CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science, Technology and Innovation

CyberArmor Security Target

Document Version:	0.0.6
Date Published:	4 February 2014

Cyber Technology Research Department
CyberSecurity Malaysia
Level 5, Sapura @ Mines,
No. 7 Jalan Tasik,
The Mines Resort City,
43300 Seri Kembangan,
Selangor, Malaysia

COPYRIGHT AND CONFIDENTIALITY STATEMENT

Registered office:
Level 5, Sapura @ Mines,
No. 7 Jalan Tasik,
The Mines Resort City,
43300 Seri Kembangan,
Selangor

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Document Revision History

Version	Date	Prepared By	Description
d1	13Sept 2012	CSM MySEF & CTR	Draft released for evaluation
d2	19 Oct 2012	CSM MySEF & CTR	Updated based on comments
0.0.1	26 Nov 2012	CSM MySEF & CTR	Change ST version
0.0.2	04 Dec 2012	CSM MySEF & CTR	Updated based on EOR_ASE 1.0
0.0.3	28 June 2013	CSM MySEF & CTR	Updated based on EOR
0.0.4	21 August 2013	CSM MySEF & CTR	Add A.ORG and OE.ORG
0.0.5	27 August 2013	CSM MySEF & CTR	Update Section 1.3
0.0.6	04 February 2014	CSM MySEF & CTR	Update Section 2.3

TABLE OF CONTENTS

1. SECURITY TARGET INTRODUCTION

1.1 Security Target Reference

Security Target Title:	CyberArmor Security Target
Security Target Version:	0.0.6
Published Date:	04 February 2014

Table 1: Security Target Reference

1.2 Target of Evaluation (TOE) Reference

TOE Name:	CyberArmor
TOE Initial in ST:	CyberArmor
TOE Version:	3.0.12
Application Notes:	All mobile phone wordings or statements are referring to BlackBerry® mobile phone, specifically bound to the scope of TOE.

Table 2: TOE Reference

1.3 Document Conventions

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

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**].
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***].
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~~.
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 FCS_CKM.1a and FCS_COP.1a.

Table 3: Statement of Operation for SFR's.

In accordance of providing additional explanations, the following conventions are used:

Application Notes	Informal explanation by the author of the ST to highlight and explain an unusual or otherwise exceptional wording either in the requirements for an artefact of the ST or in the statement of a specific artefact in the ST.

Table 4: Application Notes Convention.

1.4 Terminology and Acronyms

The following terminology and acronyms are used in the Security Target:

SMS	Short Message Service
SMSC	Short Message Service Centre
HTTPS	Hypertext Transfer Protocol Secure is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encrypted communication and secure identification of a network web server. Reference: http://en.wikipedia.org/wiki/HTTP_Secure
CyberArmor App	TOE application that is installed in BlackBerry. In this document, CyberArmor App will also be called CyberArmor Application
CyberArmor Management Server	TOE application that acts as key management server for CyberArmor application installation, key distribution, contacts management, users and organizations registrations. In this document, CyberArmor Management Server will also be called CyberArmor Server.
Ciphertext/ Encrypted SMS	SMS that is unreadable by user and represented as a string of Base64 characters.
Plaintext/ Decrypted SMS	Normal SMS that is readable by user.
Base64 Format	A group of similar encoding schemes that represent binary data in an ASCII string format. It contains the following alphanumeric characters and symbols: "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
User/Users	Terms "User" and "Users" are used in this document is referring to trusted individual by the organization that is allowed to operate BlackBerry® mobile phone and TOE. "User" is referring to one individual in aspects of Blackberry® mobile phone and TOE usage and operation. "Users" are referring to implementation and enforcement of organization security policies towards individuals that trusted by the

	organization.
Administrator	Terms “Administrator” or “Admin” used in this document is referring to trusted individual by the organization that is allowed to configure and manage CyberArmor Management Server.
Keystream	A stream of random characters produce by the CSM Stream Cipher algorithm that are XORed with a plaintext/ciphertext producing ciphertext/plaintext respectively
SMS Inbox	Native inbox on the BlackBerry® mobile phone

Table 5: Terminology and Acronyms.

1.5 References

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[4] Common Methodology for Information Technology Security Evaluation (CEM): Version 3.1 Revision 4, September 2012, CCMB-2012-09-004.

2. TARGET OF EVALUATION (TOE) OVERVIEW

2.1 Usage and major security features of TOE

CyberArmor is a data protection product commercialized by CyberSecurity Malaysia for securing plaintext messages between two parties communicating using short message service (SMS). TOE consists of two major components: CyberArmor App (also will be referred as CyberArmor Application) and CyberArmor Management Server (also will be referred as CyberArmor Server or Management Server in this document).

CyberArmor App is an application that is integrated with SMS Message List inside BlackBerry® application as a menu item that allows users to encrypt an SMS for an intended recipient / recipients. The recipient needs to have the same application installed in order to decrypt the encrypted SMS. This operation is password protected. The password is set earlier during configuration process.

Each encrypted SMS is sent as a string of Base64 characters; providing secure communication and secure data transaction environment from any breach of data confidentiality and integrity. The ciphertext SMS is accessible within BlackBerry® SMS application. Each ciphertext SMS received is protected by password. Each new ciphertext SMS has a different pattern (Base64 format) to protect its content from being read or guessed by unauthorized user.

CyberArmor Management Server consists of organization and user management function such as registration, de-activation and downloadable contact. It also consists of key management function where key can be generated, activated, revoked and distributed to users. TOE installer for BlackBerry® can be downloaded by user through a link in e-mail that is sent by the CyberArmor server.

The following are the summary of major security features of CyberArmor:

- Data Protection
- Identification, Authentication and Authorization
- Management Server

For more details, refer to Section Target of Evaluation (TOE) Description.

2.2 TOE Type

CyberArmor is a data protection application that provides cryptographic services for Short Message Service (SMS) in BlackBerry® mobile phones.

2.3 Requirements of Non-TOE Hardware, Software or Firmware

CyberArmor is a supporting application (add-on) for SMS Message List. It runs as a background service inside BlackBerry® mobile phone. There are several models of BlackBerry® mobile phones that support the TOE depending on the operating system (OS).

The following are the non-TOE hardware and software requirements:

#	Requirements:	Items:	Descriptions:
1.	Hardware	BlackBerry® Bold BlackBerry® Torch	Mobile phone devices.
2.		Management Server	Intel compatible 2.13 GHz processor 12MB L3 Cache At least 1Gig RAM At least 2Gig of free hard disk space
3.	Software	BlackBerry® Operating System (OS)	Version 6.0 to 7.0
4.		Management Server	Ubuntu Server 12.04.3 32-Bit Apache Web Server C++ compiler CSM Stream Cipher Ext JS Javascript Library Version 3.3.1 and Version 4.1.0 Java MySQL Database OpenSSL Perl SSH SSL Certificate

Table 6: List of Non-TOE Requirements.

3. TARGET OF EVALUATION (TOE) DESCRIPTION

3.1 Physical Scope of TOE

CyberArmor is a supporting application for SMS text messages in BlackBerry® mobile phones by providing users with Graphical User Interface (GUI) for sending encrypted SMS. Then, the recipient can decrypt the encrypted SMS received if the same application is installed in the BlackBerry® mobile phone. Objectives of this approach are to provide secure end-to-end communication and secure message transaction between two parties, ensuring confidentiality and integrity is not breached.

CyberArmor runs on BlackBerry® operating system (OS) version 6.0 to 7.0. CyberArmor requires Java Development Environment (JDE) as plug-in used in providing interface for users. BlackBerry® OS and JDE are not part of the scope of evaluation.

Installation of CyberArmor will be done using an over-the-air (OTA) method. CyberArmor Server administrator will send download links to the registered users via email. Users need to connect from the mobile phones to the CyberArmor Management Server using wireless connection (i.e. WiFi) or GSM data network (i.e. 3G, 4G) to download the application. Installation guidance of CyberArmor on BlackBerry® mobile phone is described in Preparative Guidance documentation.

CyberArmor Application will run automatically at start up after installation. The menus "Encrypt SMS" and "Decrypt SMS" will be available to user.

There are two roles defined in the operational scope of CyberArmor, which are users and administrators. A user is a trusted individual assigned by the organization to operate the CyberArmor Application. Administrator is trusted personnel who perform management and configuration of CyberArmor Management Server such as user management, the Management Server installation, key management and other related matters.

Figure 1 shows basic implementation and deployment of CyberArmor Application and Management Server.

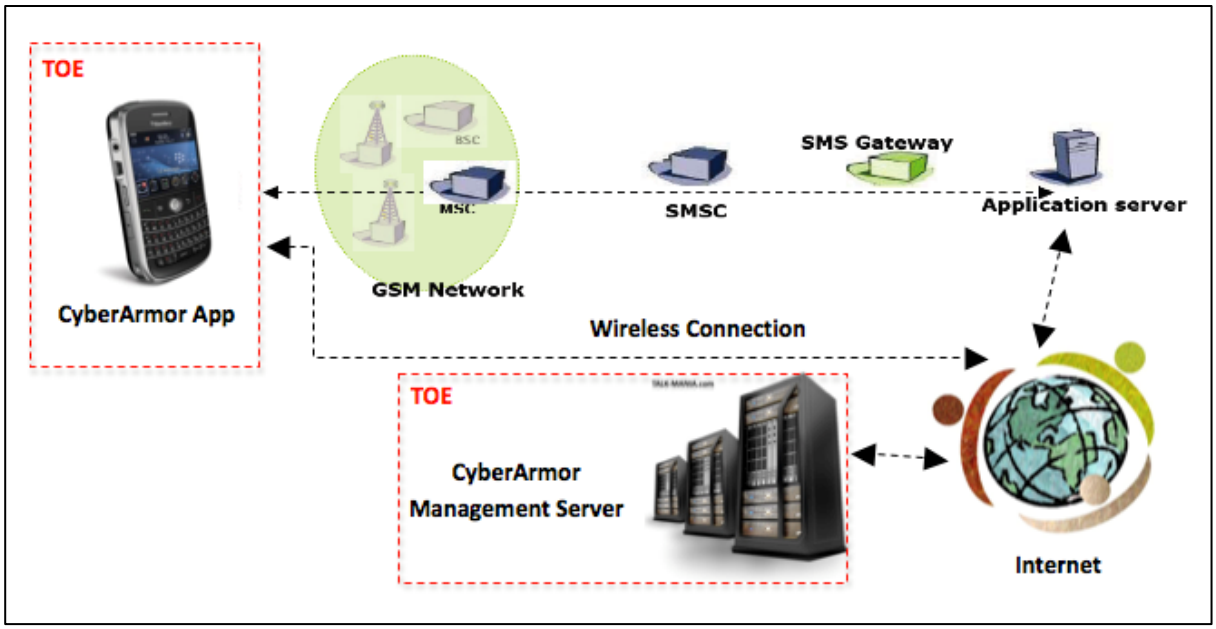

Figure 1: CyberArmor Implementation and Operation.

3.2 Logical Scope of TOE

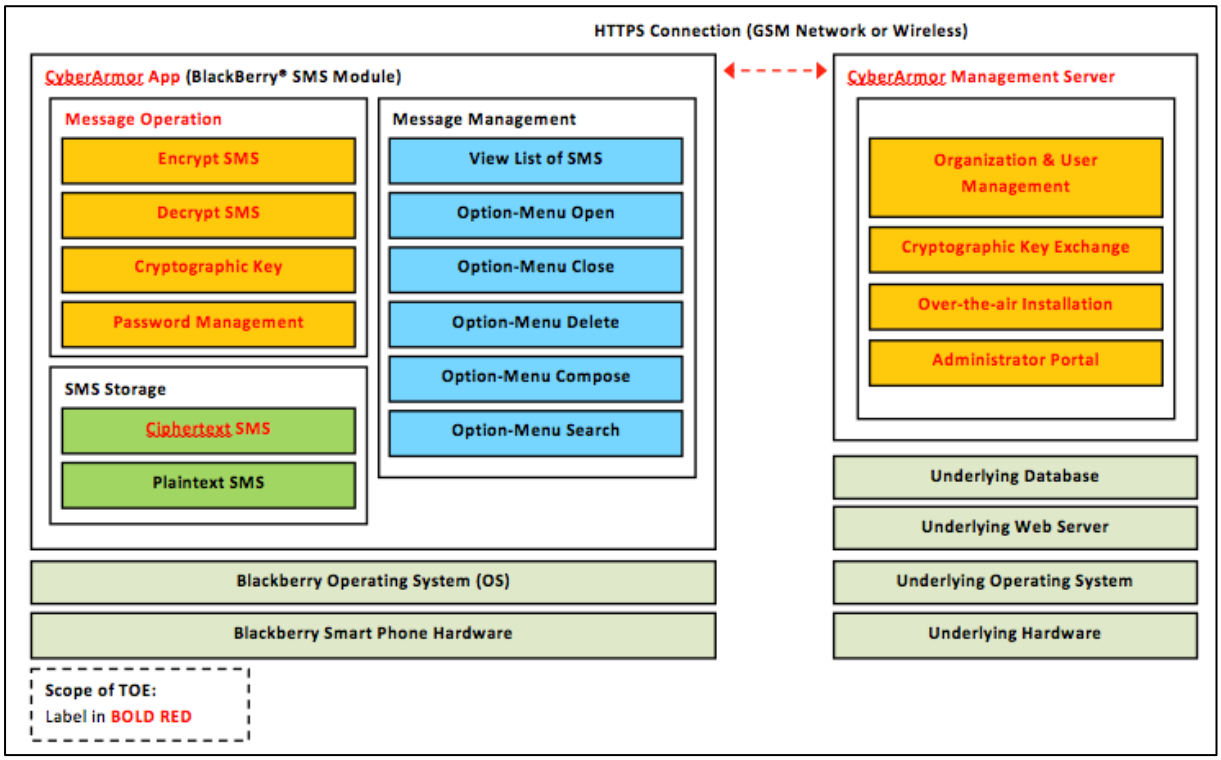

Figure 2: Scope of TOE

- Data Protection

CyberArmor is developed by CyberSecurity Malaysia using its own in-house developed symmetric algorithm which is called CSM Stream Cipher Algorithm. It is used in SMS encryption and decryption. Keystream which consist of random characters produced by CSM Stream Cipher algorithm are XORed with the plaintext/ciphertext SMS producing ciphertext/plaintext respectively. Cryptographic key as the input for keystream generation is generated by using AES algorithm, 256-bit. The strength of CSM Stream Cipher Algorithm and AES is not part of the scope.

User can access the main screen of CyberArmor Application from SMS Message List. There are two application menu items available in addition to native menus in SMS Message List called “Encrypt SMS” and “Decrypt SMS”.

Each ciphertext SMS sent by user is stored in the “Outbox” folder which is a SQLite database file stored in the phone’s SD Card. There is also database file for application configuration. Both outbox and configuration database are encrypted on the phone’s SD Card.

Ciphertext SMS received by the phone is stored in “SMS Inbox” folder. Any SMS in the “SMS Inbox” cannot be edited or deleted by CyberArmor Application. The ciphertext SMS received by user is in form of encrypted format until they are decrypted. Decryption process requires user (authorized user of BlackBerry® mobile phone) to enter a correct password set earlier during configuration. Failure to enter the correct password will result in the ciphertext SMS being inaccessible for decryption.

Cryptographic operations in aspects of encryption and decryption processes are performed using 128-bit key, which securely resides in encrypted SQLite database file.

The database encryption and decryption is executed by BlackBerry® OS. Database encryption and decryption is not part of the scope.

In the event of any IT incident of mobile phone lost or stolen, organization will advise users to retrieve a new key from the management server. The old key in the management server will be revoked. User will get a PIN number in an email message to update the new key to the new mobile phone. Unauthorized user or the thief would need to know the password for old key in the lost or stolen mobile phone to decrypt the ciphertext SMS. Additionally, the old key in the stolen or lost phone will be expired as per expiry period set during the key generation process.

A new key downloaded from the management server will overwrite any old key stored in the mobile phone.

- Identification, Authentication and Authorization

  a. **For CyberArmor Application:**

  Each encrypted SMS is displayed as a string of Base64 characters which represents encrypted binary data. It can be decrypted by accessing the option-menu "Decrypt SMS" by entering the correct password.

  Password protection is a feature in CyberArmor application for providing layer of protection from unauthorized access of unknown users to the encrypted message.

  CyberArmor application shall enforce users to use password alphanumeric and special characters combination with a length between 4 to 14 characters.

  b. **For CyberArmor Management Server:**

  CyberArmor management server required administrator to login to Management Server application by providing username and password. The password is a combination of alphanumeric and special characters with at least 6 characters.

- Management Server

Organization & User Management module provides organization and user registration and de-registration. The management server hosts a web-based application or portal for managing CyberArmor users. In this module, a function to allow users to download contacts to their device is available. All organization and user information will be stored in database. However, the database is not in the scope of evaluation.

Cryptographic Key Exchange module provides general cryptographic key management function. The functions are key generation, activation and deactivation (revocation). If there is any IT incident on mobile phone such as lost or stolen, user is required to inform the organization based on procedures of organizational security policies. Upon that IT incident, all users will be informed to retrieve new cryptographic key from the management server. Previous (old) key will be revoked and not allowed to be used for CyberArmor operation. HTTPS connection will be enforced through GSM data network or wireless connection during the key distribution communication between user and server.

Registered users will receive a 6-digit pin number via email in order to download current key that belongs to his organization. This pin will be prompted when user wants to update the key. The key update is catered by CyberArmor Management Server via HTTPS. The cryptographic key will be saved in the encrypted database stored in phone's

SD card. The database is encrypted using the same key used for application code signing provided by BlackBerry. The key provided by BlackBerry, database encryption and application code signing are not part of the scope.

Over-the-air installation module is also part of the Management Server function. Server Administrator shall configure the server to send download link to user through email. User can download the CyberArmor App installer using that link and install it directly to their mobile phone. Each link has randomized id assigned uniquely for each user. The link is valid for just one download.

Administrator portal is the web interface module that allows the administrator to access and manage the Management Server function remotely. The Management Server only opens ports 22 for SSH/SCP and 443 for HTTPS to the external network. Access to the administrator portal will only be allowed using HTTPS connection. Administrator can also manage the server using shell over SSH. Application files will be transferred to the Management Server using SCP connection. However, the HTTPS, SSH and SCP connections are not part of the scope of evaluation. Management Server identity is protected by digital certificate when communicate with user mobile phone. However, this function is not part of the scope.

4. CONFORMANCE CLAIM

The following conformance claims are made by Security Target:

CC Conformant	Conformant to Common Criteria version 3.1, revision 4.
CC Part 2 Conformant	Conformant to Common Criteria Part 2.
CC Part 3 Conformant	Conformant to Common Criteria Part 3.
Package Conformant	Package conformant to Common Criteria Evaluation Assurance Level 1 (EAL 1).
Protection Profile Conformant	Does not claim to any Protection Profile (PP).

Table 7: Conformance Claims.

5. ASSUMPTIONS

The following are the Assumptions for the TOE:

A.PASSWD	It is assumed that user will keep the password secret and does not write them down or disclose them to any other system or user.
A.APPS	It is assumed that all third party applications installed inside the mobile phone are trusted and shall not perform malicious actions to compromise the operation of TOE. Since the database files are encrypted using the public-private key pair of CyberArmor developer, other applications do not have digital right access to the files.
A.USER	It is assumed that authorized users of mobile phone are not malicious, attempts to interact with the CyberArmor App in compliance with the organization security policies, and exercises precautions to reduce risk of loss or theft towards the CyberArmor App.
A.ADMIN	It is assumed that TOE administrators are individuals who are trusted by organization of performing management of CyberArmor App and CyberArmor Server in compliance with the organization security policies.
A.SECURECOMM	It is assumed that the communication between Administrator host/User mobile phone and Management Server is secure and encrypted.
A.DATABASE	It is assumed that the server and mobile phone database are encrypted.
A.ORG	It is assumed that only one (1) single organization will be using

	TOE.

Table 8: Assumptions.

6. SECURITY OBJECTIVES

6.1 Security Objectives for the Operational Environment

The following are the Security Objectives for the Operational Environment:

OE.PASSWD	Users and administrators are advised to not disclose any information regarding the password to others. Users/Administrators shall create a strong password combination of mix of alphanumeric characters and symbols. The password created shall be a combination of alphanumeric and special characters which at least 6 characters.
OE.APPS	Users and administrators must follow organization security policies that prohibit installation of all un-trusted applications into the mobile phone, where TOE is being used and initialized.
OE.USER	User of mobile phone is trustworthy not malicious, has enough knowledge on mobile phone and CyberArmor App operations, attempts to interact with the CyberArmor App in compliance with the organization security policies, and exercises precautions to reduce risk of loss or theft towards the CyberArmor App.
OE.ADMIN	TOE administrators are individual that are trusted by organization of performing management of CyberArmor App and CyberArmor Server.
OE.SECURECOMM	The communication between TOE administrator host/User mobile phone and Management Server must be secure and encrypted.
OE.DATABASE	The database used in Management Server and mobile phone are encrypted.
OE.ORG	Only one (1) single organization shall be using TOE.

Table 9: Security Objectives for the Operational Environment.

7. IT SECURITY REQUIREMENTS

This section specifies requirements for the TOE, addition to the operations that have been applied on the selected functional requirement components.

7.1 TOE Security Assurance Requirements (SAR's)

The following are the SAR's for EAL1 comply by TOE:

ADV: Development	ADV_FSP.1Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security Objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE Summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Table 10: SAR's.

7.2 TOE Security Functional Requirements (SFR's)

The following are the SFR's that comply by TOE:

Requirement Class:	Requirement Components:
Class FCS: Cryptographic support	FCS_CKM.1 Cryptographic key generation
	FCS_CKM.2 Cryptographic key distribution
	FCS_CKM.4 Cryptographic key management
	FCS_COP.1 Cryptographic operation
Class FDP: User data protection	FDP_ACC.1 Subset access control
	FDP_ACF.1 Security attribute based access control
	FDP_ITT.1 Basic internal transfer protection
	FDP_RIP.2 Full residual information protection
Class FIA: Identification and authentication	FIA_SOS.1 Verification of secrets
	FIA_UAU.1 Timing of authentication
	FIA_UID.2 User identification before any action
Class FMT: Security Management	FMT_MTD.1a Management of TSF data (CyberArmor App)
	FMT_MTD.1b Management of TSF data (CyberArmor Management Server)
	FMT_REV.1 Revocation
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles

Table11: SFR's.

7.2.1 Class FCS: Cryptographic support

1.	**SFR's Class:**	Class FCS: Cryptographic support
	Class Family:	Cryptographic key management (FCS_CKM)
	SFR Component:	FCS_CKM.1 Cryptographic key generation
	Hierarchical to:	No other component.
	Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
	FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**assignment: AES**] and specified cryptographic key sizes [**assignment: 256-bits**] that meet the following: [**assignment: FIPS 197**].
	Application Notes:	Key generated by AES algorithm will be used as input to create keystream using CSM Stream Cipher algorithm.
2.	**SFR's Class:**	Class FCS: Cryptographic support
	Class Family:	Cryptographic key management (FCS_CKM)
	SFR Component:	FCS_CKM.2 Cryptographic key distribution
	Hierarchical to:	No other component.
	Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import user data with security attributes, or

		FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
	FCS_CKM.2.1	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [**assignment: using Diffie-Hellman**] that meets the following: [**assignment: RFC 2631**].
	Application Notes:	Diffie-Hellman is used for Cryptographic key exchange and distribution method. CyberArmor App will use Diffie-Hellman to create its public key, generated on the fly when user enters the PIN number. The IMEI number, PIN and public key will be sent to Management Server for verification before cryptographic key is delivered. Management server will verify the values submitted for verification and respond back with server's public key generated using Diffie-Hellman and cryptographic key. User is enforced to use secure communication via HTTPS when connecting to the management server upon requesting new cryptographic key.

3.	**SFR's Class:**	Class FCS: Cryptographic support
	Class Family:	Cryptographic key management (FCS_CKM)
	SFR Component:	FCS_CKM.4 Cryptographic key destruction
	Hierarchical to:	No other components.
	Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security, or FCS_CKM.1 Cryptographic key generation]
	FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**assignment: overwrite previous cryptographic key with new cryptographic key**] that meets the following: [**assignment: none**].
	Application Notes:	New cryptographic key generated in the Management Server will be downloaded to mobile phone. The new key will overwrite the old key in the mobile phone's database.

4.	**SFR's Class:**	Class FCS: Cryptographic support
	Class Family:	Cryptographic operation (FCS_COP)
	SFR Component:	FCS_COP.1 Cryptographic operation
	Hierarchical to:	No other components.
	Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
	FCS_COP.1.1	The TSF shall perform [**assignment: encrypt and decrypt**] in accordance with a specified cryptographic algorithm [**assignment: CSM Stream Cipher Algorithm (symmetric)**] and cryptographic key sizes [**assignment: 128-bits**] that meet the following: [**assignment: none**].
	Application Notes:	CSM Stream Cipher algorithm will use cryptographic key generated by AES algorithm to produce a keystream. Keystream is XORed with plaintext/ciphertext SMS to create the ciphertext/plaintext respectively.

Table12: FCS SFR's.

7.2.2 Class FDP: User data protection

5.	**SFR's Class:**	Class FDP: User data protection
	Class Family:	Access control policy (FDP_ACC)
	SFR Component:	FDP_ACC.1 Subset access control
	Hierarchical to:	No other component.
	Dependencies:	FDP_ACF.1 Security attribute based access control
	FDP_ACC.1.1	The TSF shall enforce the [**assignment: access control SFP**] on [**assignment: as listed in Table 13**].
	Application Notes:	

Subject:	**Object:**	**Operations:**
User	Plaintext SMS	Encrypt
User	Encrypted SMS	View encrypted SMS
User	Encrypted SMS	Decrypt
User	Cryptographic key and PIN	Use or Overwrite
User	Public key	Transmit
User	Contacts	Update
User	IMEI number	Transmit
User	Password	Create or Change

		Administrator	Organization	Add, modify and delete
		Administrator	User	Add, modify, delete, activate, deactivate
		Administrator	Cryptographic key	Generate, send, revoke
		Administrator	Installation file	Send
		Administrator	PIN number	Send

Table 13

6.	**SFR's Class:**	Class FDP: User data protection
	Class Family:	Access control functions(FDP_ACF)
	SFR Component:	FDP_ACF.1 Security attribute based access control
	Hierarchical to:	No other component.
	Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
	FDP_ACF.1.1	The TSF shall enforce the [**assignment: access control SFP**] to objects based on the following: [**assignment: as listed in Table 13**].
	FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**assignment:** **a) User can perform encryption of plaintext SMS in CyberArmor App** **b) User who enters correct password can decrypt and view the encrypted SMS in CyberArmor App** **c) User can use the cryptographic key and overwrite the cryptographic key by updating the PIN in CyberArmor App** **d) User can update the contacts in CyberArmor App** **e) IMEI number, PIN number and Diffie-Hellman public key will be transmitted to Management server for identification and verification purpose before cryptographic key is sent to CyberArmor App** **f) IMEI number of user's mobile phone will be transmitted to Management Server for verification before contacts can be downloaded to mobile phone**

		i) Administrator can generate, send and revoke cryptographic key in Management Server **j) Administrator can send the CyberArmor App installation file and PIN number to User through e-mail**].
	FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**assignment: none**].
	FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**assignment: none**].
	Application Notes:	None.

7.	**SFR's Class:**	Class FDP: User data protection
	Class Family:	Internal TOE transfer (FDP_ITT)
	SFR Component:	FDP_ITT.1 Basic internal transfer protection
	Hierarchical to:	No other component.
	Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control
	FDP_ITT.1.1	The TSF shall enforce the [**assignment: access control SFP**] to prevent the [***selection: disclosure, modification***] of user data when it is transmitted between physically-separated parts of the TOE.
	Application Notes:	When user invokes the Contacts update in CyberArmor App, HTTPS connection is established from CyberArmor App and Management Server. HTTPS connection is provided by the server and mobile phone which is not part of the TOE scope. When request is send from CyberArmor App, IMEI number for mobile phone is included as part of identification. Management Server will verify the validity of IMEI number before

		uploading the contact to CyberArmor App.

<table>
<tr><td rowspan="7">8.</td><td>SFR's Class:</td><td>Class FDP: User data protection</td></tr>
<tr><td>Class Family:</td><td>Residual information protection (FDP_RIP)</td></tr>
<tr><td>SFR Component:</td><td>FDP_RIP.2 Full residual information protection</td></tr>
<tr><td>Hierarchical to:</td><td>FDP_RIP.1 Subset residual information protection</td></tr>
<tr><td>Dependencies:</td><td>No dependencies.</td></tr>
<tr><td>FDP_RIP.2.1</td><td>The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: deallocation of the resource from] all objects.</td></tr>
<tr><td>Application Notes:</td><td>Declaration of SFR (FDP_RIP.2) are meant for items that stated in table 14, which will be deallocation from all objects and operation of TOE, inaccessible by users or TOE.
<table>
<tr><th>Items:</th><th>Usage:</th><th>Reason of deallocation:</th></tr>
<tr><td>User Password</td><td>Decrypt/view encrypted message</td><td>Old password will be deleted from encrypted database when new key is updated in the database.</td></tr>
<tr><td>Cryptographic key</td><td>Supports encryption and decryption processes.</td><td>Users will be supplied with new cryptographic key in their mobile phone by overwriting the old key in the database. The cryptographic key is encrypted in the encrypted database.</td></tr>
<tr><td>Contacts</td><td>Updating contacts.</td><td>Current contact list will be deleted from database and replaced with contacts</td></tr>
</table></td></tr>
</table>

				downloaded from Management Server.

Table 14

Table15: FDP SFR's.

7.2.3 Class FIA: Identification and authentication

9.	**SFR's Class:**	Class FIA: Identification and authentication
	Class Family:	Specification of secret (FIA_SOS)
	SFR Component:	FIA_SOS.1 Verification of secrets
	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
	FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [**assignment:** **a) mix of alphanumeric characters and symbols with length between 4 to 14 characters for CyberArmor mobile phone application** **b) mix of alphanumeric characters and symbols at least 6 characters for CyberArmor Management Server**].
	Application Notes:	None

10.	**SFR's Class:**	Class FIA: Identification and authentication
	Class Family:	User authentication (FIA_UAU)
	SFR Component:	FIA_UAU.1 Timing of authentication
	Hierarchical to:	No other components.
	Dependencies:	FIA_UID.1 Timing of identification
	FIA_UAU.1.1	The TSF shall allow [**assignment:** **a. view list of SMS and its content;** **b. view contact information of sender;** **c. create new ciphertext SMS and send to expected recipient** **d. updating contacts** **e. updating key**] on behalf of the user to be performed before the user is authenticated **refinement: at CyberArmor Application only.**
	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 **refinement: at CyberArmor Application and CyberArmor Management Server.**
	Application Notes:	User is allowed to access BlackBerry® message (SMS) module to view all content of SMS and ciphertext SMS. Viewing ciphertext SMS before any decryption process is allowed but user can only see ciphertext. The plaintext SMS can be viewed when user provide the correct password to decrypt the SMS. User is allowed to create new ciphertext SMS and send to expected recipient without the needs of entering password. Access to cryptographic key is not within TOE controlled. The environment protects the cryptographic key, which is the operating system of the mobile phone. Another layer of protection is the database encryption which is also enforced by the environment.

		CyberArmor Management Server required administrator to login to Management Server application by providing username and password before allowing any TSF-mediated actions on behalf of the administrator.

11.	**SFR's Class:**	Class FIA: Identification and authentication
	Class Family:	User identification (FIA_UID)
	SFR Component:	FIA_UID.2 User identification before any action
	Hierarchical to:	FIA_UID.1 Timing of identification
	Dependencies:	No dependencies.
	FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
	Application Notes:	CyberArmor Management Server required administrator to login to Management Server application by providing username and password before allowing any TSF-mediated actions on behalf of the administrator. This SFR is not applicable to CyberArmor App.

Table 16: FIA SFR's.

7.2.4 Class FMT: Security Management

12.	**SFR's Class:**	Class FMT: Security management
	Class Family:	Management of TSF data (FMT_MTD)
	SFR Component:	FMT_MTD.1a Management of TSF data (CyberArmor App)
	Hierarchical to:	No other components.
	Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
	FMT_MTD.1a.1	The TSF shall restrict the ability to [***selection: modify, [assignment: view, update]***] the [**assignment: list of plaintext or ciphertext SMS, password, contacts and PIN**] to [**assignment: user**].
	Application Notes:	User can view the plaintext or ciphertext SMS using CyberArmor App. Before encrypting or decrypting the SMS, user must set a password and enter a valid PIN number to perform cryptographic operations. User can use the Contact Updater to update contacts of CyberArmor users for sending and receiving encrypted SMS.

13.	**SFR's Class:**	Class FMT: Security management
	Class Family:	Management of TSF data (FMT_MTD)
	SFR Component:	FMT_MTD.1b Management of TSF data (CyberArmor Management Server)
	Hierarchical to:	No other components.
	Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
	FMT_MTD.1b.1	The TSF shall restrict the ability to [***selection: modify, delete, [assignment: add, generate, activate, deactivate, revoke, send]***] the [**assignment: organization account, user account, cryptographic key, TOE installer, PIN**] to [**assignment: administrator**].
	Application Notes:	Administrator is able to add, modify and delete Organization/User account in CyberArmor Management Server. User account can be activated or deactivated from using TOE. Cryptographic key management such as generation, activation and revocation is manageable by administrator. Key is activated once being generated. Using Download Links option, administrator will send email containing CyberArmor App installer for user installation in mobile phone. After key is generated, administrator will use Send Key option to email that contains PIN number for cryptographic key activation in mobile phone.

14.	**SFR's Class:**	Class FMT: Security management
	Class Family:	Revocation (FMT_REV)
	SFR Component:	FMT_REV.1 Revocation
	Hierarchical to:	No other components.
	Dependencies:	FMT_SMR.1 Security roles
	FMT_REV.1.1	The TSF shall restrict the ability to revoke [**assignment: cryptographic key**] associated with the [***selection: users, [assignment: TOE]***] under the control of the TSF to [**assignment: administrator**].
	FMT_REV.1.2	The TSF shall enforce the rules [**assignment:** **a) Manual revocation by disabling the cryptographic key** **b) Cryptographic key is expired on its End Date**]
	Application Notes:	In accordance of IT emergency or IT incident such as lost or stolen of mobile phone, administrator of Management Server will revoke old cryptographic key and distribute new generated cryptographic key. The revocation is executed by manually disabling the key. Cryptographic key will also automatically be revoked or expired when it has reached its expiry date or End Date configured by administrator.

15.	**SFR's Class:**	Class FMT: Security management
	Class Family:	Specification of management functions (FMT_SMF)
	SFR Component:	FMT_SMF.1 Specification of management functions
	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
	FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**assignment:** **a. View list of SMS either plaintext or ciphertext;** **b. Modify password;** **c. Update Contacts to mobile phone;** **d. Retrieve new cryptographic key by updating PIN;** **e. Add, modify and delete organization account** **f. Add, modify, delete, activation and deactivation of user account; Cryptographic Key generation, activation and deactivation (revocation);Send email containing installer downloadable link and PIN**].
	Application Notes:	None.

16.	**SFR's Class:**	Class FMT: Security management
	Class Family:	Security management roles (FMT_SMR)
	SFR Component:	FMT_SMR.1 Security roles
	Hierarchical to:	No other components.
	Dependencies:	FIA_UID.1 Timing of identification
	FMT_SMR.1.1	The TSF shall maintain the roles [**assignment: administrator, user**].
	FMT_SMR.1.2	The TSF shall be able to associate users with roles.
	Application Notes:	None.

Table 17: FMT SFR's.

7.3 TOE Security Assurance Requirements (SAR's) Rationale

The set of SARs selected for the TOE constitute the entire evaluation assurance level EAL1 with no augmentations. As a basic EAL1 package, the set of SARs is an internally consistent and mutually supportive set of SARs.

On occasion of TOE operation, any process of retrieving original SMS messages shall be done only by providing correct password and accessing the menu of "Decrypt SMS".

Concluded, it is sufficient for the TOE to be engineered and demonstrated sufficient assurance against logical attacks by malicious software through externally visible interfaces as demonstrated by EAL1.

8. TOE SUMMARY SPECIFICATION (TSS)

8.1 Data Protection

CyberArmor is developed by CyberSecurity Malaysia using its own in-house developed symmetric algorithm which is called CSM Stream Cipher Algorithm. It is used in SMS encryption and decryption. Keystream which consist of random characters produced by CSM Stream Cipher algorithm are XORed with the plaintext/ciphertext SMS producing ciphertext/plaintext respectively. Cryptographic key as the input for keystream generation is generated by using AES algorithm, 256-bit. The strength of CSM Stream Cipher Algorithm and AES is not part of the scope.

Diffie-Hellman is used for Cryptographic key exchange and distribution method. CyberArmor App will use Diffie-Hellman to create its public key, generated on the fly when user enters the PIN number. The IMEI number, PIN and public key will be sent to Management Server for verification before cryptographic key is delivered. Management server will verify the values submitted for verification and respond back with server's public key generated using Diffie-Hellman and cryptographic key. User is enforced to use secure communication via HTTPS when connecting to the management server upon requesting new cryptographic key. HTTPS connection is not part of the TOE scope.

A new cryptographic key will overwrite any old key stored in the mobile phone's database. Old password will be deleted from encrypted database when new key is updated in the database. Database used to store the cryptographic key and password is encrypted. However, the database encryption is not part of the scope.

User can access the main screen of CyberArmor Application from SMS Message List. There are two application menu items available in addition to native menus in SMS Message List called "Encrypt SMS" and "Decrypt SMS".

Each ciphertext SMS sent by user is stored in the "Outbox" folder which is a SQLite database file stored in the phone's SD Card. There is also database file for application configuration. Both outbox and configuration database are encrypted on the phone's SD Card.

Ciphertext SMS received by the phone is stored in "SMS Inbox" folder. The ciphertext SMS received by user is in form of encrypted format until they are decrypted. Decryption process requires user (authorized user of BlackBerry® mobile phone) to enter a correct password set earlier during configuration. Failure to enter the correct password will result in the ciphertext SMS being inaccessible for decryption. Password can be modified or changed by user.

Cryptographic operations in aspects of encryption and decryption processes are performed using 128-bit key, which securely resides in encrypted SQLite database file. The database encryption and decryption is executed by BlackBerry® OS. Database encryption and decryption is not part of the scope.

Ciphertext SMS can only be sent if Contacts is updated. User must update the list of contact using Contact Updater in CyberArmor App. IMEI number for mobile phone will be transmitted to Management Server for user verification before being allowed to update the contacts. Current contact list will be deleted from database and replaced with contacts downloaded from Management Server.

In the event of any IT incident of mobile phone lost or stolen, organization will advise users to retrieve a new key from the management server. The old key in the management server will be revoked. User will get a cryptographic key PIN number in an

email message to update the new key to the new mobile phone. Unauthorized user or the thief would need to know the password for old key in the lost or stolen mobile phone to decrypt the ciphertext SMS. Additionally, the old key in the stolen or lost phone will be expired as per expiry period set during the key generation process.

The following are the SFR's mapped to this logical scope:

Data Protection	FCS_CKM.1 Cryptographic key generation
	FCS_CKM.2 Cryptographic key distribution
	FCS_CKM.4 Cryptographic key destruction
	FCS_COP.1 Cryptographic operation
	FDP_ACC.1 Subset access control
	FDP_ACF.1 Security attribute based access control
	FDP_ITT.1 Basic internal transfer protection
	FDP_RIP.2 Full residual information protection
	FMT_MTD.1a Management of TSF data (CyberArmor App)
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles

Table 18: List of SFR's mapped to Data Protection.

8.2 Identification, Authentication and Authorization

a. For CyberArmor mobile phone application:

Each encrypted SMS is displayed as a string of Base64 characters which represents encrypted binary data. It can be decrypted by accessing the option-menu "Decrypt SMS" by entering the correct password.

Password protection is a feature in CyberArmor application for providing layer of protection from unauthorized access of unknown users to the encrypted message.

CyberArmor application is configurable by users to use password combination with a length between 4 to 14 of mix alphanumeric characters and symbols.

Before user presents the password to be authenticated to encrypt or decrypt SMS, use is allowed to do several actions at CyberArmor App:

a. view list of SMS and its content;
b. view contact information of sender;
c. create new ciphertext SMS and send to expected recipient
d. updating contacts
e. updating key

b. For CyberArmor Management Server:

CyberArmor management server required administrator to login to Management Server application by providing username and password. The password is a combination of alphanumeric and symbols of at least 6 characters.

Administrator is not able to perform any actions before being identified and authenticated by Management Server.

The following are the SFR's mapped to this logical scope:

	FIA_SOS.1 Verifications of secrets
	FIA_UAU.1 Timing of authentication
	FIA_UID.2 User identification before any action
	FMT_SMR.1 Security roles

Table 19: List of SFR's mapped to Password Enforcement.

8.3 Management Server

Organization & User Management module provides organization and user registration and de-registration. Administrator is able to add, modify and delete organizations and users. Administrator also is able to activate or deactivate users. The management server hosts a web-based application or portal for managing CyberArmor users. In this module, a function to allow users to download contacts to their device is available. All organization and user information will be stored in database. However, the database is not in the scope of evaluation.

Cryptographic Key Exchange module provides general cryptographic key management function. The functions are key generation, send and deactivation (revocation). If there is any IT incident on mobile phone such as lost or stolen, user is required to inform the organization based on procedures of organizational security policies. Upon that IT incident, all users will be informed to retrieve new cryptographic key from the management server. Previous (old) key will be revoked and not allowed to be used for CyberArmor operation. The revocation is executed by manually disabling the key.

Cryptographic key will also automatically be revoked or expired when it has reached its expiry date or End Date configured by administrator.

Using Download Links option, administrator will send email containing CyberArmor App installer for user installation in mobile phone. After key is generated, administrator will use Send Key option to email that contains PIN number for cryptographic key activation in mobile phone. Registered users will receive a 6-digit pin number via email in order to download current key that belongs to his organization. This pin will be prompted when user wants to update the key. The key update is catered by CyberArmor management server via HTTPS. The cryptographic key will be saved in the encrypted database stored in phone's SD card. The database is encrypted using the same key used for application code signing provided by BlackBerry. The key provided by BlackBerry, database encryption and application code signing are not part of the scope.

Over-the-air installation module is also part of the Management Server function. Server Administrator shall configure the server to send download link to user through email.

User can download the CyberArmor App installer using that link and install it directly to their mobile phone. Each link has randomized id assigned uniquely for each user. The link is valid for just one download. The randomized id is not part of the scope.

Administrator portal is the web interface module that allows the administrator to access and manage the Management Server function remotely. The Management Server only opens ports 22 for SSH/SCP and 443 for HTTPS to the external network. Access to the administrator portal will only be allowed using HTTPS connection. Administrator can also manage the server using shell over SSH. Application files will be transferred to the Management Server using SCP connection. However, the HTTPS, SSH and SCP connections are not part of the scope of evaluation. Management Server identity is protected by digital certificate when communicate with user mobile phone. However, this function is not part of the scope.

The following are the SFR's mapped to this logical scope:

Management Server	FCS_CKM.1 Cryptographic key generation
	FCS_CKM.2 Cryptographic key distribution
	FCS_CKM.4 Cryptographic key destruction
	FDP_ITT.1 Basic internal transfer protection
	FDP_ACC.1 Subset access control
	FDP_ACF.1 Security attribute based access control
	FMT_MTD.1b Management of TSF data (CyberArmor Management Server)
	FMT_SMF.1 Specification of management functions
	FMT_REV.1 Revocation
	FMT_SMR.1 Security roles

Table 19: List of SFR's mapped to Key Distribution and Management.

-- [End of Document] --