Windows Mobile 5.0 MSFP

Security Target

EAL2 augmented with ALC_FLR.1

Version 1.0

February 2008

Document History

Version	Date	Author	Description
1.0	25-Feb-08	Doug Stuart	Released.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Overview

1 The Target of Evaluation (TOE), Windows Mobile 5.0 MSFP, 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 5.0 MSFP provides the basis for establishing a secure enterprise mobile messaging solution that can securely synchronize and access email, contacts, tasks and calendar while users are away from their corporate network. Windows Mobile 5.0 MSFP can be managed by Microsoft's Exchange Server so that corporate mobile device security policies and standards can be established.

3 Windows Mobile 5.0 MSFP offers device management and security features, and a broad set of advanced tools and solutions to help businesses meet today's demanding data and mobile device security policy requirements.

4 Through a combination of security services, settings, and features, the Windows Mobile security architecture helps protect critical data and systems from exposure and theft. Windows Mobile 5.0 MSFP enables the establishment of a strong password policy and the ability to wipe the device in response to a defined number of failed authentication attempts.

5 To help simplify enterprise administration of mobile solutions, Windows Mobile also provides centralized device management features, such as the ability to perform a remote wipe, verify passwords, and enforce security policies over the air to multiple devices simultaneously.

6 As illustrated in Figure 1, the security and device management features of Windows Mobile 5.0 MSFP deliver a secure mobile messaging solution with simplified administration, increased monitoring, and flexible policy management.

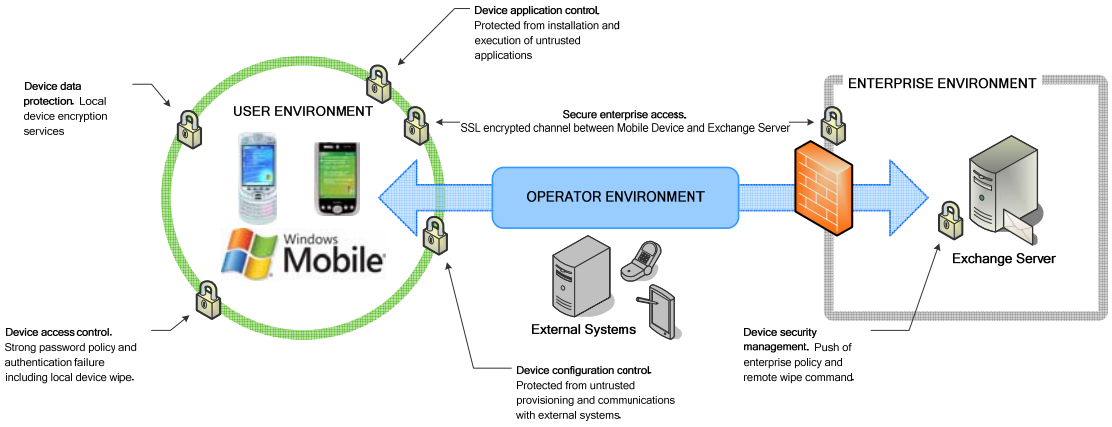

Figure 1 – Windows Mobile 5.0 MSFP security architecture

1.2 ST and TOE identification

Table 1 – ST and TOE identification information

ST Title	Windows Mobile 5.0 MSFP Security Target
ST Version	1.0, 25-Feb-08
TOE Software	Windows Mobile Version 5.0 MSFP (Messaging and Security Feature Pack (MSFP), derived from Windows CE 5.1, which includes the following editions: • Windows Mobile 5.0 MSFP for Smartphone • Windows Mobile 5.0 MSFP for Pocket PC Phone Edition This evaluation includes the following Adaptation Kit Updates (AKUs): • Build 14847 AKU 2.0 • Build 14914 AKU 2.1 • Build 14928 AKU 2.2 • Build 14929 AKU 2.2.1 • Build 14932 AKU 2.2.2 • Build 14955 AKU 2.3 • Build 14957 AKU 2.3.1 • Build 14959 AKU 2.3.2 • Build 14960 AKU 2.4 • Build 14967 AKU 2.5 • Build 14989 AKU 2.6 • Build 14992 AKU 2.6.1 • Build 14994 AKU 2.6.2 • Build 14995 AKU 2.6.3 • Build 15096 AKU 3.0 • Build 15097 AKU 3.0.1 • Build 15314 AKU 3.1 • Build 15633 AKU 3.2 • Build 15671 AKU 3.3 • Build 15673 AKU 3.3.1 • Build 15359 AKU 3.4 • Build 15361 AKU 3.4.1 • Build 15362 AKU 3.4.2 • Build 15363 AKU 3.4.3

	• Build 15704 AKU 3.5 • Build 15705 AKU 3.5.1 • Build 15706 AKU 3.5.2
Assurance Level	EAL2 augmented with ALC_FLR.1
CC Identification	Common Criteria for Information Technology (IT) Security Evaluation, Version 2.3, August 2005. International Standard – International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 15408:1999.

1.3 Conformance Claims

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

a) **Part 2 extended.** Extends the Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 2.3, August 2005, CCMB-2005-002.

b) **Part 3 conformant, EAL2 augmented.** Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 2.3, August 2005, CCMB-2005-003. Evaluation is EAL2 augmented with ALC_FLR.1.

1.4 Strength of function

8 The EAL2 (augmented with ALC_FLR.1) Common Criteria evaluation of Windows Mobile 5.0 MSFP provides a basic level of independently assured security.

9 The assurance requirements and the minimum Strength of Function (SOF) of basic (SOF-basic) were chosen to be consistent with this security objective.

1.5 Document conventions

10 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 2 – 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.
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.

Term	Description
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 Exchange Server	The Microsoft Exchange Server used within the enterprise to communicate with Mobile Devices to provide policy and configuration information and for user's to access their Exchange Mailbox.
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.
Exchange ActiveSync Mailbox Policy	The password and device management policy that can be applied to a device by the Enterprise Administrator through Exchange ActiveSync.
Exchange Commands	Commands that can be sent to the Mobile Device to either perform a remote wipe or remove a partnership.
Exchange Management Console	The external user interface provided for the Enterprise Administrator to establish mobile device policy and security configurations.
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.
Local Device Wipe	The wipe of TOE Security Function (TSF) and user data in response to reaching the threshold for failed authentication attempts.

Term	Description
Mailbox Items	Items that can be synchronized through Exchange ActiveSync such as emails, contacts, tasks and calendar appointments.
MSFP	Messaging and Security Feature Pack is an addition to the Windows Mobile 5.0 operating system that has been incorporated since AKU 2.0.
Mobile Device	The physical device, either Smartphone or Pocket PC, that provides the hardware platform for the installation of the Windows Mobile 5.0 MSFP 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.
Remote Device Wipe	The wipe of TSF and user data in response to an Exchange Command issued from the Enterprise Exchange Server.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.

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

1.7 References

[1] Deploying Windows Mobile 6 Powered Devices with Microsoft Exchange Server 2007, Microsoft white paper, Nov-07.

[2] Windows Mobile 5.0 MSFP Installation and Administrator Guide, Feb-08.

[3] Security for Windows Mobile Messaging in the Enterprise, Microsoft white paper, Feb-07.

[4] Microsoft Windows CE and Windows Mobile Enhanced Cryptographic Provider 5.00.911762, 5.01.01603 and 5.04.17228: FIPS 140-2 Documentation (Security Policy), Microsoft document, 30-Mar-07

1.8 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 Overview

12 Windows Mobile 5.0 MSFP is a single user operating system designed for use with Smartphone and Pocket PC devices. The intended method of use of the TOE is as a mobile messaging solution that allows users to stay connected to their email, contacts and calendar whilst away from their enterprise workstation.

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

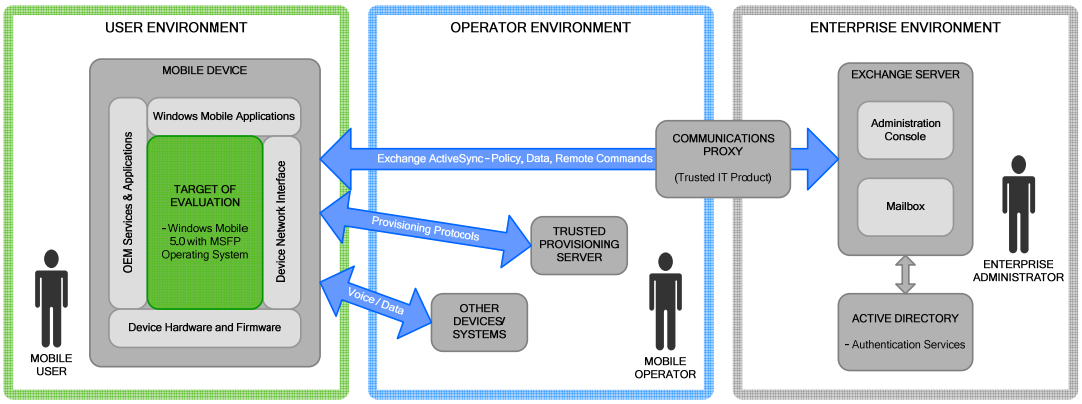

Figure 2 – The TOE operating environment

2.2 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 5.0 MSFP 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 5.0 MSFP operating 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.

2.3 Operator environment

18 The operator environment is provided and controlled by the Mobile Operator. Continual provisioning can occur within this environment so that the Mobile Device can be updated with new capabilities and services.

19 The Mobile Device must also be capable of communicating with other devices and systems using a range of communication mechanisms, including WAP, Wi-Fi and voice.

2.4 Enterprise environment

20 Users can use the TOE to gain access to resources residing on corporate networks through use of the Exchange ActiveSync protocol which establishes a secure communications link between the enterprise and the Mobile Device using methods such as SSL/HTTPS.

21 The TOE is supported by a trusted management console which provides configuration and policy data to the TOE over the Exchange ActiveSync communications channel. The Exchange Management Console is provided by Exchange Server, which while outside the scope of this evaluation, provides a mechanism for securely communicating and configuring the TOE. The TOE sends and receives email, calendar and contacts information to and from a trusted email server that has been configured to do so.

22 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.

23 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.

24 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.

2.5 TOE Security Features

25 Table 3 highlights the range of security functions and features that the TOE implements.

Table 3 – TOE security functions and features

Security function	TOE security feature
Device data protection. The TOE provides the capability to protect data in transit.	**SSL/TLS channel encryption.** SSL/TLS encrypts data transmitted between the device and server, over-the-air or through a wired connection.
	Certified cryptographic module. The TOE includes a certified FIPS validated cryptographic module. Applications can make use of cryptographic modules to perform cryptographic operations.
Device application control. The TOE provides the capability to only permit trusted applications to be installed and executed 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 operating system.
	Controlled application execution. Code execution control allows the device to be locked so that only applications signed with a trusted certificate can run.
Secure enterprise access. The TOE provides the capability to securely synchronize data items with the Mobile User's Exchange Mailbox.	**Secure channel.** Windows Mobile establishes a secure channel for communicating with another trusted IT product.
	Synchronization of Mailbox Items. Mobile Users can apply the secure channel to synchronize their emails, tasks, calendar and contacts with their enterprise mailbox.
Device configuration control. The TOE provides the capability to protect against modification by un-trusted systems.	**Exchange ActiveSync Mailbox Policy.** The Enterprise Administrator can use the secure channel to push down an enterprise policy for the Mobile Device.
	Trusted provisioning. Windows Mobile can implement secure communications with a trusted source that has the ability to provide provisioning and configuration data.
	Local configuration control. The authenticated user has the ability to locally manage specific configurations and settings.
Device access control. The TOE has inbuilt security mechanisms that can be enabled to provide controlled	**Device authentication and lock.** Windows Mobile can be configured to require a password to gain access to the Mobile Device, however, it is possible to receive incoming calls and to make emergency calls without authenticating.

Security function	TOE security feature
access to the Mobile Device.	**Local device wipe.** Windows Mobile can be configured to perform a local device wipe after a specified number of incorrect login attempts. **Note:** This feature only wipes TSF and user data on the Mobile Device. Data is not wiped from installed removable storage cards.
Device security management. The TOE has configurable security policies that establish which actions a user or application may take.	**Security roles.** Windows Mobile maintains multiple management roles which determine access to device resources.
	Security policies. Security policies establish the foundation configuration for the Mobile Device, they can be set to configure low-level device configuration policies and also implement enterprise password policy.
	Remote wipe. The Enterprise Administrator can issue a command to wipe a managed device if it has been lost or stolen. **Note:** This feature only wipes TSF and user data on the Mobile Device. Data is not wiped from installed removable storage cards.

2.6 Scope of the TOE

26 The TOE comprises the core software components of Windows Mobile 5.0 MSFP operating 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.

27 Windows Mobile 5.0 MSFP 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.

28 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.

29 In the evaluated configuration, all communication between the TOE and the Exchange Management Console, Exchange Server, and data resources are mediated by the Communications Proxy. The Communications Proxy is a trusted IT product that is used to establish a trusted path for the secure communication of both TSF and user data.

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

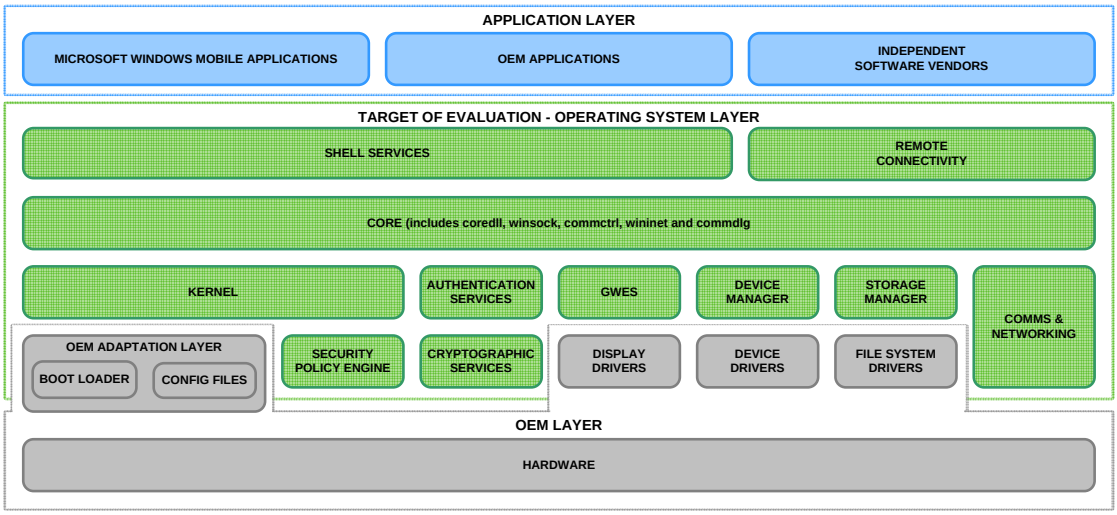

Figure 3 – TOE Scope

3 TOE Security Environment

3.1 Overview

31 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: • follow user guidance, • ensure that the TOE continues to operate in the evaluated configuration, • only permit ActiveSync connections between the Mobile Device and trusted computing devices, and • 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 Enterprise Exchange Server and Active Directory Server are located within the enterprise boundary and are protected from unauthorized logical/physical access.
A.IT_MOBILE	The Trusted Provisioning Server is located within the Mobile Operator's network boundary and is protected from unauthorized logical and 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.OPERATOR	The Mobile Operator will not transmit configuration messages that undermine the security objectives of the TOE.
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.

Identifier	Assumption statement
A.COMMS_ENT	The IT environment will provide the server-side of a secure channel between the Enterprise Exchange Server and the Mobile Device.
A.COMMS_NET	The IT environment will provide the server-side of a secure channel between the Trusted Provisioning Server and the Mobile Device.
A.SEC_POLICY	The IT environment will provide a mechanism for setting enterprise policy and pushing it to the Mobile Device.

3.3 Threats to security

Table 5 – Threats to security

Identifier	Threat statement
T.EAVESDROPPING	An attacker may compromise the confidentiality of user or TSF data by monitoring communications between the TOE and either the Enterprise Exchange Server or Trusted Provisioning Server.
T.INTERCEPT	An attacker may compromise the integrity of user data or TSF data by intercepting and altering communications between the TOE and either the Enterprise Exchange Server or Trusted Provisioning Server.
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 and/or TSF data.
T.MASQUERADE	An attacker may masquerade as the Enterprise Exchange Server or a Trusted Provisioning Server and attempt to compromise the integrity of the TSF by sending malicious management messages to the TOE.
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 stored on the Mobile Device.
T.WEAK_SECRET	A user may select a weak password thereby enabling an attacker to compromise the confidentiality of user data.

4 Security objectives

4.1 Overview

32 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 data and TSF data transmitted between the TOE and the Enterprise Exchange Server and the Trusted Provisioning Server.
O.COMMS_INT	The TOE shall preserve the integrity of user data and TSF data transmitted between the TOE and the Enterprise Exchange Server and the Trusted Provisioning Server.
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 on the Mobile Device.
O.LOCAL_WIPE	The TOE shall be able to make user and TSF data stored on the Mobile Device 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.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.

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 the Enterprise Exchange Server.
OE.COMMS_NET	The IT environment must authenticate the end-points and encrypt communications between the Mobile Device and the Trusted Provisioning Server.
OE.SEC_POLICY	The IT environment must provide an administration console for securely creating and applying security policies and issuing remote commands to the Mobile Device.

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: • follow user guidance relating to the operating system, installed applications and the Mobile Device; • 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; • only permit ActiveSync connections between their Mobile Device and computing devices that can be trusted; and • 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 Enterprise Exchange Server and Active Directory Server are protected from unauthorized logical and physical access.
OE.IT_MOBILE	The Mobile Operator shall ensure that the Trusted Provisioning Server is located within the Mobile Operator's network boundary and is 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.
OE.OPERATOR	The Mobile Operator shall not transmit configuration messages that undermine the security objectives of the TOE.

5 IT Security Requirements

5.1 Overview

33 This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 2.3 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

5.2 TOE Security Functional Requirements

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

35 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 1.4 of this ST.

Table 9 – Summary of TOE Security Functional Requirements

Identifier	Title
Device data protection	
FCS_CKM.1	Cryptographic key generation
FCS_COP.1	Cryptographic operation (SSL/TLS)
FCS_CKM.4	Cryptographic key destruction
Device application control	
FDP_ACC.1a	Subset access control (Device Application Control SFP)
FDP_ACF.1a	Security attribute based access control (Device Application Control SFP)
Secure enterprise access	
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
Device configuration control	
FDP_ACC.1b	Subset access control (Device Configuration Control SFP)
FDP_ACF.1b	Security attribute based access control (Device Configuration Control SFP)
Device access control	

Identifier	Title
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
Device security management	
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.2	Secure security attributes
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 Device data protection

5.2.1.1 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, and** **b) 3DES**] and specified cryptographic key sizes [**a) 384 through to a maximum 16384 bits (RSA), and** **b) 168 bits (3DES)**] that meet the following: [**a) RFC 2437 "PKCS #1: RSA Cryptography Specifications Version 2.0", October 1998; and** **b) Federal Information Processing Standard (FIPS) Publication 46-3, "Data Encryption Standard", 25 October 1999.**].
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes
Notes:	None.

5.2.1.2 FCS_COP.1 Cryptographic operation (SSL/TLS)

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [**encryption, decryption and digital signing for Exchange ActiveSync and Trusted Provisioning communications**] 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), and** **b) 168 bits (3DES),** **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; and** **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 FMT_MSA.2 Secure security attributes
Notes:	None.

5.2.1.3 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] FMT_MSA.2 Secure security attributes
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.

5.2.2 Device application control

5.2.2.1 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 cpf file extension),** **ii. Themes (hme and tsk file extensions),** **iii. Dynamic Link Libraries (dll file 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 SFP specifies the rules for implementing controls associated with both installing and executing applications on the TOE. 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.

5.2.2.2 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 Theme files digitally 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 execute on the TOE.** **ii. Unsigned Executables or DLLs will require permission from the Mobile User to access device resources and execute on 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 5.0 MSFP Installation and Administrator Guide (Ref. [2]).

5.2.3 Secure enterprise access

5.2.3.1 FDP_IFC.1 Subset 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, and** **ii. Enterprise Exchange Server.** **b) Information:** **i. Exchange ActiveSync Mailbox Policy,** **ii. Exchange Commands, and** **iii. Mailbox Items.** **c) Operations:** **i. Synchronize Mailbox Items,** **ii. Apply Exchange ActiveSync Mailbox Policy, and** **iii. Receive Remote Wipe Command**].
Dependencies:	FDP_IFF.1 Simple security attributes
Notes:	The Secure Enterprise Access SFP demonstrates that the Mobile Device communicates securely with the Enterprise Exchange Server for three different types of information exchanges. The Exchange Server can provide updates of security policy, known as the Exchange ActiveSync Mailbox Policy, which contains specific details on enterprise password policy for the Mobile Device. 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 issue Exchange Commands through the Enterprise Exchange Server to remove existing device partnerships, or to remotely wipe the Mobile Device of all user and TSF data.

5.2.3.2 FDP_IFF.1 Simple 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. Root (system) certificate store.** **b) Enterprise Exchange Server:** **i. Private key**].
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) For all specified operations the Mobile Device must have the certificate that relates to the private key of the Enterprise Exchange Server located within the Root (system) Certificate Store in order to establish an authenticated and secure connection** **b) The Mobile Device must have SSL/TLS encryption enabled for enterprise communications**].
FDP_IFF.1.3	The TSF shall enforce the [**None**].
FDP_IFF.1.4	The TSF shall provide the following [**capabilities for each operation:** **a) If the IT environment successfully authenticates the Mobile User Mailbox Items can be synchronized with the Exchange Mailbox in accordance with the rules established by the Mobile User.** **b) Apply new or modified Exchange ActiveSync Mailbox Policy pushed from the Enterprise Exchange Server to the TOE.** **c) In response to receipt of the Remote Wipe Command from the Enterprise Exchange Server the TOE will wipe all TSF and user data on the TOE**].
FDP_IFF.1.5	The TSF shall explicitly authorise an information flow based on the following rules: [**None**].
FDP_IFF.1.6	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 initialisation

Notes:	The Secure Enterprise Access SFP relates to the Exchange ActiveSync capability and not Desktop ActiveSync (often referred to simply as ActiveSync). Using SSL/TLS to protect Exchange ActiveSync communications is a configurable setting that is described in the Windows Mobile 5.0 MSFP Installation and Administrator Guide (Ref. [2]). Data stored on an inserted removable storage card will not be wiped. Once device wipe command has been issued by the Enterprise Exchange Server device wipe will only occur once the message has been received by the target Mobile Device.

5.2.3.3 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 a remote 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 or the remote trusted IT product***] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [**synchronizing Mailbox Items**].
Dependencies:	No dependencies.
Notes:	An ISA server at the enterprise boundary provides an application-layer firewall to control information flow back to the enterprise mail server and other data resources. The ISA server also provides a termination point for encrypted communications with the Mobile Device. The use of a Microsoft ISA Server at the enterprise boundary is considered best practice and is Microsoft's recommended architecture for deployment of a mobile messaging solution. The Trusted IT product initiates communication via the trusted channel for updating the Exchange ActiveSync Mailbox Policy and sending Exchange Commands such as Perform Remote Wipe. This functionality is required by the IT environment.

5.2.4 Device configuration control

5.2.4.1 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.

5.2.4.2 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:** **ii. 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 the configuration of the Mobile Device 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 initialisation
Notes:	None.

5.2.5 Device access control

5.2.5.1 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 or surpassed, 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 the Exchange ActiveSync Mailbox Policy.

5.2.5.2 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) Enterprise User Identifier,** **d) Exchange Authentication Data,** **e) Exchange Server Address, and** **f) Email address**].
Dependencies:	No dependencies.
Notes:	As Windows Mobile 5.0 MSFP is a single-user operating system there is no concept of a user identifier. However, the TOE does maintain the Exchange User Identifier for the Mobile User.

5.2.5.3 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 Enterprise Administrator and must be specified in the Exchange ActiveSync Mailbox Policy. The Windows Mobile 5.0 MSFP Installation and Administrator Guide (Ref. [2]) includes details for establishing the appropriate Exchange ActiveSync Mailbox Policy.

5.2.5.4 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) receipt of the Remote Wipe Command from the Exchange Server**] 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.

5.2.5.5 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.

5.2.5.6 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 the Exchange ActiveSync Mailbox 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 the Exchange ActiveSync Mailbox Policy.

5.2.5.7 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.

5.2.6 Device security management

5.2.6.1 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.

5.2.6.2 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.

5.2.6.3 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.

5.2.6.4 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.

5.2.6.5 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.

5.2.6.6 FMT_MSA.2 Secure security attributes

Hierarchical to:	No other components.
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for security attributes.
Dependencies:	ADV_SPM.1 Informal TOE security policy model [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

5.2.6.7 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.

5.2.6.8 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.

5.2.6.9 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.

5.2.6.10 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) manage device data protection,** **b) manage device 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.

5.2.6.11 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) Manufacturer (SECROLE_OEM)** **c) Operator (SECROLE_OPERATOR)** **d) Manager (SECROLE_MANAGER)** **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_TRUSTED_PPG)** **j) Push Initiator Authenticated (SECROLE_PPG_AUTH)** **k) Trusted Push Proxy Gateway (SECROLE_PPG_TRUSTED)** **l) Enterprise (SECROLE_ENTERPRISE)**].
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

36 The assurance package for the evaluation of Windows Mobile 5.0 MSFP is Evaluation Assurance Level 2 (EAL2), augmented by the life cycle support component that provides basic flaw remediation (ALC_FLR.1).

37 EAL2 assurance requirements provide confidence 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.

38 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.

39 EAL2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

40 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
ACM: Configuration management	ACM_CAP.2 Configuration items
ADO: Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
ALC: Life cycle support	ALC_FLR.1 Basic flaw remediation
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

5.4 Security Requirements for the IT Environment

41 This section specifies the security requirements that are to be provided by the IT environment to support the TOE and the security objectives on the IT environment. Table 11 provides a summary of the IT security functions relevant to the IT environment.

42 The IT environment needs to provide the following supporting functionality:

a) **Identification and Authentication.** The TOE relies on Active Directory to authenticate Mobile Users when using Exchange ActiveSync to access their enterprise mailbox and associated Exchange Mailbox Items.

b) **Communications Security.** The TOE communicates securely with the enterprise using SSL/TLS to support a secure communications channel over Exchange ActiveSync.

c) **Security management.** The environment must provide both the Enterprise Administrator and the Mobile Operator roles to support the secure management and configuration of the TOE.

Table 11 – Summary of IT environment security functional requirements

Identifier	Title
FCS: Cryptographic support	
FCS_CKM.1	Cryptographic key generation
FCS_COP.1	Cryptographic operation (SSL/TLS)
FCS_CKM.4	Cryptographic key destruction
FIA: Identification and Authentication	
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FIA_ATD.1	User attribute definition
FMT: Security management	
FMT_MOF.1a	Management of security functions behaviour (Enterprise)
FMT_MOF.1b	Management of security functions behaviour (Operator)
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FTP: Trusted path/channels	
FTP_ITC.1	Inter-TSF trusted channel

5.4.1 FCS: Cryptographic support

5.4.1.1 FCS_CKM.1 Cryptographic key generation

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

5.4.1.2 FCS_COP.1 Cryptographic operation (SSL/TLS)

Hierarchical to:	No other components.
FCS_COP.1.1	The **IT environment** shall perform [**encryption, decryption and digital signature functions for Exchange ActiveSync and Trusted Provisioning communications**] 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; and** **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 FMT_MSA.2 Secure security attributes
Notes:	None.

5.4.1.3 FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
FCS_CKM.4.1	The **IT environment** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zeroization**] 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] FMT_MSA.2 Secure security attributes
Notes:	None.

5.4.2 FIA: Identification and Authentication

5.4.2.1 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication.
FIA_UAU.2.1	The **IT environment** shall require each user to be successfully authenticated before allowing any TSF-mediated actions on behalf of that user.
Dependencies	FIA_UID.1 Timing of Identification
Notes:	To authenticate a user when accessing an enterprise mailbox, the Mobile Device passes the cached user's enterprise credentials to the Exchange Server, which authenticates the user against the Active Directory.

5.4.2.2 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The **IT environment** shall require each user to identify itself before allowing any TSF-mediated actions on behalf of that user.
Dependencies	No dependencies.
Notes:	See notes for FIA_UAU.2.

5.4.2.3 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.
FIA_ATD.1.1	The **IT environment** shall maintain the following list of security attributes belonging to individual users: [**a) Enterprise User Identifier,** **b) Group Memberships,** **c) Mailbox,** **d) Enterprise Authentication Data,** **e) Private Keys, and** **f) Privileges**].
Dependencies	No dependencies.
Notes:	None.

5.4.3 FMT: Security management

5.4.3.1 FMT_MOF.1a Management of security functions behaviour (Enterprise)

Hierarchical to:	No other components.
FMT_MOF.1a.1	The **IT environment** shall restrict the ability to [***enable, disable or modify the behaviour of***] the functions [**a) generate and send Exchange ActiveSync Mailbox Policy,** **b) generate and send Exchange Commands, and**] to [**Enterprise (SECROLE_ENTERPRISE)**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.4.3.2 FMT_MOF.1b Management of security functions behaviour (Operator)

Hierarchical to:	No other components.
FMT_MOF.1b.1	The **IT environment** shall restrict the ability to [***enable, disable or modify the behaviour of***] the functions [**generate and send XML Provisioning Documents**] to [**Operator (SECROLE_OPERATOR)**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.4.3.3 FMT_SMF.1 Specification of management functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The **IT environment** shall be capable of performing the following security management functions: [**a) generate and send Exchange ActiveSync Mailbox Policy (Enterprise),** **b) generate and send Exchange Commands (Operator), and** **c) generate and send XML Provisioning Documents (Operator or Enterprise)**].
Dependencies:	No dependencies.
Notes:	The IT environment provides the capability to set and establish enterprise policy that can be applied to the device through Exchange ActiveSync or OMA-DM and secure provisioning protocols.

5.4.3.4 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The **IT environment** shall maintain the roles [**a) Enterprise (SECROLE_ENTERPRISE)** **b) Operator (SECROLE_OPERATOR)**]
FMT_SMR.1.2	The **IT environment** shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	The enterprise environment provides the Enterprise Administrator role and the operator environment provides the Mobile Operator role.

5.4.4 FTP: Trusted path/channel

5.4.4.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to:	No other components.
FTP_ITC.1.1	The **IT environment** shall provide a communication channel between itself and a remote 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 **IT environment** shall permit [***the TSF or the remote trusted IT product***] to initiate communication via the trusted channel.
FTP_ITC.1.3	The **IT environment** shall initiate communication via the trusted channel for [**a) applying Exchange ActiveSync Mailbox Policy, and** **b) sending Exchange Commands**].
Dependencies:	No dependencies.
Notes:	This SFR provides the enterprise-side of the trusted channel between the Mobile Device and a remote trusted IT product.

6 TOE Summary Specification

6.1 Overview

43 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

44 The TOE security functions include the following:

a) **Device data protection.** The TOE provides the capability to protect data 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 synchronize data items with the Mobile User's Exchange Mailbox.

d) **Device configuration control.** The TOE provides the capability to protect against modification by un-trusted systems.

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

f) **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 SSL/TLS channel encryption

45 Enterprise Administrator can allow, or require, Windows Mobile-powered devices to create SSL/TLS encrypted connections with the Enterprise Exchange Server. By default, SSL/TLS encrypted connections are 128-bit.

46 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.

6.2.1.2 Certified cryptographic module

47 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.

48 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.

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

50 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.

51 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) SHA-1 hash,

k) SHA-256, SHA-384, SHA-512,

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

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

n) 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 Device application control

6.2.2.1 Controlled application installation

52 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.

53 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.

54 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.

6.2.2.2 Controlled application execution

55 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.

56 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.

6.2.3 Secure enterprise access

6.2.3.1 Secure channel

57 The Exchange Server mobile messaging features are implemented using the Exchange ActiveSync (EAS) protocol, which consists of two separate components. The EAS server component is included as part of the Exchange Server installation process. The EAS client component is included with Windows Mobile.

58 Windows Mobile software supports Microsoft Exchange ActiveSync features that can create a protected connection to the corporate Microsoft Exchange Server. With Exchange ActiveSync, the Mobile Device must establish a secure channel with the Exchange Server to ensure that both TSF and user data can pass in a secure manner.

59 In the Windows Mobile security architecture, SSL/TLS plays an important role in protecting device communications. The preferred method for establishing Exchange ActiveSync connections requires the use of SSL/TLS to encrypt the connection between the Mobile Device and the Enterprise Exchange Server.

6.2.3.2 Synchronization of Mailbox Items

60 Mobile Users can access their corporate Mailbox on the Enterprise Exchange Server by using Exchange ActiveSync, which allows the sending and receipt of e-mail, calendar, contact, and task data through Exchange Servers on the corporate network. Exchange ActiveSync connections are protected with 128-bit SSL/TLS encryption.

61 With Exchange ActiveSync, e-mail, calendar information, and other Exchange Items such as contacts and tasks, can be accessed quickly from off-site locations.

62 Synchronization can be set to occur automatically from as often as every five minutes to as seldom as every four hours, or even to only occur when manually invoked. Alternatively, synchronization can be set to occur when a new message arrives at the Exchange Server.

6.2.4 Device configuration control

6.2.4.1 Exchange ActiveSync Mailbox Policy

63 The Enterprise Administrator has the ability to enforce password and device configuration policies on the Mobile Device through the Exchange Management Console.

64 Exchange Server has the capability to create security policies that are delivered to the Mobile Device through Exchange ActiveSync. The device implements the policy and takes action when it receives the policy information from the server. Different devices have differing levels of support for Exchange ActiveSync policies, which can specify several aspects of device security:

a) Whether or not a device must be locked with a password.

b) The minimum length of the password.

c) Whether the password can be numeric-only or alphanumeric.

d) Whether failed password entry attempts should trigger a local device wipe.

65 When a Mobile Device security policy is defined, it is automatically sent to each device the next time that device starts synchronization. The Mobile User can choose to accept or decline the policy. However, the Enterprise Administrator can specify whether devices that reject the policy (or that don't implement it) may still connect.

66 The Enterprise Administrator may also define a list of Mobile Users who are exempt from security policy controls. This is useful for exempting users with special requirements, or whose devices don't completely implement the client-side Exchange ActiveSync capabilities.

6.2.4.2 Trusted provisioning

67 Windows Mobile supports Open Mobile Alliance Device Management (OMA DM). The DM client in the device supports the following security features:

a) Secure transport over SSL/TLS.

b) Device management application level client authentication.

c) Device management application level server authentication.

d) Authenticating server notification trigger.

e) Windows Mobile security role-based access control.

68 Windows Mobile-powered devices can be managed by using XML-based provisioning documents to configure operating system and application settings, including security settings. These provisioning documents can be applied to multiple Mobile Devices. The XML provisioning documents are distributed through:

a) **Over-the-air synchronizations with a device management server on the network.** This server could be Microsoft Systems Management Server (SMS), Exchange, a third-party device management solution, or a device management server operated by a Mobile Operator.

b) **Deployment in a cabinet provisioning format file (.cpf).** Application installation files are known as cabinet files (.cab); the .cpf file is a special type of cabinet file that contains the XML provisioning document. The device can download the .cpf file from a provisioning server or from an attached desktop.

69 For large deployments of Windows Mobile-powered devices, the XML provisioning not only reduces deployment efforts, but also helps standardize security settings. Along with security settings, XML provisioning allows Enterprise Administrators to create a standard configuration for Mobile Devices, including wireless and other network settings, Internet connection, and e-mail synchronization settings.

6.2.4.3 Local configuration control

70 The TOE can be configured locally by the authenticated Mobile User so that Bluetooth, Infrared, SMS, MMS and Wi-Fi communications can be enabled or disabled.

71 Through the device security policies, and locally, through the control panel, the Mobile User is capable of disabling and enabling specific communications methods and ensuring that all communications are expressly permitted.

6.2.5 Device access control

6.2.5.1 Device authentication and lock

72 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.

73 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.

74 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.

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

76 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

6.2.5.2 Local device wipe

77 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).

78 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.

79 Only data located on the mobile device will be wiped. Any data stored on an inserted removable storage card will not be wiped.

6.2.6 Device security management

6.2.6.1 Security roles

80 The TOE maintains multiple management roles which determine an individual’s degree of access to device resources.

81 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.

82 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 Exchange Administrator role, or known as the Enterprise Administrator in the context of the TOE. 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.

6.2.6.2 Security policies

83 The TOE can be configured through specific security policies to only accept certain over the air (OTA) provisioning protocols and messages.

84 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.

85 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.

86 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.

6.2.6.3 Remote wipe

87 Remote wipes occur when the Enterprise Administrator issues an explicit wipe command through the Exchange Management Console. 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.

88 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.

89 Only data located on the mobile device will be wiped. Any data stored on an inserted removable storage card will not be wiped.

6.3 Strength of Function claim

90 SOF claims are made for all permutational or probabilistic mechanisms that are non-cryptographic in nature. Device authentication and lock is the only permutational/probabilistic mechanism implemented in the TOE.

91 The SOF claim for the *device authentication and lock* mechanism is SOF-basic.

6.4 Assurance Measures

92 The following groups of assurance measures are applied to Windows Mobile to satisfy CC EAL2 augmented with flaw remediation:

a) configuration management,

b) delivery and operation,

c) development,

d) guidance documents,

e) life cycle support,

f) tests, and

g) vulnerability assessment.

6.4.1 Configuration management

93 The Configuration Management (CM) measures applied by Microsoft ensure that Configuration Items (CIs) are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE.

94 Microsoft ensures changes to the implementation representation are controlled with the support of automated tools and that TOE associated CI modifications are properly controlled. Microsoft performs CM on the TOE implementation representation, design, tests, user and administrator guidance, the CM documentation, lifecycle documentation and vulnerability analysis.

95 Microsoft ensures that the TOE is uniquely referenced and labeled with its own reference. Microsoft uses, and documents how they use, automated tools to support TOE generation.

96 These activities are documented in the Windows Mobile 5.0 MSFP & 6 Configuration Management Documentation.

6.4.2 Delivery and operation

97 Microsoft provides delivery documentation and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up.

98 Microsoft's delivery procedures describe the electronic and non-electronic procedures to be used to detect modification to the TOE. The installation and generation procedures describe the steps necessary to place Windows Mobile and the device into the evaluated configuration.

99 Delivery procedures are documented in the Windows Mobile 5.0 MSFP & 6 Delivery Process.

100 Installation, generation and start-up information is contained in the Windows Mobile 5.0 MSFP Installation and Administrator Guide.

6.4.3 Development

101 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 5.0 MSFP 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 5.0 MSFP High-Level Design.** The high-level design of Windows Mobile 5.0 MSFP provides a description of the TSF in terms of subsystems and relates these units to the functions that they provide.

c) **Windows Mobile 5.0 MSFP Correspondence Demonstration.** This document provides correspondence between the various representations provided for the EAL2 evaluation.

6.4.4 Guidance documents

102 Microsoft provides administrator and user guidance on how to perform the TOE security functions and warnings to authorized administrators and users about actions that can compromise the security of the TOE.

103 Administrator guidance is documented in the Windows Mobile 5.0 MSFP Installation and Administrator Guide.

104 User guidance is provided in help files contained on the Windows Mobile powered device and is supplemented by the Windows Mobile 5.0 MSFP & 6 User Guide Supplement.

6.4.5 Life cycle support

105 Microsoft applies procedures to accept and act upon reported security flaws. Microsoft designates specific points of contact for user reports and security related inquiries.

106 The procedures are documented and describe how security flaws are tracked and that for each security flaw a description and status of the correction is provided.

107 The procedures ensure that all reported flaws are addressed by Microsoft and that corrections do not introduce new flaws. The procedures also ensure a timely response to reported flaws and the automatic distribution of reports to the affected users.

108 These activities are documented in the Windows Mobile 5.0 MSFP & 6 Flaw Remediation Process.

6.4.6 Tests

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

110 The Windows Mobile 5.0 MSFP & 6 Security Testing document consists of the following:

a) **Test plan.** The test plan describes the form, content, and organization of test documentation. It also summarizes each of the test suites and includes high-level procedures for exercising the tests.

b) **Test procedures.** The test procedures include both documentation and an actual implemented test (if applicable). Test suites 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.

c) **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.

6.4.7 Vulnerability assessment

111 Documented analysis of the strength of TSF has been created to support the SOF claims for the TOE.

112 Microsoft has performed a vulnerability analysis of Windows Mobile to identify weaknesses that can be exploited in the TOE. Microsoft documents the status of identified vulnerabilities and demonstrates that for each vulnerability, the vulnerability cannot be exploited in the intended environment and that the TOE is resistant to obvious penetration attacks.

113 Strength of function analysis is provided in the Windows Mobile 5.0 MSFP & 6 SOF Analysis document.

114 Vulnerability analysis is documented in the Windows Mobile 5.0 MSFP & 6 Vulnerability Assessment document.

7 Rationale

7.1 Overview

115 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 12 – Mapping of TOE security objectives to threats

Threats	Objective	Justification
T.EAVESDROPPING	O.COMMS_CONF	The threat of eavesdropping is mitigated by implementing mechanisms to preserve the confidentiality of transmitted data.
T.INTERCEPT	O.COMMS_INT	The threat of interception is mitigated by implementing mechanisms 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.
T.TOE_ACCESS	O.USER_AUTH O.REMOTE_WIPE O.LOCAL_WIPE O.SESSION_LOCK O.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. • O.REMOTE_ADMIN enables the Enterprise Administrator to apply remote wipe commands.

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.

7.2.2 Security objectives for the non-IT environment

Table 13 – 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 of the TOE in normal operating conditions are appropriately protected.
A.IT_MOBILE	OE.IT_MOBILE	This objective for the environment ensures that the assumption is upheld that the Trusted Provisioning Server, bootstrapped to provision the TOE, is protected.
A.ADMIN	OE.ADMIN	This objective for the environment upholds the assumption that administration personnel can be trusted.
A.OPERATOR	OE.OPERATOR	This objective for the environment ensures that the assumption is upheld that the network provider does not undermine the security functionality of the TOE.

7.2.3 Security objectives for the IT environment

Table 14 – 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.COMMS_NET	OE.COMMS_NET	This objective for the IT environment ensures that the assumption is upheld that the user environment 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 15 – 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 FMT_MSA.2 Secure security attributes	FCS_COP.1 FCS_CKM.4 FMT_MSA.2
FCS_COP.1	[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 FMT_MSA.2 Secure security attributes	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2
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] FMT_MSA.2 Secure security attributes	FCS_CKM.1 FMT_MSA.2
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

SFR	Dependency	Inclusion
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
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.2	ADV_SPM.1 Informal TOE security policy model [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Not included – see rational below. FDP_ACC.1 and FDP_IFC.1 FMT_MSA.1 FMT_SMR.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

SFR	Dependency	Inclusion
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

116 ADV_SPM.1 is a dependency of FMT_MSA.2 that has not been included. In this case, the requirement for an Informal Security Policy Model (ISPM) has been met by a clear statement of the TOE security policy within this Security Target. In addition, the subordinate policies are straightforward and complete.

117 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 16 – 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 IT environment SFR dependency demonstration

Table 17 – IT environment 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 FMT_MSA.2 Secure security attributes	 FCS_COP.1 FCS_CKM.4 FMT_MSA.2
FCS_COP.1	[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 FMT_MSA.2 Secure security attributes	 FCS_CKM.1 FCS_CKM.4 FMT_MSA.2
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] FMT_MSA.2 Secure security attributes	 FCS_CKM.1 FMT_MSA.2
FIA_UAU.2	FIA_UID.1 Timing of Identification	FIA_UID.2
FIA_UID.2	No dependencies	N/A
FIA_ATD.1	No dependencies	N/A
FMT_MOF.1a	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1

SFR	Dependency	Inclusion
FMT_MOF.1b	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FTP_ITC.1	No dependencies	N/A

7.3.5 TOE IT requirements correspondence

Table 18 – Mapping TOE SFRs to objectives

Objective	SFRs	Demonstration
O.COMMS_CONF	FCS_CKM.1 FCS_COP.1 FCS_CKM.4	FCS_CKM.1 provides support for implementing communications that have both confidentiality and integrity security properties. FCS_COP.1 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.1 and FCS_CKM.4 combine to ensure that the O.COMMS_CONF objective is met.
O.COMMS_INT	FCS_CKM.1 FCS_COP.1 FCS_CKM.4	FCS_CKM.1 provides support for implementing communications that have both confidentiality and integrity security properties. FCS_COP.1 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.1 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.

Objective	SFRs	Demonstration
		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 FMT_MOF.1a FMT_MSA.1a FMT_MSA.1b FMT_MSA.1c FMT_MOF.1b FMT_MSA.2 FMT_MSA.3a FMT_MSA.3b FMT_MSA.3c FMT_SMF.1	FDP_IFC.1 provides the basis for implementing a policy within the TOE for controlling the flow of information, mailbox items, Exchange ActiveSync Mailbox Policy and Exchange Commands, between the TOE and the Enterprise Exchange Server. FDP_IFF.1 implements the policy that governs the flow of information between the TOE and the Enterprise Exchange Server, including TSF and user data. FTP_ITC.1 provides the capability to support a trusted and secure channel between the TOE and Enterprise Exchange Server 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

Objective	SFRs	Demonstration
		device access control functionality of the TOE. FMT_MSA.2 provides assurance that security attributes established for each of the security policies are loaded with appropriate default values, supporting the secure management 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.2, 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.
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 stored on the Mobile Device 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.SESSION_LOCK	FTA_SSL.1.EX FTA_SSL.2.EX	FTA_SSL.1.EX provides the ability to lock an 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.

Objective	SFRs	Demonstration
O.REMOTE_WIPE	FDP_IFC.1 FDP_IFF.1	FDP_IFC.1 ensures that the Mobile Device can accept a remote wipe command from the Enterprise Administrator through the Enterprise Exchange Server. FDP_IFF.1 implements the policy that governs the flow of information between the TOE and the Enterprise Exchange Server 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.

7.3.6 IT environment requirements correspondence

Table 19 – Mapping IT environment SFRs to objectives

Objective	SFRs	Demonstration
OE.I&A_ENTERPRISE	FIA_UAU.2 FIA_UID.2 FIA_ATD.1	FIA_UAU.2 ensures that the Enterprise Administrator is properly authenticated in the enterprise environment so that trust can be placed in the integrity of the management functions being performed via the Exchange Server. FIA_UID.2 ensures that the Enterprise Administrator is properly identified, prior to authentication, in the enterprise environment so that trust can be placed in the integrity of the management functions being performed via the Exchange Server. FIA_ATD.1 provides the necessary attributes required to support the identification and authentication of the Enterprise Administrator. FIA_UAU.2, FIA_UID.2 and FIA_ATD.1 combine to ensure that the OE.I&A_ENTERPRISE environment objective is met.
OE.COMMS_ENT	FCS_CKM.1 FCS_COP.1 FCS_CKM.4 FTP_ITC.1	FCS_CKM.1 provides cryptographic support through key generation that enables the implementation of cryptographic operations for secure communications between the TOE and components/systems within the enterprise environment. FCS_COP.1 provides the cryptographic operations to implement secure communications between the TOE and components/systems within the enterprise environment. FCS_CKM.4 provides a mechanism for securely disposing of cryptographic keys that have been generated by the various systems/components within the enterprise environment that communicate using cryptographic protection with the TOE. FTP_ITC.1 implements an inter-TSF trusted channel, this SFR within the IT environment provides the other end of the trusted channel for the enterprise environment. FCS_CKM.1, FCS_COP.1, FCS_CKM.4 and FTP_ITC.1 combine to ensure that the OE.COMMS_ENT environment objective is met.

Objective	SFRs	Demonstration
OE.COMMS_NET	FCS_CKM.1 FCS_COP.1 FCS_CKM.4 FTP_ITC.1	FCS_CKM.1 provides cryptographic support through key generation that enables the implementation of cryptographic operations for secure communications between the TOE and components/systems within the network environment. FCS_COP.1 provides the cryptographic operations to implement secure communications between the TOE and components/systems within the network environment. FCS_CKM.4 provides a mechanism for securely disposing of cryptographic keys that have been generated by the various systems/components within the network environment that communicate using cryptographic protection with the TOE. FTP_ITC.1 implements an inter-TSF trusted channel, this SFR within the IT environment provides the other end of the trusted channel for the network environment. FCS_CKM.1, FCS_COP.1, FCS_CKM.4 and FTP_ITC.1 combine to ensure that the OE.COMMS_NET environment objective is met.
OE.SEC_POLICY	FMT_MOF.1a FMT_MOF.1b FMT_SMF.1 FMT_SMR.1	FMT_MOF.1a ensures that the Enterprise Administrator is able to provide the necessary security management functions within the enterprise environment. FMT_MOF.1b ensures that the Mobile Operator is able to provide the necessary security management functions within the network environment. FMT_SMF.1 defines the set of security management functions that must be provided within the enterprise and network environments to support the security functionality of the TOE. FMT_SMR.1 ensures that the necessary security roles required within the enterprise and network environment to provide security management functionality for the TOE. FMT_MOF.1a, FMT_MOF.1b, FMT_SMF.1 and FMT_SMR.1 combine to ensure that the OE.SEC_POLICY is met.

7.3.7 TOE assurance requirements

118 This ST contains the assurance requirements from the CC EAL2 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.

119 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.

7.3.8 Demonstration of Mutual Support

120 The dependency analysis provided at Table 15 and the analyses provided in Table 17, Table 18, Table 19 and Table 20 demonstrate that the IT security functions work together to satisfy the stated security functionality of the TOE.

121 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 20 – Mapping TOE SFRs to TOE security functions

SFR	Device data protection	Device application control	Secure enterprise access	Device configuration control	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.1	**X**						The device data protection security function implements the FCS_COP.1 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.

SFR	Device data protection	Device application control	Secure enterprise access	Device configuration control	Device access control	Device security management	Demonstration
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.
FDP_ACC.1b				**X**			The device configuration 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 configuration control security function implements the FDP_ACF.1 requirement by implementing the set of subjects and objects specified by this policy for accepting and applying configuration data.
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.

SFR	Device data protection	Device application control	Secure enterprise access	Device configuration control	Device access control	Device security management	Demonstration
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.
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.
FMT_MOF.1a						**X**	The device security management security function implements the FMT_MOF.1a requirement by enabling the specified management functionality for the 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 configuration control	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.2						**X**	The device security management security function implements the FMT_MSA.2 requirement by ensuring that only secure values can be applied to security attributes.
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.

SFR	Device data protection	Device application control	Secure enterprise access	Device configuration control	Device access control	Device security management	Demonstration
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 21 – Assurance measures rationale

Assurance requirement	Assurance measures	Demonstration
ACM_CAP.2 Configuration items	Configuration management	The configuration management assurance measure provides a detailed description of the configuration management system used by Microsoft to control the development of the TOE. The documentation also provides a configuration list for the TOE.
ADO_DEL.1 Delivery procedures	Delivery and operation	The delivery and operation assurance measures provides a set of delivery procedures that provide effective guidance for ensuring that the TOE can be delivered to the end-user in a secure and controlled manner. This assurance measure also provides an installation guide that supports the initiation of the TOE so that it can be initially installed and configured in the evaluated configuration.
ADO_IGS.1 Installation, generation, and start-up procedures		
ADV_FSP.1 Informal functional specification	Development	The development assurance measure provides all the necessary design documentation to support the effective detailed analysis of the TOE for an evaluation at EAL2. The functional specification provides a detailed description of the external interfaces to the security functions of the TOE. The high-level design provides detailed description of the subsystems of the TOE that implement the security functions. The correspondence demonstration provides a method for mapping between the design representations provided for the TOE.
ADV_HLD.1 Descriptive high-level design		
ADV_RCR.1 Informal correspondence demonstration		
AGD_ADM.1 Administrator guidance	Guidance documents	The guidance documents assurance measure provides the guidance documentation for both users and administrators of the TOE. These documents provide all the necessary instructions and direction for ensuring that the TOE is used and administered in a secure manner.
AGD_USR.1 User guidance		

Assurance requirement	Assurance measures	Demonstration
ALC_FLR.1 Basic flaw remediation	Life cycle support	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.
ATE_COV.1 Evidence of coverage	Tests	The tests assurance measure ensures that the TOE has been appropriately tested for the claimed set of security functions. The test plan 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_FUN.1 Functional testing		
ATE_IND.2 Independent testing – sample		
AVA_SOF.1 Strength of TOE security function evaluation	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.
AVA_VLA.1 Developer vulnerability analysis		