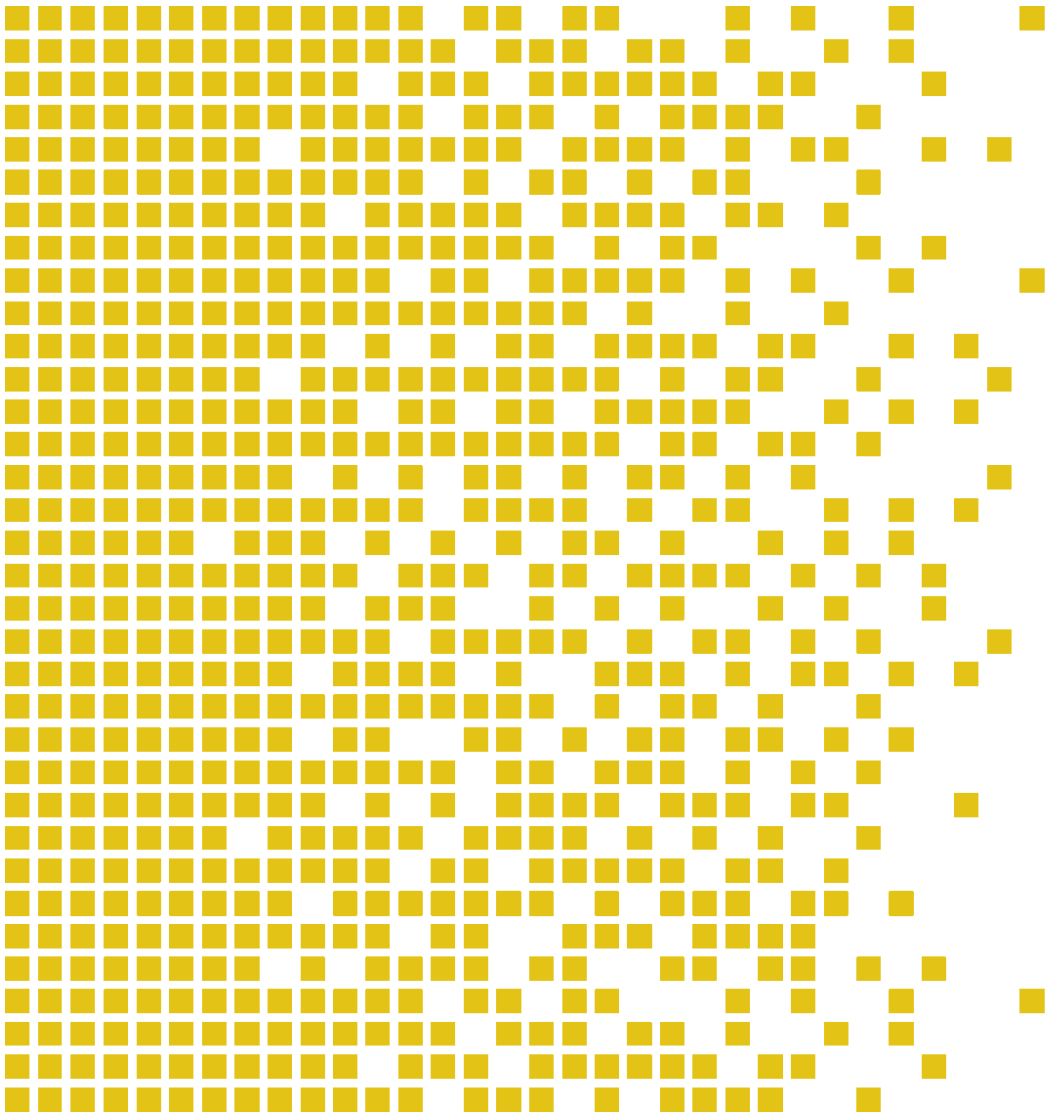
SERTIT-039 CR Certification Report

Issue 1.0 12 August 2013

Good For Enterprise System



SERTIT, P.O. Box 14, N-1306 Bærum postterminal, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Contents

1	**Certification Statement**	**4**
2	**Abbreviations**	**5**
3	**References**	**6**
4	**Executive Summary**	**7**
4.1	Introduction	7
4.2	Evaluated Product	7
4.3	TOE scope	7
4.4	Protection Profile Conformance	8
4.5	Assurance Level	8
4.6	Security Policy	8
4.7	Security Claims	8
4.8	Threats Countered	8
4.9	Threats and Attacks not Countered	8
4.10	Environmental Assumptions and Dependencies	9
4.11	IT Security Objectives	9
4.12	Non-IT Security Objectives	9
4.13	Security Functional Requirements	10
4.14	Evaluation Conduct	10
4.15	General Points	11
5	**Evaluation Findings**	**12**
5.1	Introduction	12
5.2	Delivery	12
5.3	Installation and Guidance Documentation	12
5.4	Misuse	12
5.5	Vulnerability Analysis	12
5.6	Developer's Tests	13
5.7	Evaluators' Tests	13
6	**Evaluation Outcome**	**14**
6.1	Certification Result	14
6.2	Recommendations	14
Annex A: Evaluated Configuration		**15**
TOE Identification		15
TOE Documentation		15
TOE Configuration		16

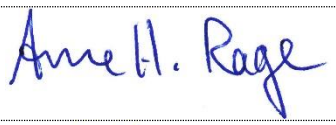
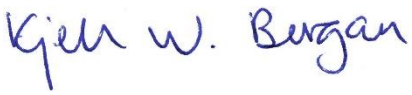
1 Certification Statement

Good Technology's Good For Enterprise System is a comprehensive platform providing secure end-to-end, wireless, real-time messaging, collaboration, and Intranet access.

Good For Enterprise System has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 4 augmented with ALC_FLR.1 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended functionality (see ST [1] chapter 5) functionality when running on the platforms specified in Annex A.

Product version numbers included in this evaluation:

- Good For Enterprise iOS client: 2.1.5
- Good For Enterprise Android client: 2.1.2
- Good Mobile Control Server 64bit-Domino: 2.3.1
- Good Mobile Control Server 64bit-Exchange: 2.3.0
- Good Mobile Messaging Server for Exchange: 7.1.0
- Good Mobile Messaging Server for Domino: 7.0.2

Author	Arne Høye Rage Certifier	
Quality Assurance	Kjartan Jæger Kvassnes Quality Assurance	
Approved	Kjell W. Bergan Head of SERTIT	
Date approved	12 August 2013	

2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
GMC	Good Mobile Control
GMM	Good Mobile Messaging
POC	Point of Contact
SERTIT	Norwegian Certification Authority for IT Security
SFP	Security Function Policy
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy

3 References

[1] Security Target for Good For Enterprise System, Version 1.19, 7 August 2013.

[2] Common Criteria Part 1, CCMB-2009-07-001, Version 3.1 R3, July 2009.

[3] Common Criteria Part 2, CCMB-2009-07-002, Version 3.1 R3, July 2009.

[4] Common Criteria Part 3, CCMB-2009-07-003, Version 3.1 R3, July 2009.

[5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2009-07-004, Version 3.1 R3, July 2009.

[7] Evaluation Technical Report for the evaluation project SERTIT-039, Issue 1.1, 7 August 2013.

(For references to guidance documents, see Annex A.)

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Good For Enterprise System (Versions listed in 4.2) and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target [1], which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The product evaluated was Good For Enterprise System and versions:

- Good For Enterprise iOS client: 2.1.5
- Good For Enterprise Android client: 2.1.2
- Good Mobile Control Server 64bit-Domino: 2.3.1
- Good Mobile Control Server 64bit-Exchange: 2.3.0
- Good Mobile Messaging Server for Exchange: 7.1.0
- Good Mobile Messaging Server for Domino: 7.0.2

These products are also described in this report as the Target of Evaluation (TOE). The developer was Good Technology.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The scope of the evaluation includes software that forms the TOE and the TOE security functions that are stated in the Section 7 of the Security Target for Good for Enterprise System.

The following product features have been excluded from the CC evaluated configuration:

- Self-Service Portal
- Windows 7 and legacy (e.g. Palm, Symbian and Windows Mobile) clients
- GMC Web Services
- Application Management

The settings are described in the document “Good For Enterprise Security Best Practices Version 1.1”.

4.4 Protection Profile Conformance

The Security Target [1] does not claim conformance to any protection profile.

4.5 Assurance Level

The Security Target [1] specifies the assurance requirements for the evaluation. Predefined evaluation assurance level EAL 4 augmented with ALC_FLR.1 is used. Common Criteria Part 3 [4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

The TOE security policies are detailed in ST [1] chapter 4.

Organizational Security Policies are detailed in ST [1] chapter 3.

4.7 Security Claims

The Security Target [1] fully specifies the TOE's security objectives, threats and OSP's which these objectives meet and security functional requirements and security functions to elaborate the objectives. Most of the SFR's are taken from CC Part 2 [3]; use of this standard facilitates comparison with other evaluated products. There are however some functional components that are extended. The rationale for these components can be found in the Security Target [1], chapter 5.

4.8 Threats Countered

- **TT.Eavesdropping**: Malicious actor(s) eavesdropping on intelligible information on mobile devices, and/or data communications in transit between mobile devices.
- **TT.Theft**: A malicious actor or an unauthorized user may get access to corporate information on the mobile device, by theft and/or loss of mobile devices.
- **TT.Tampering**: An unauthorized user or process may be able to bypass the TOE's
  security mechanisms by tampering with the TOE or TOE environment.
- **TT.Access_Info**: A malicious actor passes of as a handheld user, and erases the corporate information on the mobile device.
- **TT.Mod_Conf**: A malicious actor or an unauthorized user may modify the TOE configuration to gain unauthorized access to mobile devices.

4.9 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.10 Environmental Assumptions and Dependencies

- **A.Install**: The TOE has been installed and configured according to the appropriate installation guides, and all traffic between clients and servers flows through it.
- **A.Manage**: There is one or more competent individual (administrator) assigned to manage the TOE and the security of the information it contains.
- **A.No_Evil**: The administrators of the TOE are non-hostile, appropriately trained, and follow all guidance.
- **A.Locate**: The processing resources of the TOE servers will be located within controlled access facilities, which will prevent unauthorized physical access.

4.11 IT Security Objectives

- **O.Secure_Communications**: The TOE shall use secure communications functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted to the TOE.
- **O.Protect**: The TOE must ensure the integrity of audit, system data and corporate information by protecting itself from unauthorized modifications and access to its functions and data, and preserve correct operations during specified failure events.
- **O.Admin**: The TOE must include a set of functions that allow management of its functions and data, ensuring that TOE administrators with the appropriate training and privileges and only those TOE administrators, may exercise such control.
- **O.Authenticate_Admin**: The TOE must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data.
- **O.Authenticate_User**: The TOE must be able to identify and authenticate users prior to allowing access to mobile device functions and data.
- **O.Audit**: The TOE must record the actions taken by administrators, prevent unauthorized deletion of the audit records stored on the TOE, and provide the authorized administrators with the ability to review the audit trail.
- **O.Access_Int**: The TOE must allow access to server resources on protected/internal network only as defined by the Access Control SFP.

4.12 Non-IT Security Objectives

- **OE.Secure_Communications**: The Operational Environment will provide secure communications functions to the TOE including encryption and decryption functions.
- **OE.Manage**: Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely. The reliability of the TOE's timestamps will be ensured via periodic manual checks by the TOE administrator.

- **OE.Physical**: The physical environment must be suitable for supporting TOE servers in a secure setting.
- **OE.Install**: Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
- **OE.Person**: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.

4.13 Security Functional Requirements

- FAU_GEN.1 Audit data generation
- FAU_GEN.1B Client audit data generation
- FAU_GEN.2 User identity association
- FDP_ACC.1A Subset access control - Administrator
- FDP_ACC.1B Subset access control - User
- FDP_ACF.1A Security attribute based access control - Administrator
- FDP_ACF.1B Security attribute based access control - User
- FDP_ITC.2 Import of user data with security attributes
- FDP_SWA_EXP.1 Secure web access
- FDP_CDD_EXP.1 Client Data Deletion
- FIA_AFL.1 Authentication failure handling
- FIA_ATD.1 User attribute definition
- FIA_UAU.1A Timing of authentication - Administrator
- FIA_UAU.1B Timing of authentication - User
- FIA_UID.1 Timing of identification
- FIA_USB.1 User-subject binding
- FMT_MOF.1A Management of security functions behaviour - Administrator
- FMT_MOF.1B Management of security functions behaviour - User
- FMT_MSA.1A Management of Security Attributes - Administrator
- FMT_MSA.1B Management of Security Attributes - User
- FMT_MSA.3A Static Attribute Initialisation - Administrator
- FMT_MSA.3B Static Attribute Initialisation - User
- FMT_SMF.1A Specification of management functions - Administrator
- FMT_SMF.1B Specification of management functions - User
- FMT_SMR.1 Security roles
- FPT_ITT_EXP.1 Basic internal TSF data transfer protection
- FPT_STM.1 Reliable time stamps
- FPT_TDC.1 Inter-TSF basic TSF data consistency
- FTP_ITC_EXP.1 Inter-TSF trusted channel
- FTP_TRP_EXP.1 Inter-TSF trusted path

4.14 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001 [5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a

member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [1], which prospective consumers are advised to read. To ensure that the Security Target [1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [4] and the Common Evaluation Methodology (CEM) [6].

SERTIT monitored the evaluation, which was carried out by Advanced Data Security Commercial Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR) [7] to SERTIT 7 August 2013. SERTIT then produced this Certification Report.

4.15 General Points

The evaluation addressed the security functionality claimed in the Security Target [1] with reference to the assumed operating environment specified by the Security Target [1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target [1]. The results of this work were reported in the ETR [7] under the CC Part 3 [4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

The TOE is delivered electronically. The Good Mobile Control (GMC) and Good Mobile Messaging (GMM) servers are downloaded from the Good Technology's public web site. The iOS client is downloaded from the Apple App Store and the Android client is downloaded from the Google Store.

5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with all the documents that comprise the administrator guidance, user guidance and installation guide provided by the developer.

These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Users of the TOE should follow the guidance for the TOE in order to ensure that it operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

The evaluators have searched for potential vulnerabilities and penetration tests have been devised and performed. The evaluators have not found any exploitable vulnerabilities or residual vulnerabilities in the TOE.

5.6 Developer's Tests

The evaluators have examined the developers test plan and determined that it describes the scenarios for performing each test, including any ordering dependencies on results of other tests. The test plan provides information about the test configuration being used: both on the configuration of the TOE and on any test equipment being used, as well as information about how to execute the tests.

All TSFIs are covered by the developer's tests.

5.7 Evaluators' Tests

The evaluators have employed a combination of a random sampling method and a method based on their intent to cover the TSFI, Security Functions, and subsystems to the maximum extent possible.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR [7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Good For Enterprise System meets Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 4 augmented with ALC_FLR.1 for the specified Common Criteria Part 2 extended functionality, in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of Good For Enterprise System should understand the specific scope of the certification by reading this report in conjunction with the Security Target [1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above in Section 4.3 “TOE Scope” and Section 5 “Evaluation Findings”.

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

- Good For Enterprise iOS client: 2.1.5
- Good For Enterprise Android client: 2.1.2
- Good Mobile Control Server 64bit-Domino: 2.3.1
- Good Mobile Control Server 64bit-Exchange: 2.3.0
- Good Mobile Messaging Server for Exchange: 7.1.0
- Good Mobile Messaging Server for Domino: 7.0.2

TOE Documentation

The supporting guidance documents evaluated were:

[a] Security Target for Good for Enterprise System, v 1.18

[b] Good For Enterprise Security Best Practices, Version 1.1

[c] Good for Enterprise Common Criteria Supplement, Version 1.4

[d] Good Mobile Messaging Good Mobile Control for Microsoft Exchange Administrator's Guide, GMC 2.3.0, GMM 7.1.0, Last revised 05/15/13

[e] Good Mobile Messaging Good Mobile Control for IBM Lotus Domino Administrator's Guide, Good Mobile Control 2.3.1, Good Mobile Messaging 7.0.2, Last revised 05/08/13

[f] Good for Enterprise iPhone User's Guide, Version 2.1.5

[g] Good for Enterprise iPad User's Guide, Version 2.1.5

[h] Good for Enterprise Android Handheld and Tablet User's Guide, Version 2.1.2

[i] Good Mobile Messaging Server Version 7.1.0.34, Good Mobile Control Server 2.3.0.402, for Microsoft Windows Exchange release notes, Updated 02/26/13

[j] Good for Enterprise – iOS v2.1.5.1551 Release Notes, Updated March 26, 2013

[k] Good for Enterprise – Android 2.1.2.254 Release Notes (Service Release), Updated: May 03, 2013

[l] S/MIME on Good for Enterprise Client for iOS, Release Notes, Updated May 30, 2013

[m] S/MIME on Good for Enterprise Client for Android, Updated May 30, 2013

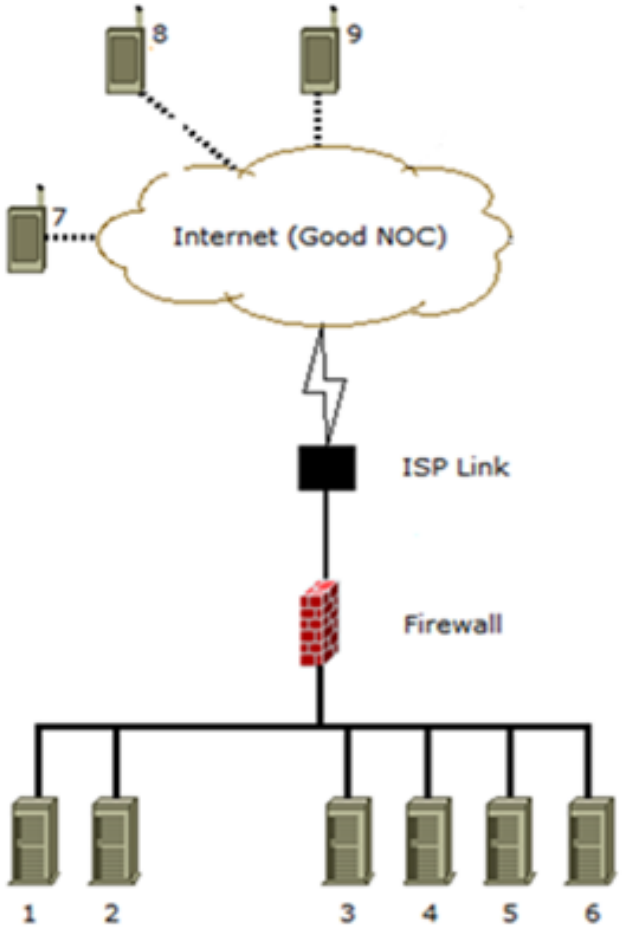
[n] Good Mobile Messaging™ Version 6.0 Installing the Good Mobile Messaging Client from an SD Card README, Last revised 01/08/10

[o] Good Mobile Messaging Good Mobile Control for Microsoft Exchange Quick Installation Guide, Last revised 05/15/13

[p] Good Mobile Messaging Good Mobile Control for IBM Lotus Domino Quick Installation Guide, Last revised 03/28/13
[q] Good for Enterprise - Good Mobile Access (Secure Browser) Guide, Last revised 05/22/13

TOE Configuration

The following configuration was used for testing:



The following tools were used during the evaluation:

- Nessus Vulnerability Scanner, Version 5.0.2
- Wireshark Network Protocol Analyzer - version 1.8.3