Australian Government
Department of Defence

Australasian Information Security Evaluation Program

CyberSecurity Malaysia
CyberArmor 3.0.12

Certification Report
2014/88

22 Dec 2014
Version 1.0

Commonwealth of Australia 2014

Reproduction is authorised provided
the report is copied in its entirety.

Amendment Record

Version	Date	Description
1.0	22 Dec 2014	Public

Executive Summary

This report describes the findings of the IT security evaluation of CyberSecurity Malaysia CyberArmor data protection product.

The Target of Evaluation (TOE) is CyberArmor, developed by CyberSecurity Malaysia, which provides users with the ability to securely send and receive encrypted SMS. The TOE is comprised of two components – the Management Server provides a platform for organisational/user management and cryptographic key control and the Application distribution component that is distributed to users and installed on their BlackBerry handset.

This report describes the findings of the IT security evaluation of CyberSecurity Malaysia CyberArmor to the Common Criteria (CC) to evaluation assurance level EAL1. The report concludes that the product has met the target assurance level of EAL1 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by BAE Systems Applied Intelligence and was completed on 14 April 2014.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target at Ref (10) and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 – Introduction

1.1 Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

The purpose of this Certification Report is to:

a) Report the certification of results of the IT security evaluation of the CyberSecurity Malaysia CyberArmor 3.0.12 against the requirements of the Common Criteria (CC) assurance level of EAL1 and

b) Provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target (Ref 10) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

The TOE is CyberArmor version 3.0.12 developed by CyberSecurity Malaysia.

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program.
TOE	CyberSecurity Malaysia CyberArmor
Software Version	3.0.12
Security Target	CyberArmor Security Target version 0.0.6, dated 04 Feb 2014
Evaluation Technical Report	Evaluation Technical Report CyberSecurity CyberArmor 14 April 2014, Version 1.0, Document reference EFS-T032-ETR
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 and Part 3 conformant September 2012, Version 4

Methodology	Common Methodology for Information Technology Security
Evaluation level	EAL 1
Sponsor	CyberSecurity Malaysia Level 5, Sapura @ Mines, No. 7 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor, Malaysia
Developer	CyberSecurity Malaysia Level 5, Sapura @ Mines, No. 7 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor, Malaysia
Evaluation Facility	BAE Systems Applied Intelligence Level 1 / 14 Childers St Canberra ACT 2600 Australia

Chapter 2 – Target of Evaluation

2.1 Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, its architectural components, the scope of evaluation, security policies, and its secure usage.

2.2 Description of the TOE

The Target of Evaluation (TOE) is CyberArmor version 3.0.12 developed by CyberSecurity Malaysia. The TOE provides users with the ability to securely send and receive encrypted SMS. The TOE is comprised of two components – the Management Server provides a platform for organisational/user management and cryptographic key control and the Application distribution component that is distributed to users and installed on their BlackBerry handset.

The CyberArmor application component is distributed to users and installed on their BlackBerry handset. Once the application has been configured and the cryptographic key and contact list downloaded from the Management Server, users are able to send encrypted text messages to any user within their organisation.

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 CyberArmor User Installation and Operational Guide (Ref 13).

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 organisation 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.

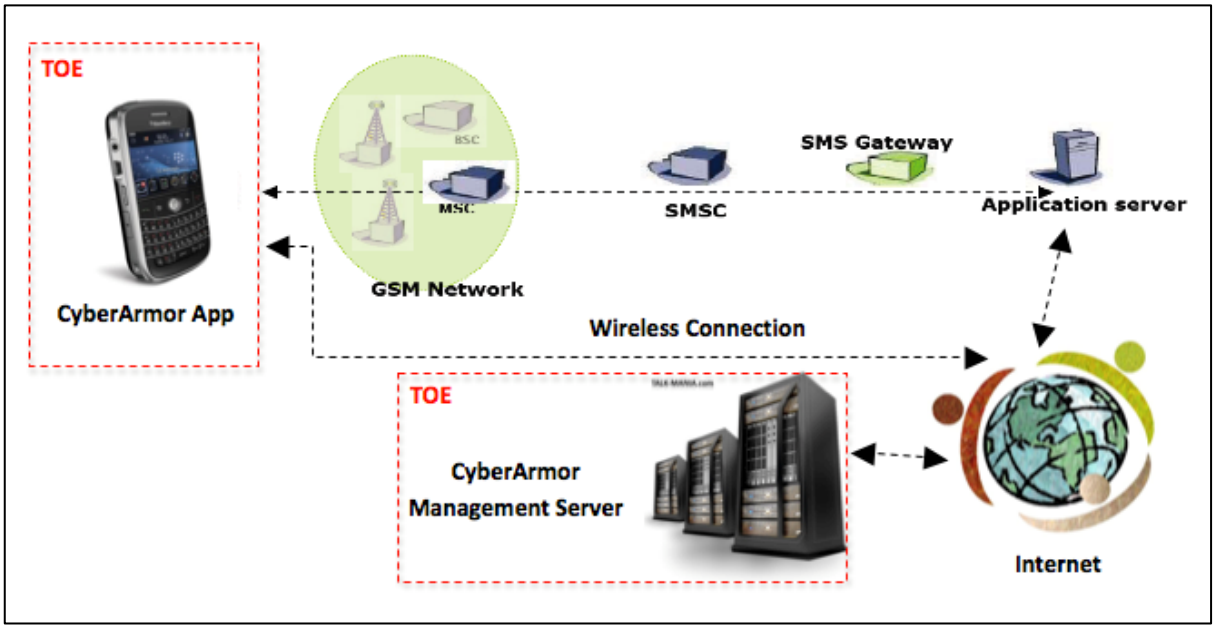

Figure 1: CyberArmor Implementation and Operation.

2.3 TOE Functionality

The functionality defined in the Security Target that was subsequently evaluated is as follows:

- **Data Protection -** CyberArmor makes use of a proprietary cryptographic algorithm (CSM Stream Cipher Algorithm) to encrypt and decrypt SMS. The algorithm makes use of 256-bit AES keys. The algorithm and associated keys are excluded from the scope of evaluation. When not being encrypted/decrypted, messages are stored and protected by the underlying BlackBerry SMS system. If a phone is lost, a user may contact the Management Server operators – they will revoke the previous cryptographic key and a new key will be issued for the replacement phone. This prevents any prior messages from being decrypted.
- **Identification, Authentication and Authorisation –** The CyberArmor application will only allow a user to decrypt and read an SMS if the correct password (specified during the TOE installation, must be between 4 to 14 alphanumeric & special characters) is input. If the correct password is not entered, the message remains unencrypted and can only be viewed as a string of Base64 characters.
  The Management Server protects against unauthorised access by requiring all users to authenticate with the platform using their username and password.
- **Management Server –** The Management Server platform provides a number of modules for administrators to configure and manage their TOE installation. All Management Server functionality is accessed via a web portal.

2.4 TOE Architecture

The TOE consists of the following major architectural components:

CyberArmor Application:

- Message Operations: Encrypt/Decrypt SMS
- Crypto key
- Password management
- Ciphertext SMS

CyberArmor Management Server:

- User and organisation Management
- Cryptographic key exchange
- Over-To-Air installation
- Administrator portal

2.5 Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the Security Target (Ref 9) and includes the following:

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

2.5.1 Evaluated Functionality

The TOE provides the following evaluated security functionality:

- 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.

A 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, organisation 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 Authorisation

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” and 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

Organisation & User Management module provides organisation 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 organisation and user information will be stored in database. 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, the user is required to inform the organisation based on procedures of organisational 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 organisation. 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. The server Administrator shall configure the server to send a 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. The Administrator can also manage the server using shell over SSH. Application files will be transferred to the Management Server using SCP connection. 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. This function is not part of the scope.

2.5.2 Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information Security Manual (ISM) (Ref 6) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

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 and are considered outside of the scope of the TOE:

#	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

2.6 Security

2.6.1 Security Policy

The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The Security Target (Ref 10) contains no explicit security policy statements.

2.6.2 Security Target

The Security Target (Ref 10) introduction contains an overview which describes the usage and major security features of the TOE.

This report describes the findings of the IT security evaluation of CyberSecurity Malaysia CyberArmor version 3.0.12 against:

- The Common Criteria (CC) Part 2 Security Functional Components Extended Package, Version 3.1 Revision 4 (Ref 2)
- The Common Criteria (CC) Part 3 Security Assurance Components Extended Package, Version 3.1 Revision 4 (Ref 3)

2.7 Usage

2.7.1 Evaluated Configuration

The evaluated configuration is based on default installation of the TOE and on the instructions provided in the CyberArmor Management Server Installation Guide (Ref 12) and User Installation and Operational Guide (Ref 13).

Australian Government users should refer to the ISM (Ref 6) to ensure that the configuration meets the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

2.7.2 Determining the Evaluated Configuration

The developer-provided CyberArmor Acceptance Checklist (Ref 11) defines the procedures to be followed when receiving the TOE. Recipients should ensure that the product version is as expected and the installer and container have not been tampered with.

Recipients should also ensure that the following items have been delivered alongside the TOE:

- CyberArmor Management Server Installation Guide (Ref 12)
- CyberArmor User Installation & Operational Guide (Ref 13)
- CyberArmor Management Server Operational Guide (Ref 14)

The Acceptance Checklist also provides a suite of tests to be performed upon acceptance and installation of the TOE. These tests are performed on both the Management Server and Application components of the TOE to ensure that all functions perform as expected.

2.7.3 Installation of the TOE

The TOE is installed in two steps. First, the Management Server platform is installed per the Management Server Installation Guide (Ref 12). Once the Management Server has been installed, an organisation, at least one user and a cryptographic key must be created.
Once the above have been completed, the User Installation and Operational Guide (Ref 13) provide the steps (and accompanying images) to download and install the TOE to a compatible BlackBerry handset.

2.7.4 Testing Activity

The evaluators examined the TOE prior to testing and determined that the test configuration was consistent with the configuration under evaluation as specified in the ST. The evaluators followed the user installation and configuration guidance to ensure that the TOE had been installed correctly and was in a known state prior to conducting testing.

The evaluators performed all applicable tests developed for independent testing of security functionality. The evaluators found that the results obtained were consistent with the expected test results.

The evaluators performed a search of publicly available information for known or potential vulnerabilities in the TOE and supporting components.

The evaluators performed penetration testing based on their vulnerability analysis. Based on the results of this testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

2.7.5 Testing Coverage

All tests performed by the evaluators were devised based on the TOE and received documentation. These tests are designed in such a way to provide a full coverage of testing for all security functions claimed by the TOE. All SFRs listed in both the Security Target were exercised during testing.

2.8 Delivery Procedures

Installation of CyberArmor application 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.

The developer-provided CyberArmor Acceptance Checklist (Ref 11) defines the procedures to be followed when receiving the TOE. Recipients should ensure that the product version is as expected and the installer and container have not been tampered with.

The Acceptance Checklist also provides a suite of tests to be performed upon acceptance and installation of the TOE. These tests are performed on both the Management Server and Application components of the TOE to ensure that all functions perform as expected.

2.9 Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased:

- CyberArmor Management Server Installation Guide (Ref 12)
- CyberArmor User Installation & Operational Guide (Ref 13)
- CyberArmor Management Server Operational Guide (Ref 14)

All common criteria guidance material is available at **www.commoncriteriaportal.org**. The Information Security Manual (ISM) is available at **www.asd.gov.au**.

2.10 Secure Usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

No assumptions were noted in the testing documentation or the resultant reports.

Chapter 3 – Evaluation

3.1 Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

3.2 Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4 (Refs 1, 2 and 3).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 3 (CEM) (Ref 4).

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs 7, 8 and 9). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref 5) were also upheld.

The evaluated configuration is based on default installation of the TOE, based on the instructions provided in the CyberArmor Management Server Installation Guide (Ref 12) and User Installation and Operational Guide (Ref 13).

3.3 Functional Testing

To gain confidence that the developers testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

3.4 Penetration Testing

The developer performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapsed time)

b) Specialist technical expertise required (specialist expertise)

c) Knowledge of the TOE design and operation (knowledge of the TOE)
Window of opportunity

d) IT hardware/software or other equipment required for the exploitation.

Chapter 4 – Certification

4.1 Overview

This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen, and recommendations made by the certifiers.

4.2 Assurance

EAL1 provides a basic level of assurance by a limited security target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behaviour.

The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TSF.

EAL 1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

The EAL provides a meaningful increase in assurance over unevaluated IT.

4.3 Certification Result

After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref 15) the Australasian Certification Authority **certifies** the evaluation of the CyberSecurity Malaysia CyberArmor version 3.0.12 data protection product performed by the Australasian Information Security Evaluation Facility, BAE Systems Applied Intelligence.

BAE Systems Applied Intelligence **has determined** that CyberSecurity Malaysia CyberArmor uphold the claims made in the Security Target (Ref 10) and **has met** the security assurance level of EAL 1.

Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref 6) and New Zealand Government users should consult the GCSB.

In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed, the ACA also recommends that users and administrators:

a) Ensure that the TOE is operated in the evaluated configuration

b) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved.

Annex A – References and Abbreviations

A.1 References

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, September 2012, Version 3.1, Revision 4
2. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2012, Version 3.1 Revision 4
3. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2012, Version 3.1 Revision 4
4. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2012, Version 3.1, Revision 4
5. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000
6. 2014 Australian Government Information Security Manual (ISM), Australian Signals Directorate
7. AISEP Policy Manual, APM, Version 4.0, August 2011, Defence Signals Directorate
8. AISEP Certifier Policy, ACP. Version 4.0, August 2011, Defence Signals Directorate
9. AISEP Evaluator Policy, AEP. Version 4.0, August 2011, Defence Signals Directorate.
10. CyberArmor Security Target, Version 0.0.6, 04-Feb-14
11. CyberArmor Acceptance Checklist, Version 1.0.6, 02-July-13
12. CyberArmor Management Server Installation Guide, Version 1.0.7, 10-Sep-13
13. CyberArmor User Installation and Operational Guide, Version 1.0.10, 10-Sep-13
14. CyberArmor Management Server Operational Guide, Version 0.1.8, 10-Sep-13
15. CyberArmor Evaluation Technical Report Version 1.0, 14 April 2014

A.2 Abbreviations

ACA	Australasian Certification Authority
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program

ASD	Australian Signals Directorate
CC	Common Criteria
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
HTTPS	Hypertext Transfer Protocol Secure
ISM	Information Security Manual
SFP	Security Function Policy
SFR	Security Functional Requirements
SAR	Security Assurance Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy