software Packages is permitted if:** **i. the Mobile Device and SCDMDM Gateway Server have mutually authenticated,** **ii. an active IPsec VPN session has been established between the SCMDM Gateway Server and the Mobile Device, and** **iii. an SSL session has been established between the Mobile Device and the MDM Device Management Server**].
FDP_IFF.1.3	The TSF shall enforce the [**None**].
FDP_IFF.1.4	The TSF shall explicitly authorise an information flow based on the following rules: [**None**].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [**None**].

Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization
Notes:	This policy reflects access to the Mobile Device from the perspective of the enterprise environment. Therefore, authentication of the device/user to LOB servers is not covered. The focus is on the enterprise providing correct credentials to the device to allow enterprise communications.

5.2.13 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to:	No other components.
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit [***the TSF***] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for **[** **a) receiving SCMDM policies,** **b) receiving software packages,** **c) communicating with LOB servers, and** d) **receiving a remote wipe command]**.
Dependencies:	No dependencies.
Notes:	SCMDM is also an evaluated product and is used to provide the communications endpoint for all interactions with the enterprise environment.

5.2.14 FDP_ACC.1b Subset access control (Device Configuration Control SFP)

Hierarchical to:	No other components.
FDP_ACC.1b.1	The TSF shall enforce the [**Device Configuration Control SFP**] on [**a) Subjects:** **i. Mobile Operator (SECROLE_OPERATOR),**

	ii. **Trusted Provisioning Server (SECROLE_OPERATOR_TPS),** iii. **Manager (SECROLE_MANAGER),** iv. **Enterprise Administrator (SECROLE_ENTERPRISE),** v. **Authenticated User (SECROLE_USER_AUTH), and** vi. **Unauthenticated User (SECROLE_USER_UNAUTH)** b) **Objects:** i. **Configuration Service Providers** c) **Operations:** i. **Query device configuration, and** ii. **Modify device configuration**].
Dependencies:	FDP_ACF.1 Security attribute based access control
Notes:	None.

5.2.15 FDP_ACF.1b Security attribute based access control (Device Configuration Control SFP)

Hierarchical to:	No other components.
FDP_ACF.1b.1	The TSF shall enforce the [**Device Configuration Control SFP**] to objects based on the following: [a) **All subjects:** i. **Security role** b) **All objects:** i. **Access privilege**].
FDP_ACF.1b.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [a) **Querying the configuration of the Mobile Device will be permitted if the security role associated with the requesting subject has the read access privilege for the relevant Configuration Service Provider being accessed.** b) **Modification of Mobile Device configuration will be permitted if the security role associated with the requesting subject has write access privilege for the relevant Configuration Service Provider**].
FDP_ACF.1b.3	The TSF shall explicitly authorise access of subjects to objects based on

	the following additional rules: [**a) If a subject has been granted the Manager role (SECROLE_MANAGER) through the Grant Manager Policy then the associated security role will be granted the same privileges as that of Manager**].
FDP_ACF.1b.4	The TSF shall explicitly deny access of subjects to objects based on the [**None**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
Notes:	None.

5.2.16 FIA_AFL.1 Authentication failure handling

Hierarchical to:	No other components.
FIA_AFL.1.1	The TSF shall detect when [**an Enterprise Administrator configurable positive integer within** [**1 through 4294967295**]] unsuccessful authentication attempts occur related to [**Mobile Device Authentication**].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**perform a local wipe of all TSF and user data**].
Dependencies:	FIA_UAU.1 Timing of authentication
Notes:	The Enterprise Administrator has the ability to configure the device to perform a secure wipe of the device once the threshold for unsuccessful device authentication attempts has been met. This is configurable through SCMDM policy.

5.2.17 FIA_ATD.1 User attribute definition

Hierarchical to:	No components.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual **Mobile Device** users: [**a) Mobile Device Identifier,** **b) Mobile Device User Authentication Data,** **c) LOB Authentication Data,**

	d) SCMDM Gateway Address **e) SCMDM Gateway Certificate, and** **f) User's Email Address**].
Dependencies:	No dependencies.
Notes:	As Windows Mobile 6.5 is a single-user operating system there is no concept of a user identifier.

5.2.18 FIA_SOS.1 Verification of secrets

Hierarchical to:	No other components.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet **the following quality checks for Mobile Device User Authentication:**[**a) must include both alpha and numeric characters,** **b) must not contain a repeating predictable sequence,** **c) must contain a configurable minimum number of characters (as specified by the Enterprise Administrator), and** **d) must be different from a configurable number of previous passwords (as specified by the Enterprise Administrator)**].
Dependencies:	No dependencies.
Notes:	While the TOE has the mechanisms to implement the above quality checks for secrets, these settings are configurable by the policies set through SCMDM. The Windows Mobile 6.5 guidance documentation includes details for establishing the appropriate device management policies.

5.2.19 FIA_UAU.1 Timing of authentication

Hierarchical to:	No other components.
FIA_UAU.1.1	The TSF shall allow [**the** **a) display of message status,** **b) display of missed call status,** **c) display of time/date information,** **d) display of Mobile Device status information,** **e) display of Mobile User information,**

	f) display of notifications, **g) conduct of an emergency call,** **h) receipt of an incoming call,** **i) receipt of an incoming text message, and** **j) receiptof the Remote Wipe Command from SCMDM**] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	The TOE must be capable of presenting status details and to perform a number of communications without an active user session.

5.2.20 FIA_UAU.7 Protected authentication feedback

Hierarchical to:	No other components.
FIA_UAU.7.1	The TSF shall provide only [**a) a single asterix (*) per authentication character typed;** **b) the number of incorrect authentication attempts;** **c) a prompt to enter a confirmation string, after an Enterprise Administrator configurable number of missed authentication attempts; and** **d) a warning for the last possible authentication attempt prior to device wipe**] to the user while the authentication is in progress.
Dependencies:	FIA_UAU.1 Timing of authentication
Notes:	The prompting for the entry of a confirmation string after a number of failed attempts is designed to prevent the device from being accidentally wiped by inadvertent key presses. The correct entry of the confirmation string is not considered to be a correct authentication attempt nor is the incorrect entry of the string considered a failed authentication attempt.

5.2.21 FTA_SSL.1-EX TSF-initiated session locking

Hierarchical to:	No other components.

FTA_SSL.1-EX.1	The TSF shall lock an interactive session after [**a period of inactivity specified by the Enterprise Administrator through applied SCMDM policy**] by a) locking the display and only displaying notifications and/or status information permitted by FIA_UAU.1, and b) disabling any activity of the current user session other than activities permitted by FIA_UAU.1 and unlocking the session.
FTA_SSL.1-EX.2	The TSF shall require the following events to occur prior to unlocking the session: [**successful Mobile Device Authentication**].
Dependencies:	FIA_UAU.1 Timing of authentication
Notes:	This setting is configurable by the Enterprise Administrator and is specified through SCMDM.

5.2.22 FTA_SSL.2-EX User-initiated locking

Hierarchical to:	No other components.
FTA_SSL.2-EX.1	The TSF shall allow user-initiated locking of the user's own interactive session, by a) locking the display and only displaying notifications and/or status information permitted by FIA_UAU.1, and b) disabling any activity of the current user session other than activities permitted by FIA_UAU.1 and unlocking the session.
FTA_SSL.2-EX.2	The TSF shall require the following events to occur prior to unlocking the session: [**successful Mobile Device Authentication**].
Dependencies:	FIA_UAU.1 Timing of authentication
Notes:	None.

5.2.23 FMT_MOF.1a Management of security functions behaviour(Device Data Protection)

Hierarchical to:	No other components.
FMT_MOF.1a.1	The TSF shall restrict the ability to [**enable, disable or modify the behaviour of**] the functions [**related to managing the Device Data Protection function**] to [**Manager (SECROLE_MANAGER)**].
Dependencies:	FMT_SMR.1 Security roles

	FMT_SMF.1 Specification of Management Functions
Notes:	This SFR was used in preference to FMT_MSA.1 as it better reflects TOE functionality.

5.2.24 FMT_MSA.1a Management of security attributes (Device Application Control SFP)

Hierarchical to:	No other components.
FMT_MSA.1a.1	The TSF shall enforce the [**Device Application Control SFP**] to restrict the ability to [***query***] the security attributes [**a) Developer name,** **b) Digital signature, and** **c) Device resource type**] to [**Manager (SECROLE_MANAGER)**].
Dependencies:	[FDP_ACC.1 Subset access control, FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.25 FMT_MSA.1b Management of security attributes (Secure Enterprise Access SFP)

Hierarchical to:	No other components.
FMT_MSA.1b.1	The TSF shall enforce the [**Secure Enterprise Access SFP**] to restrict the ability to [***modify***] the security attributes [**Root (system) certificate store**] to [**Manager (SECROLE_MANAGER)**].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.26 FMT_MSA.1c Management of security attributes (Device Configuration Control SFP)

Hierarchical to:	No other components.
FMT_MSA.1c.1	The TSF shall enforce the [**Device Configuration Control SFP**] to restrict the ability to [***query or modify***] the security attributes [**a) Security role, and** **b) Access privilege**] to [**Manager (SECROLE_MANAGER)**].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.27 FMT_MOF.1b Management of security functions behaviour (Device Access Control)

Hierarchical to:	No other components.
FMT_MOF.1b.1	The TSF shall restrict the ability to [**enable, disable or modify the behaviour of**] the functions [**related to managing the Device Access Control function**] to [**Manager (SECROLE_MANAGER)**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	This SFR was used in preference to FMT_MSA.1 as it better reflects TOE functionality.

5.2.28 FMT_MSA.3a Static attribute initialisation (Device Application Control SFP)

Hierarchical to:	No other components.
FMT_MSA.3a.1	The TSF shall enforce the [**Device Application Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3a.2	The TSF shall allow the [**Manager (SECROLE_MANAGER)**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

5.2.29 FMT_MSA.3b Static attribute initialisation (Secure Enterprise Access SFP)

Hierarchical to:	No other components.
FMT_MSA.3b.1	The TSF shall enforce the [**Secure Enterprise Access SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3b.2	The TSF shall allow the [**Enterprise (SECROLE_ENTERPRISE)**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

5.2.30 FMT_MSA.3c Static attribute initialisation (Device Configuration Control SFP)

Hierarchical to:	No other components.
FMT_MSA.3c.1	The TSF shall enforce the [**Device Configuration Control SFP**] to provide [***restrictive***] default values for security attributes that are used to

	enforce the SFP.
FMT_MSA.3c.2	The TSF shall allow the [**Manager (SECROLE_MANAGER)**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

5.2.31 FMT_SMF.1 Specification of management functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: [**a) managedevice data protection,** **b) managedevice application control,** **c) manage secure enterprise access,** **d) manage device configuration control, and** **e) manage device access control**].
Dependencies:	No dependencies.
Notes:	The TOE provides the capability to manage each of the TOE security functions through remote and local policy configuration of settings specifying the behavior of: **a) User password,** **b) Remote and local device wipe,** **c) Permitted communication mediums,** **d) Removable storage use,** **e) Application installation and execution operation,** **f) Security certificates,** **g) Device and removable media encryption,** **h) TOE security updates,** **i) Enterprise connectivity, and** **j) Key exchange algorithms.**

5.2.32 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**a) None (SECROLE_NONE)** **b) Manager (SECROLE_MANAGER)** **c) Enterprise (SECROLE_ENTERPRISE)** **d) Operator (SECROLE_OPERATOR)** **e) Authenticated User (SECROLE_USER_AUTH)** **f) Unauthenticated User (SECROLE_USER_UNAUTH)** **g) Trusted Provisioning Server (SECROLE_OPERATOR_TPS)** **h) Known Push Proxy Gateway (SECROLE_KNOWN_PPG)** **i) Device Trusted Push Proxy Gateway (SECROLE_PPG_TRUSTED)** **j) Push Initiator Authenticated (SECROLE_PPG_AUTH)** **k) Trusted Push Proxy Gateway (SECROLE_TRUSTED_PPG)** **l) Any Push Message (SECROLE_ANY_PUSH_SOURCE)**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	The Windows Mobile security roles allow or restrict access to the Mobile Device resources. Roles are used to determine whether a remote message is accepted, and if it is, what level of access it is allowed.

5.3 TOE Security Assurance Requirements

34 The assurance package for the evaluation of Windows Mobile 6.5is Evaluation Assurance Level 4 (EAL4), augmented by the life cycle support component that provides basic flaw remediation (ALC_FLR.1).

35 EAL4assurance requirements provideconfidence in the security functionality of the TOE by analysis using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behavior.

36 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities.

37 EAL4 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

38 Table 10 below provides a summary of the TOE security assurance requirements for this evaluation. Complete details of all assurance components are located in part 3 of the Common Criteria.

Table 10 – Summary of TOE security assurance requirements

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures

Assurance class	Assurance components
	ALC_FLR.1Basic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.2 Testing: security enforcing modules
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

6 TOE Summary Specification

6.1 Overview

39 This chapter provides the TOE summary specification, a high-level definition of the security functions claimed to meet the functional and assurance requirements.

6.2 Security functions

40 The TOE security functions include the following:

a) **Device data protection.** The TOE provides the capability to protect data at rest and in transit.

b) **Device application control.** The TOE provides the capability to only permit trusted applications to be installed and executed on the Mobile Device.

c) **Secure enterprise access.** The TOE provides the capability to securely transfer data between the Mobile Device and trusted systems within the Enterprise.

d) **Device access control.** The TOE has inbuilt security mechanisms that can be enabled to provide controlled access to the Mobile Device.

e) **Device security management.** The TOE has configurable security policies that establish which actions a user or application may take.

6.2.1 Device data protection

6.2.1.1 S/MIME support

41 Secure/Multi-purpose Internet Mail Extensions (S/MIME) provides additional protection features for e-mail messages, whether in transit between device and server or at rest. S/MIME uses an authentication process which helps verify that messages were not tampered with en route.

42 The TOE uses the RSAENH cryptographic module to support this cryptographic function. Additionally, the following related security policy settings can be set for Windows Mobile:

a) **SMIME Signing Policy.** This policy specifies whether the Inbox application will send all messaged signed.

b) **SMIME Encryption Policy.** This policy specifies whether the Inbox application will send all messages encrypted.

c) **SMIME Signing Algorithm Policy.**This policy specifies which signing algorithm is to be used, which is either SHA-1 or MD5 algorithm.

d) **SMIME Encryption Algorithm Policy.** This policy specifies which algorithm to use to encrypt a message, which may be either the 3DES or DES algorithm.

6.2.1.2 Sensitive Data Protection

43 The TOE provides support for encryption of data stored on the Mobile Device through the Sensitive Data Protection (SDP) function. SDP supports Advanced Encryption Standard (AES) in 128 bit cipher strength.

44 Encryption is transparent to applications and the user. SDP can be managed by the Enterprise Administrator and the local user (if permissible by the Enterprise Administrator).

45 The TOE provides support for encryption of data stored in removable storage cards. Removable storage card encryption supports Advanced Encryption Standard (AES) in 128 bit cipher strength.

46 The TOE can encrypt data written from the Mobile Device to removable media. The data will be encrypted for use on the encrypting device only. If unencrypted data is transferred to the storage card by another Mobile Device, the content is not encrypted by the device. Exchange ActiveSync file explorer provides desktop access to encrypted data files.

47 Encryption is transparent to applications and the user. Removable storage card encryption can be managed by the Enterprise Administrator and SCMDM policies.

6.2.1.3 Certified cryptographic module

48 Windows Mobile offers the following cryptographic services:

a) **Encryption**. Provides confidentiality and authentication between two communicating parties who have exchanged a shared secret.

b) **Hashing.** Provides data integrity of information when sent over a non-secure channel such as the Internet and to protect user credentials on the device.

c) **Digital Signature.** Provides authentication of another party, or information sent by that party, without prior exchange of a shared secret.

49 Windows Mobile implements these cryptographic services through the Microsoft Windows CE and Windows Mobile Enhanced Cryptographic Provider(RSAENH). This is a general-purpose, software-based, cryptographic module for Windows CE and Windows Mobile. This module encapsulates several different cryptographic algorithms which are accessible via the Microsoft CryptoAPI. It can be dynamically linked into applications by software developers to permit the use of general-purpose cryptography.

50 The RSAENH cryptographic module meets the Level 1 FIPS 140-2 Validation requirements.

51 The RSAENH cryptographic module consists of a single dynamically-linked library (DLL) named RSAENH.DLL. The cryptographic boundary for RSAENH is defined as the enclosure of the computer system on which the cryptographic module is to be executed. The physical configuration of the module, as defined in FIPS PUB 140-2, is Multi-Chip Standalone.

52 The RSAENH cryptographic module supports the following FIPS 140-2 Approved algorithms:

a) RSA PKCS #1 (v1.5) / X9.31 sign and verify with private and public key,

b) DES keypair derivation,

c) DES keypair generation,

d) DES ECB / CBC encrypt/decrypt,

e) 3DES keypair derivation,

f) 3DES keypair generation,

g) 3DES ECB / CBC encrypt/decrypt,

h) 3DES 112 keypair generation,

i) 3DES 112 ECB / CBC encrypt/decrypt,

j) AES 128 / 192 / 256 keypair derivation,

k) AES 128 / 192 / 256 keypair generation,

l) AES ECB / CBC encrypt/decrypt,

m) SHA-1 hash,

n) SHA-256, SHA-384, SHA-512,

o) SHA-1 based Keyed-Hash Message Authentication Code (HMAC),

p) SHA-2 based Keyed-Hash Message Authentication Code (HMAC), includes HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, and

q) Approved Software Pseudo Random Number Generation (PRNG) (seeded by non-Approved PRNG) (FIPS 186-2, Appendix 3.1 and 3.3, Regular, XOriginal, SHA-1 G function, Seed-key 64 bytes only).

6.2.2 Secure enterprise access

6.2.2.1 SSL/TLS channel encryption

53 Enterprise Administrator can allow, or require, Windows Mobile-powered devices to create SSL/TLS encrypted connections with any LOB Servers. By default, SSL/TLS encrypted connections are 128-bit.

54 SSL/TLS includes a method for a client and server to negotiate an encryption algorithm and strength; this is designed to allow an arbitrary client-server pair to find the strongest encryption that both endpoints support. Both Windows Mobile and the Windows Server Internet Information Services (IIS) application server can take advantage of a broad set of cryptographic algorithms for use with SSL/TLS. In Windows Mobile 6.5, this includes support for AES which is available for SSL/TLS channel encryption in 128 and 256-bit cipher strengths.

55 Communication between the Mobile Device and enterprise resources must be performed using secure channels. In order to perform Exchange Server mobile messaging features, mailbox synchronization, Line of Business server access, and Mobile Device management SCMDM, an appropriate secure channel must first be established.

6.2.2.2 Mobile VPN

56 Enterprise Administrator can allow, or require, Windows Mobile-powered devices to connect to the Enterprise via a two tiered Mobile VPN solution. Two tiers are established through the utilization of an IPSec tunnel between the Mobile Device and the Enterprise Gateway, with an SSL/TLS encrypted communication between the Mobile Device and enterprise servers.

57 The IPSec tunnel is established through an Internet Key Exchange (IKE, version 2) which utilises the Diffie-Hellman key exchange to establish a shared session secret. Using the shared session secret, the establishment of an IPSec tunnel is performed to encrypt all communications between the Mobile Device and Enterprise Gateway using either AES or 3DES symmetric encryption.

58 Connectivity between the Mobile Device and enterprise resources (including the SMCDM and Line of Business servers) is the established utilizing an SSL/TLS encrypted channel. This approach effectively double-envelopes all communications between the Mobile Device and enterprise resources, ensuring appropriate authentication and protection from unauthorized modification or disclosure is maintained.

6.2.2.3 Enterprise authentication

59 Mobile users can access Line of Business servers within the organization using the Mobile VPN capability. An enterprise link is required to be established between the

Mobile Device and the System Center Mobile Device Manager, allowing communication between the Mobile Device and LOB server.

60 This communication allows for Mobile Users to access and use enterprise systems and resources outside of the scope of traditional mailbox and calendar functions, based on the LOB configuration and Enterprise Administrator defined policy settings.

61 The enterprise authentication capabilities are replicated and enabled on the Windows Mobile device to ensure that continuity can be maintained with the enterprise environment

6.2.3 Device application control

6.2.3.1 Controlled application installation

62 Application installation files (known as cabinet or .cab files) may be digitally signed by the application provider (Microsoft), a third-party software company, or the developer of an enterprise line-of-business application. At install time, the digital signature of the installation .cab is checked against certificates in the software publishing certificate store. If there is a match, the installation can take place.

63 The installer calls the Security Loader, which checks the digital signature of the .cab against the certificates in the Software Publishing Certificate (SPC) store to determine the security role used for the configuration.

64 The Security Loader also checks that the application revocation list does not include the certificate hashes (a certificate hash is a digest of the certificate data) and that the application revocation list does not include the .cab file hashes.

6.2.3.2 Controlled application execution

65 Digital certificates are used on Windows Mobile device to provide the basis for implementing code execution control. When an application attempts to execute on Windows Mobile, the Kernel will call the Security Loader to determine if the application is permitted.

66 Applications signed with a trusted certificate are permitted to execute. Unsigned applications, or those signed with a certificate that the Mobile Device does not recognize, require further policy checks to determine if they can run.

6.2.4 Device access control

6.2.4.1 Trusted provisioning

67 The TOE can be configured through specific security policies to only accept certain OTA provisioning protocols and messages.

68 Security policies are used for configuring security settings that are then enforced with the help of security roles and certificates. They provide the flexibility to control the level of security on the device. The policies are defined globally and enforced locally in their respective components.

69 The security policy is set during boot by executing a configuration file called provxml.provxml. This provisioning file is in ROM and it contains the default setting specified by the device manufacturer.

70 The security policies are loaded onto Windows Mobile powered devices in a security policy provisioning document, which is an Extensible Markup Language (XML) file that is assigned the correct security role to apply the security settings to the device. These security policies are enforced at critical points across the architecture of the device. Often, these policies will interact with Configuration Manager and the security settings of the Mobile Device. When the security policy document is delivered to the device, it is validated and verified by the security policy engine of the TOE, which is administered by Configuration Manager, and then applied by the Security Policy Configuration Service Provider.

6.2.4.2 Device authentication and lock

71 Device lock requires a password to access the device when it is turned on; however, it is possible to receive incoming calls and to make emergency calls without authenticating to the device.

72 The TOE enables a user to interact directly through the User Interface (UI) and lock a current session. To unlock a device the Mobile User will have to successfully authenticate using their password.

73 The TOE supports the implementation of robust password policies for local authentication to the Mobile Device. The Microsoft Default Local Authentication Plug-in (LAP) can be configured to prevent users from choosing a password that contains a simple pattern or has too few digits.

74 The feature will enable a policy that requires end users to choose a password that does not contain a:

a) repeating sequence(such as 1111), and

b) sequence with a predictable difference between values (such as 1234 or 1357).

75 The Microsoft default LAP allows Enterprise Administrator to enforce a policy of how often a user must choose a new password. The password expiration feature is dependent on the phone clock. Once the expiration period is reached the user is prompted to change their password. The new password must meet the other requirements such as password strength and password history

6.2.4.3 Local device wipe

76 Local device wipes are triggered on a Mobile Device with device lock enforced if a user incorrectly enters a password more than a specified number of times (the policy default is 8 times, but the administrator can adjust this value).

77 After a configurable number of missed attempts, the device displays a confirmation prompt that requires the user to type a confirmation string (the default is "A1B2C3") to continue. This prevents the device from being wiped by accidental key presses. Once the password retry limit is reached, the device immediately wipes itself, erasing all local data.

6.2.5 Device security management

6.2.5.1 Security roles and policies

78 The TOE maintains multiple management roleswhich determine an individual's degree of access to device resources.

79 Security roles determine access to Windows Mobile powered device resources. The security role is based on the message origin and how the message is signed. Security roles are also used with certificates to enforce security settings that are configured by using security policies.

80 The TOE implements several roles however, some of the key roles are as follows:

a) **Manager (SECROLE_MANAGER).** This role allows unrestricted access to system resources.

b) **Enterprise (SECROLE_ENTERPRISE).** Allocated to the Enterprise Administrator role. The Enterprise role allows IT administrators to manage specific device settings, such as wiping a device, setting password requirements, and managing certificates.

c) **Operator (SECROLE_OPERATOR).** Setting can be changed by a Wireless Application Protocol (WAP) Trusted Provisioning Server (TPS). Known as the Mobile Operator in the context of the TOE.

d) **Authenticated User (SECROLE_USER_AUTH).** Setting can be changed by an authenticated user. This role can be assigned to the Mobile User.

6.2.5.2 Remote wipe

81 Remote wipes occur when the Enterprise Administrator issues an explicit wipe command through SCMDM. The Mobile User can also initiate a wipe command if they've lost their device. Remote wipe operations are separate from local wipes,

and a device can be wiped remotely even if Exchange ActiveSync security policies are not in force. The wipe command is pushed as an out-of-band command, so that the device receives it on its next synchronization. The device sends an acknowledgement message when it receives the wipe command, alerting the Enterprise Administrator that the wipe has occurred. The Mobile User cannot opt out of the remote wipe.

82 Wiping the device has the effect of performing a factory or "hard" reset; all programs, data, and user-specific settings are removed from the device. The Windows Mobile device wipe implementation wipes all data, settings, and private key material on the device by overwriting the device memory with a fixed bit pattern, greatly increasing the difficulty of recovering data from a wiped device.

6.2.5.3 Device management Policies

83 Microsoft's System Center Mobile Device Manager (SCMDM, also referred to as MDM) 2008, is an enterprise server solution designed to provide a secure management and monitoring solution for Windows Mobile-powered devices. SCMDM empowers Administrators to provide a secure data and network access for their mobile workforce, while retaining a high degree of control over their mobile device usage.

84 SCMDM provides a security management platform for Windows Mobile phones with over 130 policies and settings and built-in mechanisms that help prevent the misuse of corporate data. Administrators can lock down many areas of the Windows Mobile Smartphones and Pocket PCs, including certain communications and device functionality, application installation and execution settings and more. SCMDM can be used to manage security on all Windows Mobile devices across the enterprise network, from an enterprise wide perspective down to individual Windows Mobile devices and users.

6.3 Assurance Measures

85 The following groups of assurance measures are applied to Windows Mobile to satisfy CC EAL4 augmented with flaw remediation.

6.3.1 Development (ADV)

86 The Windows Mobile Security Design Documentation provides the suite of documents that provide the various security design layers of the TOE. These documents include the following:

a) **Windows Mobile 6.5 Functional Specification.** The functional specification describes the security functionality of the TOE, and aligns with the security functional requirements specified in the ST. The functional specification also details the external interface to the TOE.

b) **Windows Mobile 6.5Security Architecture.** This document provides a detailed description of the security architecture of Windows Mobile 6.5. The described security architecture demonstrates that the operating system has been designed to be self-protecting, non-bypassable and designing to have distinct security domains for trusted execution.

c) **Windows Mobile 6.5 TOE Design.** A high-level document that identifies all the key subsystems and modules of the TOE, is also supported by low-level specifications for key security-enforcing and supporting modules.

d) **Windows Mobile 6.5Implementation Representation.** The complete source tree has been provided to the evaluators to address these requirements.

6.3.2 Guidance documents (AGD)

87 Microsoft provides device manufacturers, or original equipment manufacturers (OEMs) with guidance on how to implement the Windows Mobile 6.5 operating system in a secure and reliable manner.

88 Microsoft also provides operational guidance on how to perform the TOE security functions andwarnings to authorized administrators and users about actions that can compromise the security of the TOE.

89 Administrator guidance is documented in the Windows Mobile 6.5 Installation and Administrator Guide.

90 User guidance is provided in help files contained on the Windows Mobile powered device and is supplemented by the Windows Mobile 6.5 User Guide Supplement.

6.3.3 Life cycle support (ALC)

91 Microsoft has a development life-cycle with strong supporting business processes. The following documentation will be submitted to support the life-cycle requirements.

a) **Windows Mobile 6.5EAL4+ Lifecycle Description.**This document provides details regarding the development security, lifecycle model and tools and techniques used to develop and maintain the TOE.

b) **Windows Mobile 6.5 EAL4+ Configuration Management.**This document provides details of the configuration management capabilities and scope used for the development and maintenance of the TOE.

c) **Windows Mobile6.5 EAL4+ Delivery Process.** This document describes the security controls integrated into the delivery process provide assurance that the confidentiality and integrity of the TOE is maintained during distribution and final delivery to the end-consumer.

d) **Windows Mobile 6.5 EAL4+ Flaw Remediation Process.** This document describes Microsoft's flaw remediation process. Flaw remediation requires that discovered security flaws be tracked and corrected by Microsoft.

6.3.4 Security Target evaluation (ASE)

92 This document, the Windows Mobile 6.5 EAL4+ Security Target is used as evidence for this set of assurance requirements.

6.3.5 Tests (ATE)

93 The TOE has been tested by Microsoft to ensure that all security functional requirements have been implemented accurately within Windows Mobile.

94 The Windows Mobile 6.5 Security Testing document consists of the following:

a) **Windows Mobile 6.5 EAL4+ Security Testing.**The test plan describes the form, content, and organization of test documentation. It alsosummarizes each of the test suites and includes the following detail:

i) **Test procedures.**The test procedures include both documentation and an actual implemented test (if applicable). Testsuites are organized around tests that share a common theme. The test suite documentation describes the purpose for the test suite, the set of test variations, procedures to successfully exercise the test, and expected results.

ii) **Test results.**The results are captured for each test with summaries of the results in terms of total tests for each test suite. The results are matched against the expected results for each test.

6.3.6 Vulnerability assessment (AVA)

95 The TOE has been made available to the evaluators, including the implementation representation to conduct an analysis to identify potential vulnerabilities and exposures.

7 Rationale

7.1 Overview

96 This section provides the rationale for completeness and consistency of the ST. The rationale addresses the following areas:

a) **Security objectives rationale.** Provides coverage for the security objectives for the TOE and the environment, ensuring that all threats and assumptions are effectively addressed.

b) **Security requirements rationale.** Provides justification for TOE assurance requirements, evidence that all dependencies have been addressed, specification of strength of function for all probabilistic mechanisms and demonstration that the IT requirements address the TOE and environment objectives.

c) **TOE summary specification rationale.** Provides evidence that the IT security functions and assurance measures are adequate to implement the security functional and assurance requirements.

7.2 Security objectives rationale

7.2.1 Security objectives for the TOE

Table 11 – Mapping of TOE security objectives to threats

Threats	Objective	Justification
T.EAVESDROPPING	O.COMMS_CONF	The threat of eavesdropping is mitigated by implementing encryption capabilities to preserve the confidentiality of transmitted data.
T.INTERCEPT	O.COMMS_INT	The threat of interception is mitigated by implementing encryption and digital signature capabilities to preserve the integrity of transmitted data.
T.IMPORT	O.CODE_CTRL	The threat of a compromise of data due to import of malicious code is mitigated by requiring explicit authorization to execute code.

Threats	Objective	Justification
T.TOE_ACCESS	O.USER_AUTH O.REMOTE_WIPE O.LOCAL_WIPEO.SESSION_LOCKO.REMOTE_ADMIN	The threat of a data compromise due to a lost device is mitigated by: • O.USER_AUTH requires user authentication, preventing immediate access to data. • O.REMOTE_WIPE enables the Enterprise Administrator to remotely erase device data, reducing the time available to an attacker to compromise data. • O.LOCAL_WIPE allows the TOE to be configured to erase device data after a defined number of failed authentication attempts, detecting and reacting to authentication attacks. • O.SESSION_LOCK ensures that the user has to re-authenticate after a defined period of inactivity, reducing the likelihood that an attacker will gain possession of an 'unlocked' device.
10-JAN-10		• O.REMOTE_ADMIN enables the Enterprise Administrator to apply remote wipe commands.

Threats	Objective	Justification
T.SC_ACCESS	O.DATA_ENCRPYT O.REMOTE_WIPE O.LOCAL_WIPE	The threat of a data compromise due to an attacker gaining direct access to a removable storage card: • O.DATA_ENCYPT provides added assurance that TSF and/or user data is protected on any inserted removable storage card. • O.REMOTE_WIPE enables the Enterprise Administrator to remotely erase data stored on an inserted removable storage card. • O.LOCAL_WIPE allows the TOE to be configured to erase data stored on an inserted removable storage card after a defined number of failed authentication attempts.

Threats	Objective	Justification
T.MASQUERADE	O.MGMT_AUTH O.ROLES	The threat of acting on spurious management messages is mitigated by: • O.MGMT_AUTH implementing mechanisms to ensure all management messages have originated from a trusted source. • O.ROLES enables role base access control to assign roles to messages and processes from various sources and interfaces.
T.WEAK_SECRET	O.SECRET O.REMOTE_ADMIN	The threat that a user will chose a weak password is mitigated by: • O.SECRET implementing mechanisms to detect and prevent the selection of weak passwords. • O.REMOTE_ADMIN ensures that the Enterprise Administrator can apply strong password policies to the device.

Threats	Objective	Justification
T.MISCONFIGURE	O.MANAGEMENT	The threat that a user may inadvertently compromise the integrity of the TOE through the manipulation of settings is mitigated by: • O.MANAGEMENT implementing policy controls administered by the Enterprise Administrator specifying security and operational settings of the device that cannot be changed by the user.

7.2.2 Security objectives for the non-IT environment

Table 12 – Mapping of non-IT objectives to assumptions

Assumptions	Objectives	Justification
A.USAGE	OE.USAGE	This objective for the environment ensures that the assumption is upheld that the Mobile Users will be made aware of the need to follow guidance, that the Mobile Device when subjected to a hard-reset my not load into the evaluated configuration and the device must be re-provisioned into the evaluated configuration, that the device must be only connected to trusted computing devices for ActiveSync sessions, and that it should be appropriately protected when not in use.
A.DELIVERY	OE.DELIVERY	This objective for the environment ensures that the assumption is upheld that the Device Manufacturer and the Mobile Operator are trusted to not modify the security enforcing components of the TOE during the delivery process.
A.IT_ENTERPRISE	OE.IT_ENTERPRISE	This objective for the environment ensures that the assumption is upheld that the enterprise components that interact with the TOE in normal operating conditions are appropriately protected.
A.ADMIN	OE.ADMIN	This objective for the environment upholds the assumption that administration personnel can be trusted.

7.2.3 Security objectives for the IT environment

Table 13 – Mapping of IT environment objectives to assumptions

Assumption	Objective	Justification
A.I&A_ENTERPRISE	OE.I&A_ENTERPRISE	This objective for the IT environment ensures that the assumption is upheld that the user of the Mobile Device will be authenticated by the IT environment prior to being granted access to their Mailbox or other corporate resources.
A.COMMS_ENT	OE.COMMS_ENT	This objective for the IT environment ensures that the assumption is upheld that the enterprise will provide the other end of a secure communications channel for communicating with the Mobile Device.
A.SEC_POLICY	OE.SEC_POLICY	This objective for the IT environment ensures that the assumption is upheld that the enterprise will provide a suitable interface for creating and applying enterprise Mobile Device security policies.

7.3 Security requirements rationale

7.3.1 Dependency analysis

Table 14 – TOE SFR dependency demonstration

SFR	Dependency	Inclusion
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1 FCS_CKM.4
FCS_COP.1a	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 FCS_CKM.4
FCS_COP.1b	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 FCS_CKM.4
FCS_COP.1c	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 FCS_CKM.4

SFR	Dependency	Inclusion
FCS_COP.1d	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 FCS_CKM.4
FCS_COP.1e	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1
FDP_ACC.1a	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1a	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3
FDP_IFC.1	FDP_IFF.1 Simple security attributes	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_IFC.1 FMT_MSA.3
FTP_ITC.1	No dependencies.	N/A

SFR	Dependency	Inclusion
FDP_ACC.1a	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1a	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_ATD.1	No dependencies.	N/A
FIA_SOS.1	No dependencies.	N/A
FIA_UAU.1	FIA_UID.1 Timing of identification	Not included – see rationale below.
FIA_UAU.7	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_SSL.1.EX	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_SSL.2.EX	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FMT_MOF.1a	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1a	[FDP_ACC.1 Subset access control, FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 and FDP_IFC.1 FMT_SMR.1 FMT_SMF.1

SFR	Dependency	Inclusion
FMT_MSA.1b	[FDP_ACC.1 Subset access control, FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 and FDP_IFC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.1c	[FDP_ACC.1 Subset access control, FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 and FDP_IFC.1 FMT_SMR.1 FMT_SMF.1
FMT_MOF.1b	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_MSA.3a	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FMT_MSA.3b	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FMT_MSA.3c	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	No dependencies.	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	Not included – see rationale below.

7.3.2 Rationale for not addressing all dependencies

97 FIA_UID.1 is a dependency of FIA_UAU.1 and FIA_SMR.1 that has not been included. The TOE is a single-user operating system and the implementation of a user identifier associated with the Mobile User is therefore redundant.

7.3.3 Rationale for explicit security functional requirements

Table 15 – Rationale for explicitly stated security functional requirements

Explicit SFR	Based on	Dependency	Rationale
FTA_SSL.1-EX TSF-initiated session lock And FTA_SSL.2-EX – User-initiated locking	FTA_SSL.1 TSF-initiated session lock and FTA_SSL.2 – User-initiated locking	FIA_UAU.1	The TOE does not wipe clear the user interface after a session lock as there are a number of activities that can be performed on the TOE prior to successful authentication by a Mobile User (see FIA_UAU.1). This functionality needs to be maintained after a session lock. The modification of the base SFRs FTA_SSL.1 and FTA_SSL.2 could not be considered a refinement. Therefore, this modification had to be stated as an explicit SFR. The SFR is measurable and compliance or noncompliance can be readily determined. Additionally, as the requirement does not differ significantly from the base SFR the statement of requirement can be considered clear and unambiguous. The dependency for FTA_SSL.1 has also been retained.

7.3.4

7.3.5 TOE IT requirements correspondence

Table 16 – Mapping TOE SFRs to objectives

Objective	SFRs	Demonstration
O.COMMS_CONF	FCS_CKM.1 FCS_COP.1a FCS_COP.1b FCS_COP.1e FCS_CKM.4	FCS_CKM.1 provides support for implementing communications that have both confidentiality and integrity security properties. FCS_COP.1a implements cryptographic operations for providing secure communications with the enterprise and/or network environment. FCS_COP.1b implements cryptographic operations for providing secure email capability. FCS_COP.1e implements cryptographic operations for providing secure communications with the enterprise and/or network environment. FCS_CKM.4 provides support for implementing communications that have both confidentiality and integrity security properties. FCS_CKM.1, FCS_COP.1a, FCS_COP.1b and FCS_CKM.4 combine to ensure that the O.COMMS_CONF objective is met.
O.COMMS_INT	FCS_CKM.1 FCS_COP.1a FCS_COP.1b FCS_COP.1e FCS_CKM.4	FCS_CKM.1 provides support for implementing communications that have both confidentiality and integrity security properties. FCS_COP.1a implements cryptographic operations for providing secure communications with the enterprise and/or network environment. FCS_COP.1b implements cryptographic operations for providing secure email capability. FCS_COP.1e implements cryptographic operations for providing secure communications with the enterprise and/or network environment.FCS_CKM.4 provides support for implementing communications that have both confidentiality and integrity security properties.

Objective	SFRs	Demonstration
		FCS_CKM.1, FCS_COP.1a, FCS_COP.1b and FCS_CKM.4 combine to ensure that the O.COMMS_INT objective is met.
O.CODE_CTRL	FDP_ACC.1a FDP_ACF.1a	FDP_ACC.1a provides the basis for implementing an access control policy that ensures only permitted applications can be installed and executed on the TOE. FDP_ACF.1a provides the security policy statements designed to govern the control of applications when being installed or executed on the TOE. FDP_ACC.1a and FDP_ACF.1a combine to ensure that the O.CODE_CTRL objective is met.
O.MGMT_AUTH	FDP_ACC.1b FDP_ACF.1b	FDP_ACC.1b provides the basis for establishing a security policy within the TOE for controlling the configuration of the Mobile Device. FDP_ACF.1b provides the security policy statements to support the implementing of device configuration control for the TOE. FDP_ACC.1b and FDP_ACF.1b combine to ensure that the O.MGMT_AUTH objective is met.
O.USER_AUTH	FIA_ATD.1 FIA_UAU.1 FIA_UAU.7	FIA_ATD.1 provides the set of security attributes that must be associated with a Mobile User to enable Mobile Device Authentication. FIA_UAU.1 provides the capability for the TOE to be able to offer a number of display notifications and essential services prior to requiring a Mobile User Authentication event. This enables the TOE to operate as a mobile messaging solution without compromising TSF or user data. FIA_UAU.7 provides detailed information relating to feedback that can be provided to the user when conducting a Mobile User Authentication event. FIA_ATD.1, FIA_UAU.1 and FIA_UAU.7 combine to ensure that the O.USER_AUTH objective is met.
O.REMOTE_ADMIN	FDP_IFC.1 FDP_IFF.1 FTP_ITC.1	FDP_IFC.1 provides the basis for implementing a policy within the TOE for controlling the flow of information, mailbox item and SCMDM policy, between the TOE and the enterprise environment. FDP_IFF.1 implements the policy that governs the flow of information between the TOE and the

Objective	SFRs	Demonstration
	FMT_MOF.1a FMT_MSA.1a FMT_MSA.1b FMT_MSA.1c FMT_MOF.1b FMT_MSA.3a FMT_MSA.3b FMT_MSA.3c FMT_SMF.1	enterprise environment, including TSF and user data. FTP_ITC.1 provides the capability to support a trusted and secure channel between the TOE and the enterprise environment so that the TOE is able to access enterprise information in a secure manner. FMT_MOF.1a provides the restrictions that are necessary for protecting the management and configuration of the device data protection functionality of the TOE. FMT_MSA.1a provides the restrictions that are necessary for protecting the management and configuration of the device application control functionality of the TOE. FMT_MSA.1b provides the restrictions that are necessary for protecting the management and configuration of the secure enterprise access functionality of the TOE. FMT_MSA.1c provides the restrictions that are necessary for protecting the management and configuration of the device configuration control functionality of the TOE. FMT_MOF.1b provides the restrictions that are necessary for protecting the management of the device access control functionality of the TOE. FMT_MSA.3a provides restrictions and controls for managing security attributes associated with the device application control security policy. FMT_MSA.3b provides restrictions and controls for managing security attributes associated with the secure enterprise access security policy. FMT_MSA.3c provides restrictions and controls for managing security attributes associated with the device configuration control security policy. FMT_SMF.1 provides a specification for the set of device security management functions that are required to support the secure administration and operation of the TOE. FDP_IFC.1, FDP_IFF.1, FTP_ITC.1, FMT_MOF.1a, FMT_MSA.1a, FMT_MSA.1b, FMT_MSA.1c, FMT_MOF.1b, FMT_MSA.3a, FMT_MSA.3b, FMT_MSA.3c and FMT_SMF.1 all combine to ensure that the O.REMOTE_ADMIN objective is met.

Objective	SFRs	Demonstration
O.SECRET	FIA_SOS.1	FIA_SOS.1 provides the capability for the TOE to implement strong password policies in response to settings to be established by the Enterprise Administrator.
O.LOCAL_WIPE	FIA_AFL.1	FIA_AFL.1 provides the requirement for the TOE to implement a secure wipe of all user and TSF data in response to an Enterprise Administrator configurable number of failed authentication attempts.
O.ROLES	FMT_SMR.1	FMT_SMR.1 provides a specification of the various roles that the TOE is required to recognize and apply.
O.DATA_ENCRYPT	FCS_CKM.1 FCS_COP.1c FCS_COP.1d FCS_CKM.4	FCS_CKM.1 supports data encryption by providing key generation functions. FCS_COP.1c implements cryptographic operations for providing data encryption services for data at rest on removable storage cards to support the need for encrypting user and/or TSF data. FCS_COP.1d implements cryptographic operations for providing data encryption services for data at rest on the Mobile Device to support the need for encrypting user and/or TSF data. FCS_CKM.4 supports data encryption by providing a method for securely destroying generated keys. FCS_CKM.1, FCS_COP.1c, and FCS_CKM.4 combine to ensure that the O.DATA_ENCRYPT objective is met.
O.SESSION_LOCK	FTA_SSL.1.EX FTA_SSL.2.EX	FTA_SSL.1.EX provides the ability to lock and interactive session after an Enterprise Administrator specified period of time. FTA_SSL.2.EX provides the Mobile User with the ability to lock a current interactive session so that authentication is required to unlock Mobile Device. FTA_SSL.1.EX and FTA_SSL.2.EX combine to ensure that the O.SESSION_LOCK objective is met.
O.REMOTE_WIPE	FDP_IFC.1	FDP_IFC.1 ensures that the Mobile Device can accept a remote wipe command from the

Objective	SFRs	Demonstration
	FDP_IFF.1	Enterprise Administrator through SCMDM. FDP_IFF.1 implements the policy that governs the flow of information between the TOE and the enterprise environment and allows the application of the remote wipe command. FDP_IFC.1 and FDP_IFF.1 combine to ensure that the O.REMOTE_WIPE objective is met.
O.MANAGEMENT	FMT_SMF.1	FMT_SMF.1 ensures that the Enterprise Administrator is capable of configuring security and operational policy settings that cannot be modified by the user.

7.3.6 TOE assurance requirements

98 This ST contains the assurance requirements from the CC EAL4 assurance package augmented with ALC_FLR.1. Augmentation was chosen to provide the added assurance that is provided by defining flaw remediation procedures. This ST is based on good rigorous commercial development practices and has been developed for a general environment for a TOE that is readily available and does not require modification to meet the security needs of the environment specified in this ST.

99 The EAL chosen is based on the statement of the security environment (threats, organizational policies, assumptions) and the security objectives defined in this ST. The sufficiency of the EAL chosen is justified based on those aspects of the environment that have impact upon the assurance needed in the TOE. Specifically, that the TOE will not process information that requires protection from attackers possessing a high or moderate attack potential, and that protection from obvious vulnerabilities is required.

7.3.7 Demonstration of mutual support

100 The dependency analysis provided at Table 14 and the analyses provided in Table 16 and Table 17 demonstrate that the IT security functions work together to satisfy the stated security functionality of the TOE.

101 The demonstration of the implementation of the majority of dependencies, and a suitable rationale for those dependencies that have not been implemented, demonstrates mutual support between security requirements, and therefore, the security functions and mechanisms that implement them.

7.4 TOE summary specification rationale

7.4.1 IT security functions

Table 17 – Mapping TOE SFRs to TOE security functions

SFR	Device data protection	Device Application control	Secure enterprise access	Device access control	Device security management	Demonstration
FCS_CKM.1	***X***					The device data protection security function implements the FCS_CKM.1 requirement by creating cryptographic keys for each of the functions that protect data with a cryptographic mechanism.
FCS_COP.1a	***X***					The device data protection security function implements the FCS_COP.1a requirement by providing cryptographic protection for TSF and user data in transit between the TOE and external entities.
FCS_COP.1b	***X***					The device data protection security function implements the FCS_COP.1b requirement by providing protection for email messages through the S/MIME protocol. Data is protected both in transit and at rest.
FCS_COP.1c	***X***					The device data protection security function implements the FCS_COP.1c requirement by providing protection for TSF and/or user data while being stored on a removable storage card.
FCS_COP.1d	***X***					The device data protection security function implements the FCS_COP.1d requirement by providing protection for TSF and/or user data while being stored on the Mobile Device.

SFR	Device data protection	Device Application control	Secure enterprise access	Device access control	Device security management	Demonstration
FCS_COP.1e	***X***					The device data protection security function implements the FCS_COP.1e requirement by providing cryptographic protection for TSF and user data in transit between the TOE and external entities.
FCS_CKM.4	***X***					The device data protection security function implements the FCS_CKM.4 requirement by ensuring that cryptographic keys can be effectively destroyed.
FDP_ACC.1a		***X***				The device application control security function implements the FDP_ACC.1a requirement by controlling the installation and execution on the TOE of applications.
FDP_ACF.1a		***X***				The device application control security function implements the FDP_ACF.1a security function by implementing controls to align with the set of specific security policy rules identified in this requirement.
FDP_IFC.1			***X***			The secure enterprise access security function implements the FDP_IFC.1 requirement by implementing the information attributes that provide the foundation for controlling information flow.
FDP_IFF.1			***X***			The secure enterprise access security function implements the FDP_IFF.1 requirement by implementing controls to align with the set of specific security policy rules identified by this requirement.
FTP_ITC.1			***X***			The security enterprise access security function implements the FTP_ITC.1 requirement by providing the device-side of a secure communications channel between the TOE and enterprise.

SFR	Device data protection	Device Application control	Secure enterprise access	Device access control	Device security management	Demonstration
FIA_AFL.1				***X***		The device access control security function implements the FIA_AFL.1 requirement by implementing a mechanism to ensure that the device is wiped in response to repeated authentication failure.
FIA_ATD.1				***X***		The device access control security function implements the FIA_ATD.1 requirement by implementing the attributes that are associated with the Mobile User.
FIA_SOS.1				***X***		The device access control security function implements the FIA_SOS.1 requirement by implementing the ability to apply strong password requirements.
FIA_UAU.1				***X***		The device access control security function implements the FIA_UAU.1 requirement by permitting the use of the TOE for the specified functions prior to authentication.
FIA_UAU.7				***X***		The device access control security function implements the FIA_UAU.7 requirement by implementing the specific prompts and permitted feedback regarding authentication status.
FTA_SSL.1.EX				***X***		The device access control security function implements the FTA_SSL.1.EX requirement by providing the ability to lock and interactive session after an Enterprise Administrator specified period of time.

SFR	Device data protection	Device Application control	Secure enterprise access	Device access control	Device security management	Demonstration
FTA_SSL.2.EX				***X***		The device access control security function implements the FTA_SSL.2.EX requirement by providing the Mobile User with the ability to lock a current interactive session so that authentication is required to unlock Mobile Device.
FDP_ACC.1b				***X***		The device access control security function implements the FDP_ACC.1b requirement by providing controls to ensure that management or provisioning data will only be applied from a secure and authenticated source.
FDP_ACF.1b				***X***		The device access control function implements the FDP_ACF.1b requirement by implementing the set of subjects and objects specified by this policy for accepting and applying configuration data.
FMT_MOF.1a					***X***	The device security management security function implements the FMT_MOF.1a requirement by enabling the specified management functionality for the device data protection function and associated cryptographic attributes.
FMT_MSA.1a					***X***	The device security management security function implements the FMT_MSA.1a requirement by enabling the specified management functionality for the device application control function.
FMT_MSA.1b					***X***	The device security management security function implements the FMT_MSA.1b requirement by enabling the specified management functionality for the secure enterprise access function.

SFR	Device data protection	Device Application control	Secure enterprise access	Device access control	Device security management	Demonstration
FMT_MSA.1c					***X***	The device security management security function implements the FMT_MSA.1c requirement by enabling the specified management functionality for the device configuration control function.
FMT_MOF.1b					***X***	The device security management security function implements the FMT_MOF.1b requirement by enabling the specified management functionality for the device access control function.
FMT_MSA.3a					***X***	The device security management security function implements the FMT_MSA.3a requirement by ensuring that there are static attributes applied during initialization for the Device Application Control SFP.
FMT_MSA.3b					***X***	The device security management security function implements the FMT_MSA.3b requirement by ensuring that there are static attributes applied during initialization for the Secure Enterprise Access SFP.
FMT_MSA.3c					***X***	The device security management security function implements the FMT_MSA.3 requirement by ensuring that there are static attributes applied during initialization for the Device Configuration Control SFP.
FMT_SMF.1					***X***	The device security management security function implements the FMT_SMF.1 requirement by implementing the set of security management functions that are to be provided for the TOE.
FMT_SMR.1					***X***	The device security management security function implements the set of security roles established by the FMT_SMR.1 requirement.

7.4.2 Assurance measures

Table 18 – Assurance measures rationale

Assurance requirement	Assurance measures	Demonstration
ADV_ARC.1 Security architecture description	Development	The development assurance measure provides all the necessary design documentation to support the effective detailed analysis of the TOE for an evaluation at EAL4. The security architecture description provides a detailed description of the TSF security architecture. The functional specification provides a detailed description of the security functions of the TOE. The design documentation provides a complete definition of the TSF, allowing for sufficient analysis to be performed.
ADV_FSP.4 Complete functional specification		
ADV_IMP.1 Implementation representation of the TSF		
AGD_OPE.1 Operational user guidance	Guidance documents	The operational user guidance documentation provides the guidance for end users, administrators and other parties who will use the TOE. These documents provide all the necessary instructions and direction for ensuring that the TOE is installed, configured, used and administered in a secure manner.
AGD_PRE.1 Preparative procedures		
ALC_CMC.4 Production support, acceptance procedures and automation	Life cycle support	The life cycle support measures provide the assurance that the TOE is developed and subsequently managed using a well defined and controlled approach. Configuration management measures provide the assurance that configured items are managed and maintained in a controlled manner, through the demonstration of well defined processes, procedures and requirements.
ALC_CMS.4 Problem tracking CM coverage		

Assurance requirement	Assurance measures	Demonstration
ALC_DEL.1 Delivery procedures		By placing the TOE and its components into this configuration management list provides assurance that the TOE components are only modified in a controlled manner with proper authorization. Employing sufficient security measures in the delivery process of the TOE to consumers ensures that the TOE is not tampered with prior to its receipt. Procedural, personnel and physical security related documentation is used to ensure that the confidentiality and integrity of the TOE and its design are maintained throughout the development life cycle. The life cycle support assurance measures provides a set of procedures aimed at the identifying, reporting and addressing security flaws or bugs that may appear in the TOE. An established development lifecycle methodology is employed to guide the development of the TOE. A set of well establisheddevelopment tools exist and are employed in the development of the TOE.
ALC_DVS.1 Identification of security measures		
ALC_FLR.1Basic flaw remediation		
ALC_LCD.1 Developer defined life-cycle model		
ALC_TAT.1 Well-defined development tools		
ASE_CCL.1 Conformance claims	Security Target evaluation	Security Target evaluation assurance measures ensure that the claim to EAL4 (augmented with ALC_FLR.1) can be accurately appraised.
ASE_ECD.1 Extended components definition		
ASE_INT.1 ST Introduction		
ASE_OBJ.2 Security objectives		

Assurance requirement	Assurance measures	Demonstration
ASE_REQ.2 Derived security Requirements		
ASE_SPD.1 Security problem definition		
ASE_TSS.1 TOE summary specification		
ATE_COV.2 Analysis of coverage	Tests	The tests assurance measure ensures that the TOE has been appropriately tested for the claimed set of security functions. The test plans for the TOE identifies the set of security functions that are to be tested, the procedures for establishing the test environment and also for conducting the test cases. The results of the tests are also recorded to provide evidence of test results.
ATE_DPT.2 Testing: security enforcing modules		
ATE_FUN.1 Functional testing		
ATE_IND.2 Independent testing – sample		
AVA_VAN.3 Focused vulnerability analysis	Vulnerability assessment	The vulnerability assessment assurance measure provides confidence that the TOE and its environment have been assessed for obvious vulnerabilities or exposures. A claim is also provided for the strength of function related to probabilistic mechanisms that are non-cryptographic.