SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

SERTIT-063 CR Certification Report

Issue 1.0 09 December 2015

Good Work System

CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009E VERSION 1.1 01.07.2015

SERTIT, P.O. Box 814, N-1306 Sandvika, 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 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. [*]

"The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of the CCRA May 23rd 2000. The recognition under CCRA is limited EAL 4 and ALC_FLR CC part 3 components."

Contents

1 Certification Statement

Good Technology Corporation's Good Work System is an end to end solution for securing and managing email, calendar, contact, presence, instant messaging, secure browsing and other mobile applications.

Good Work System (for versions see chapter 4.2) 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 components of Evaluation Assurance Level EAL 4 augmented with ALC_FLR.1 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended functionality when running on the platforms specified in Annex A.

Author	Rage, Arne Høye Certifier Arne H. Rage
Quality Assurance	Lars Borgos Quality Assurance Lars Borgos
Approved	Øystein Hole Head of SERTIT Øystein Hole
Date approved	09 December 2015

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
EWP	Evaluation Work Plan
ISO/IEC 15408	Information technology –- Security techniques –- Evaluation criteria for IT security
POC	Point of Contact
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] Security Target Release 1.0 for Good Work System, 22 October 2015.

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[5] The Norwegian Certification Scheme, SD001E, Version 9.0, 02 April 2013.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[7] ETR for the evaluation project SERTIT-063, v.1.1, November 12, 2015.

[8] Good Work Security Best Practices, v1.1, October 19, 2015

[9] Good Work Common Criteria Supplement, v.1.4.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Good Work System (for versions see chapter 4.2) to the sponsor/developer, Good Technology Corporation, 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 components.

4.2 Evaluated Product

The evaluated product is Good Work System.

Product version numbers included in this evaluation:

- Good Work Client for iOS: 1.5.3.247
- Good Work Client for Android: 1.5.3.162
- Good Access Client for iOS: 2.4.3.734
- Good Access Client for Android: 2.4.3.657
- Good Dynamics SDK for iOS: 2.0.4413
- Good Dynamics SDK for Android: 2.0.1226
- Good Connect Client for iOS: 2.3.10.0.458445.12
- Good Connect Client for Android: 2.3.10.0.456604.571
- Good Control Server: 2.0.3.11
- Good Proxy Server: 2.0.3.7
- Good Enterprise Mobility Server: 1.5.35.45

This product is described in this report as the Target of Evaluation (TOE). The developer was Good Technology Corporation

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 Work System.

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

- Windows clients are not part of this evaluation
- Domino server interface to GEMS is not supported in this evaluation
- Cloud service is not part of this evaluation

- GFE Client is not part of this evaluation (GFE is covered under separate evaluation).

The settings are described in the document Good Work Security Best Practices[8].

4.4 Protection Profile Conformance

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

4.5 Assurance Level

The Security Target[1] specified the assurance components for the evaluation. Predefined evaluation assurance level EAL 4 augmented with ALC_FLR.1 was 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 the ST[1], chapter 3.

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats and policies which these objectives counter and security functional components 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.

The extended security functional components and the rationale are detailed in the ST[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 off as a mobile device 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 Security Objectives for the TOE

- **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 Good applications 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 Security Objectives for the environment

- **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 Components

Security Audit

FAU_GEN.1	Audit data generation
FAU_GEN.1B	Client audit data generation
FAU_GEN.2	User identity association

User Data Protection

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

Identification and Authentication

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

Security Management

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

Protection of the TSF

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

Trusted Channel/Path

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 SD001E[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 the Advanced Data Security Commercial Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR)[7] to SERTIT in 12 November 2015. 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 delivery and acceptance procedures are described in section 6 of the document Good Work Common Criteria Supplement document[9].

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 guidance 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 deviced a test subset and testing strategy with the intent to cover the TSFI, Security Functions, subsystems and modules to the maximum extent possible. The independent tests concentrated on critical functionality of the TOE, and all tests are passed.

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 Work System (for versions see chapter 4.2) meet the Common Criteria Part 3 conformant components 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 Work System (for versions see chapter 4.2) 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 Work Client for iOS: 1.5.3.247
- Good Work Client for Android: 1.5.3.162
- Good Access Client for iOS: 2.4.3.734
- Good Access Client for Android: 2.4.3.657
- Good Dynamics SDK for iOS: 2.0.4413
- Good Dynamics SDK for Android: 2.0.1226
- Good Connect Client for iOS: 2.3.10.0.458445.12
- Good Connect Client for Android: 2.3.10.0.456604.571
- Good Control Server: 2.0.3.11
- Good Proxy Server: 2.0.3.7
- Good Enterprise Mobility Server: 1.5.35.45

TOE Documentation

The supporting guidance documents evaluated were:

[a] [1] Security Target Release 1.0 for Good Work System, 22 October 2015
[b] Good Work Product Guide, Version 1.4
[c] Determining Versions of Good Work Servers and Clients Document (Dec. 3, 2014)
[d] Good Work Software Development Tools Document (January 22, 2015)
[e] Good Technology Acceptable User Policy, v3.1
[f] Good Work Common Criteria Supplement, Version: 1.4
[g] Collaboration - Good Connect Client Licenses Document
[h] Open Source Components Document
[i] Collaboration - Good 3 Client Licenses – Android Document
[j] Collaboration - Good 3 Client Licenses – iOS Document
[k] GMA on GD - Approved Open Source Licenses Document
[l] GEMS Third Party Library Inventory Document
[m] Good Work Exchange Active Sync Security and Guidance document, Version 0.1
[n] Good Work Cloud Deployment Guide, Version 1.0
[o] Good Work iOS User's Guide, v1.4.3, May 19, 2015
[p] Good Work iOS Release Notes, Version 1.1.1
[q] Good Work Android User's Guide, Version 1.0
[r] Good Work Android Release Notes, Version 1.1.1
[s] Good Access Secure Browser Product Guide, Version 2.1
[t] Good Access Release Notes – iOS, Version 2.1
[u] Good Access Release Notes – Android, Version 2.1
[v] Presence API Specification document, Version 1.0

[w] Good Dynamics Direct Connect, Version 1.8

[x] Good Work Security White Paper, Version 1.02, October 23, 2015

[y] Good Dynamics Server Deployment Planning and Installation Guide, Version 1.8 (Oct. 21, 2014)

[z] Good Dynamics Kerberos Constrained Delegation, Version 1.8

[æ] Good Control Web Services, June 8, 2015 [GD_Web]

[ø] Good Control Console Online Help, Version 1.8

[å] Good Dynamics Backup and Restore, Version 1.8

[aa] Good Dynamics Easy Activation Feature Overview, Version 1.8

[bb] Good Control Cloud Online Help, Version 1.8

[cc] Good Dynamics Secure Mobile Platform for Administrators and Developers

[dd] GEMS Deployment Planning Guide, v2.4 Product Version: 1.4, Doc Rev 3.5.1, June 15, 2015

[ee] GEMS Installation and Configuration Guide, v2.6 Product Version: 1.4, Doc Rev 3.12.2, Last Updated: June 12, 2015

[ff] GEMS Release Notes, Version 1.1

[gg] Good Connect User Guide – iOS, Version 2.0

[hh] Good Connect User Guide – Android, Version 2.0

[ii] Good Access Release Notes – Android, V. 2.1 (Nov. 3, 2014)

[jj] Good Access Release Notes – iOS, V. 2.1 (Nov. 3, 2014)

[kk] Good Dynamics: Good Proxy 1.8.42.11 Release Notes (Dec. 22, 2014)

[ll] Good Dynamics Direct Connect Feature Summary and Configuration Guide, 2014

[mm] Good Dynamics Security White Paper, GD Version 1.6

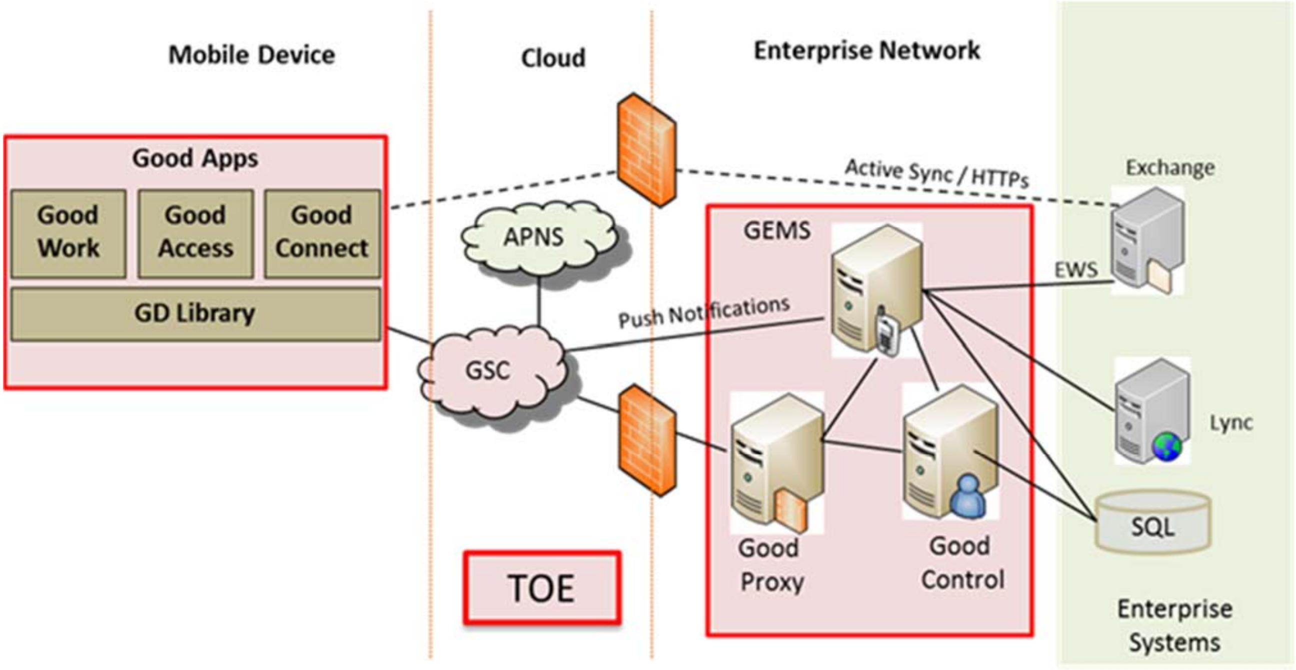
[nn] Good Dynamics Introducing Good Dynamics, 2013

[oo] Good Work Security Best Practices, v1.1, October 19, 2015

[pp] Good Control Web Services, June 8, 2015 [GD_Web]

TOE Configuration

The following configuration was used for testing:


Mobile Device
Cloud
Enterprise Network
Good Apps
Good Work
Good Access
Good Connect
GD Library
APNS
GSC
Push Notifications
Active Sync / HTTPs
GEMS
Exchange
EWS
Lync
SQL
Good Proxy
Good Control
TOE
Enterprise Systems