C081 Certification Report

Lockswitch Bluetooth Access Control System

File name: ISCB-5-RPT-C081-CR-v1
Version: v1
Date of document: 24 August 2017
Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

C081 Certification Report

Lockswitch Bluetooth Access Control System

24 August 2017

ISCB Department

CyberSecurity Malaysia
Level 5, Sapura@Mines,
No 7 Jalan Tasik, The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8992 6888 Fax: +603 8992 6841
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C081 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C081-CR-v1
ISSUE:	v1
DATE:	24 August 2017

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

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

Registered in Malaysia – Company Limited by Guarantee
Company No. 726630-U

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 24 August 2017, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Disclaimer

The Information Technology (IT) product identified in this certification report and its associated certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	4 August 2017	All	Initial draft of certification report
v1	24 August 2017	All	Final version of certification report

Executive Summary

Lockswitch Bluetooth Access Control System is the Target of Evaluation (TOE) for the Common Criteria Evaluation Assurance Level 2 evaluation. Lockswitch Bluetooth Access Control System which consists of Lockswitch Bluetooth Controller (firmware v1.2.4, Hardware v5.4), Lockswitch Cloud (v1.3.1) and Lockswitch Mobile Application (v1.3.4). The TOE provides secure access control systems using Bluetooth technology to restrict unauthorized user to physically access to a restricted assets area. Physical access control is a matter of whom, where, and when. The TOE determines who is allowed to enter or exit, where they are allowed to exit or enter, and when they are allowed to enter or exit. The TOE improved efficiency by minimising operational setbacks and cost related to management of lost keys or cards and broken locks. It also increased accountability by always knowing which assets are accessed when and by whom.

The scope of evaluation covers major security features as follows:

a) **Security Audit**: The TOE (Lockswitch Cloud) generates audit records for security events. The administrator has the ability to view/export the audit logs.

b) **Identification & Authentication**: Lockswitch Cloud users (Administrator and User) and Lockswitch Mobile Application users (Supervisor and Operator) are required to identify or authenticate with the TOE prior to any user action or information flow being permitted.

c) **Security Management**: The TOE (Lockswitch Cloud) provides a wide range of security management functions. The administrator able to configure the TOE via a web browser portal (accessible through any supported web browser stated in Section 1.4.3 in Security Target). Administrator can configure the TOE, manage device, manage user account and view/export the audit logs.

d) **Secure Communication**: The TOE can protect the user data from disclosure and modification by using SSL and Bluetooth encryption as a secure communication.

e) **Tamper Protection**: The TOE (Lockswitch Bluetooth Controller) includes built-in optical and motion tamper detection mechanisms that trigger an alarm response mechanisms to alert the users.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for the TOE, the security function requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2). This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by Securelytics MySEF (Malaysia Security Evaluation Facility) and completed on 25 July 2017.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that Lockswitch Bluetooth Access Control System meets their requirements. It is recommended that a potential user of Lockswitch Bluetooth Access Control System refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE) is Lockswitch Bluetooth Access Control System which consists of Lockswitch Bluetooth Controller, Lockswitch Cloud and Lockswitch Mobile Application. The TOE provides secure access control systems using Bluetooth technology to restrict unauthorized user to physically access to a restricted assets area. Physical access control is a matter of whom, where, and when. The TOE determines who is allowed to enter or exit, where they are allowed to exit or enter, and when they are allowed to enter or exit. The TOE improved efficiency by minimising operational setbacks and cost related to management of lost keys or cards and broken locks. It also increased accountability by always knowing which assets are accessed when and by whom.

2 **Lockswitch Bluetooth Controller** (firmware v1.2.4, Hardware v5.4) - Lockswitch Bluetooth Controller is a hardware Bluetooth access control device built with both physical and network security features to cater for a wide variety of applications. Everything that is required has been built into one compact and easy to install package that takes up a minimal footprint. Below are the features:

a) Battery backed real time clock and non-volatile memory for event recording and storage.

b) OTA firmware update through Bluetooth connection.

c) Configurable output settings for connection to locking devices such as EM Lock, Door strikes, Drop bolts and Electronic Latches.

d) Optical and acoustic indicators to show operation, connection and relay status. Built in optical and motion tamper detection.

e) It comes with wide input voltage range and low power consumption.

3 **Lockswitch Mobile Application** (Android v1.3.4) – Lockswitch Mobile Application runs on an Android platform and act as an access card or physical keys for users to access into a restricted assets area via Lockswitch Bluetooth Controller. Each user utilizes one device policy to prevent sharing of user IDs and passwords on different smartphones. Below are the features:

a) Automatically push all pending events to server and update accessibility changes whenever possible.

b) Does not require data connection to operate as long as accessibility settings have been updated.

c) User automatically locked out on expiry of mandatory sync time.

d) Easy to operate with no local configurations required.

e) Easily view and navigate through all devices.

f) Quick access using PIN or fingerprint validation when switching between tasks.

g) Single app for Lockswitch device initialisation and operation. Capabilities depends on the login user which can be managed by the administrator

h) Optimised design to ensure low data usage and minimal battery drain for the smartphone device.

4 **Lockswitch Cloud** (v1.3.1) - Lockswitch Cloud is a management server that can be hosted either in Lockswitch cloud environment or deployed into customer's privately hosted servers. It enables the user to be constantly in control of all aspects of the system ranging from managing of accessibility, monitoring activities, report generation as well as change tracking. Below are the features:

a) Web based system enable user to access management portal anytime, anywhere.

b) All connections from mobile app and browser to server are done through secure channels via HTTPS.

c) Flexible scheduling to control who can access which device when and for how long.

d) Able to assign individual device rights and accessibility to every single user.

e) Full event and audit trail records with data export functions.

f) Single portal to manage and configure all device and users.

5 The details of TOE functions can be found starting in section 1.4 of the Security Target version 1.0

6 There are five (5) security functionalities covered under the scope of the evaluation which are:

Security Function	**Description**
Security Audit	The TOE (Lockswitch Cloud) generates audit records for security events. The administrator has the ability to view/export the audit logs.
Identification and Authentication	Lockswitch Cloud users (Administrator and User) and Lockswitch Mobile Application users (Supervisor and Operator) are required to identify or authenticate with the TOE prior to any user action or information flow being permitted.
Security Management	The TOE (Lockswitch Cloud) provides a wide range of security management functions. The administrator able to configure the TOE via a web browser portal (accessible through any supported web browser stated in Section 1.4.3). Administrator can configure the TOE, manage device,

	manage user account and view/export the audit logs.
Secure Communication	The TOE can protect the user data from disclosure and modification by using Secure Socket Layer (SSL) and Bluetooth encryption as a secure communication.
Tamper Protection	The TOE (Lockswitch Bluetooth Controller) includes built-in optical and motion tamper detection mechanisms that trigger an alarm response mechanisms to alert the users.

1.2 TOE Identification

7 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C081
TOE Name	Lockswitch Bluetooth Access Control System which consists of: • Lockswitch Bluetooth Controller • Lockswitch Cloud • Lockswitch Mobile Application
TOE Version	• Lockswitch Bluetooth Controller (firmware v1.2.4, Hardware v5.4) • Lockswitch Cloud (v1.3.1) • Lockswitch Mobile Application (Android v1.3.4)
Security Target Title	Lockswitch Bluetooth Access Control System Security Target
Security Target Version	1.0
Security Target Date	10 July 2017
Assurance Level	Evaluation Assurance Level 2 (EAL2)
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref [2])
Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref [3])
Protection Profile Conformance	None

Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant
Sponsor and Developer	Lockswitch Sdn Bhd 32A-2B, Jalan PJU 1/3B, Sunway Mas Commercial Centre, Petaling Jaya, 47301 Selangor Darul Ehsan
Evaluation Facility	Securelytics MySEF

1.3 Security Policy

8 There are no organisational security policies that have been defined regarding the use of the TOE.

1.4 TOE Architecture

9 The TOE includes both logical and physical boundaries, which are described in Section 1.5 of the Security Target (Ref [6]).

10 The following figure 1 shows the evaluated configuration that comprise the TOE:

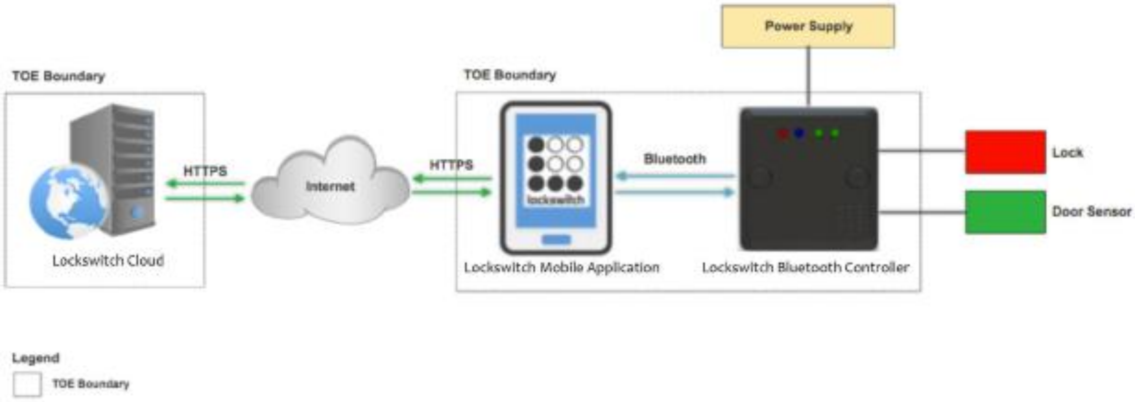

Figure 1: TOE Deployment Architecture

:

1.4.1 Logical Boundaries

11 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality:

a) Security Audit: The TOE (Lockswitch Cloud) generates audit records for security events. The administrator has the ability to view/export the audit logs.

b) Identification and Authentication: Lockswitch Cloud users (Administrator and User) and Lockswitch Mobile Application users (Supervisor and Operator) are required to identify or authenticate with the TOE prior to any user action or information flow being permitted.

c) Security Management: The TOE (Lockswitch Cloud) provides a wide range of security management functions. The administrator able to configure the TOE via a web browser portal (accessible through any supported web browser stated in Section 1.4.3 in Security Target). Administrator can configure the TOE, manage device, manage user account and view/export the audit logs.

d) Secure Communication: The TOE can protect the user data from disclosure and modification by using SSL and Bluetooth encryption as a secure communication.

e) Tamper Protection: The TOE (Lockswitch Bluetooth Controller) includes built-in optical and motion tamper detection mechanisms that trigger an alarm response mechanisms to alert the users.

1.4.2 Physical Boundaries

12 The TOE includes both logical and physical boundaries, which are described in Section 1.5.1 and 1.5.2 of the Security Target (Ref [6]).

1.5 Clarification of Scope

13 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, trained personnel, and secure communication in accordance with user guidance that is supplied with the product.

14 Section 1.4 of this document describes the scope of the evaluation which was limited to those claims made in the Security Target (Ref [6]).

15 Potential consumers of the TOE are advised that some functions and services of the overall product have not have been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

16 This section summarises the security aspects of the environment/configuration in which the IT product is intended to operate. Consumers should understand their own IT environments that are required for secure operation of the TOE, which is defined in the Security Target (Ref [6]).

1.6.1 Usage assumptions

17 Assumption for the TOE usage as listed in Security Target:

a) One or more competent, trusted personnel who are not careless, willfully negligent, or hostile, are assigned and authorized as the TOE Administrators, and do so using and abiding by guidance documentation.
b) Mobile device users are not willfully negligent or hostile, and use the device within compliance of a reasonable Enterprise security policy.

1.6.2 Environment assumptions

18 Assumptions for the TOE environment listed in the Security Target are:

a) The appliance hosting the operating system and database are in a secure operating facility with restricted physical access and non-shared hardware.

b) The TOE relies upon a trustworthy platform and local network from which it provides administrative capabilities. The TOE relies on this platform to provide logon services via a local or network directory service, and to provide basic audit log management functions. The platform is expected to be configured specifically to provide TOE services, employing features such as a host-based firewall which limits its network role to providing TOE functionality.

c) The platforms on which the TOE operate shall be able to provide reliable time stamps.

1.7 Evaluated Configuration

19 The evaluated configuration is described in Section 4 Lockswitch Bluetooth Access Control System Guidance Document.

20 All software installed on the underlying platform must be examined and vetted prior to installation to ensure that it is not malicious or potentially harmful.

21 Both the TOE and the underlying operating system must be regularly updated with software and security patches to ensure continuing secure operation.

1.8 Delivery Procedures

22 The delivery process as stated below:

a) For Lockswitch Cloud, there are two (2) delivery processes practised by Lockswitch Sdn Bhd.

   i) For Lockswitch Public Cloud subscriber, a login credential will be provided to the appointed Administrator by the client/customer. This login credential will then be used to login and perform operations on Lockswitch Public Cloud.

   ii) For Lockswitch Private Cloud subscriber (private server deployment), Lockswitch Sdn Bhd will have a consultant to initiate a project with the client/customer which cover server and network planning.

b) For Lockswitch Mobile Application on Android platform, it can be downloaded from Google Playstore. Lockswitch Sdn Bhd will provide a user manual that has a link and QR code to download from play store.

c) For Lockswitch Bluetooth Controller, it will be packaged using foam in a packaging box and secured using security seal. Upon receiving the product, Administrator shall verify that the controller is not tampered during delivery process by checking the security seal. Any tampered product shall be returned to Lockswitch Sdn Bhd immediately.

23 Further information about these procedures is provided in Section 2 of the Delivery documentation.

1.9 Documentation

24 It is important that the TOE is used in accordance with the guidance documentation in order to ensure secure usage of the product.

25 The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product:

[1]. Lockswitch Bluetooth Access Control System Guidance Document, Version 1.0, 10 July 2017

2 Evaluation

26 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 4 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 (EAL2). The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [5]).

2.1 Evaluation Analysis Activities

27 The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

28 The evaluators checked that the TOE provided for evaluation is labelled with its reference.

29 The evaluators checked that the TOE references used are consistent.

30 The evaluators examined the method of identifying configuration items to determine that it describes how configuration items are uniquely identified.

31 The evaluators examined the configuration items to determine that they are identified in a way that is consistent with the CM documentation.

32 The evaluators checked that the configuration list includes the

a) the TOE itself;

b) the parts that comprise the TOE;

c) the evaluation evidence required by the SARs

33 The evaluators examined the configuration list to determine that it uniquely identifies each configuration item.

34 The evaluators checked that the configuration list indicates the developer of each TSF relevant configuration item.

35 The evaluators examined the delivery documentation to determine that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

36 The evaluators examined aspects of the delivery process to determine that the delivery procedures are used.

2.1.2 Development

37 The evaluators examined the functional specification to determine that the TSF is fully represented, it states the purpose of each TSFI and the method of use for each TSFI is given.

38 The evaluators examined the presentation of the TSFI to determine that it completely identifies all parameters associated with every TSFI.

39 The evaluators examined the presentation of the TSFI to determine that it completely and accurately describes all parameters associated with every TSFI.

40 The evaluators examined the presentation of the TSFI to determine that it completely and accurately describes the SFR-enforcing actions associated with the SFR-enforcing TSFIs.

41 The evaluators examined the presentation of the TSFI to determine that it completely and accurately describes error messages that may result from SFR-enforcing actions associated with each SFR-enforcing TSFI.

42 The evaluators checked that the tracing links the SFRs to the corresponding TSFIs.

43 The evaluators examined the functional specification to determine that it is a complete and accurate instantiation of the SFRs

44 The evaluators examined the security architecture description to determine that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design document.

45 The evaluators examined the security architecture description to determine that it describes the security domains maintained by the TSF.

46 The evaluators examined the security architecture description to determine that the initialisation process preserves security.

47 The evaluators examined the security architecture description to determine that it contains information sufficient to support a determination that the TSF is able to protect itself from tampering by untrusted active entities.

48 The evaluators examined the security architecture description to determine that it presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

49 The evaluators examined the TOE design to determine that the structure of the entire TOE is described in terms of subsystems and all subsystems of the TSF are identified.

50 The evaluators examined the TOE design to determine that each SFR-supporting or SFR-non-interfering subsystem of the TSF is described such that the evaluator can determine that the subsystem is SFR-supporting or SFR-non-interfering.

51 The evaluators examined the TOE design to determine that it provides a complete, accurate, and high-level description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

52 The evaluators examined the TOE design to determine that interactions between the subsystems of the TSF are described.

53 The evaluators examined the TOE design to determine that it contains a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

54 The evaluators examined the TOE security functional requirements and the TOE design, to determine that all ST security functional requirements are covered by the TOE design.

55 The evaluators examined the TOE design to determine that it is an accurate instantiation of all security functional requirements.

2.1.3 Guidance documents

56 The evaluators examined the operational user guidance to determine that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

57 The evaluators examined the operational user guidance to determine that it describes, for each user role, the secure use of the available interfaces provided by the TOE.

58 The evaluators examined the operational user guidance to determine that it describes, for each user role, the available security functionality and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

59 The evaluators examined the operational user guidance to determine that it describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

60 The evaluators examined the operational user guidance and other evaluation evidence to determine that the guidance identifies all possible modes of operation of the TOE (including, if applicable, operation following failure or operational error), their consequences and implications for maintaining secure operation.

61 The evaluators examined the operational user guidance to determine that it describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

62 The evaluators examined the operational user guidance to determine that it is clear and it is reasonable.

2.1.4 IT Product Testing

63 Testing at EAL2 consists of assessing developer tests, performing independent functional tests, and performing penetration tests. The TOE testing was conducted by evaluators from Securelytics MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Report.

2.1.4.1 Assessment of Developer Tests

64 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator).

65 The evaluators analysed the developer's test coverage and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

66 At EAL2, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing sample of the developer's test plan, and creating test cases that augment developer tests.

67 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The evaluators confirmed that the developer supplied test documentation includes test plans, expected test results and actual test results. The results of the independent functional tests that were developed and performed by the evaluators are consistent with the expected test results in the test documentation.

Identifier	Security Function	Descriptions
F001 – Identification and Authentication (Lockswitch Cloud) Security Management (Lockswitch Cloud) Subset access control Security attribute based access control	FIA_ATD.1a FIA_UID.2 FIA_UAU.2 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1b FMT_SMF.1 FMT_SMR.1 FDP_ACC.1 FDP_ACF.1	1. To test that each user to be successfully authenticated and identified before allowing any other TSF-mediated actions on behalf of that user. 2. To test that the TOE maintains the roles Administrator and Authorised User 3. To test that the TOE enforce the access control SFP to restrict the ability to change default and modify the security attributes Password, Roles and Permission to Administrators. 4. To test that the TOE maintain the following list of security attributes belonging to individual users; Username, Password, Role. 5. To test that the TOE enforce access control SFP to provide permissive default values for security attributes that are used to enforce the SFP. 6. To test that the TOE performs the following management functions: a. Account Management, b. Device Management, c. User Management, 7. To test that the TOE restricts the ability to manage the TSF data on the Lockswitch Cloud to Administrators and Authorised User 8. To test that the TOE enforces the access control SFP on objects listed in Section 5.2.4 of the Security Target (Ref [6]). 9. To test that first-time Lockswitch Cloud users must enter a verification code before performing any action on the TOE for the first time

Identifier	Security Function	Descriptions
F002 – Identification and Authentication (Lockswitch Cloud) Security Management (Lockswitch mobile application and controller) Subset access control Security attribute based access control	FIA_ATD.1b FMT_MTD.1a FDP_ACC.1 FDP_ACF.1	1. To test that the TOE maintains the following list of security attributes belonging to individual users; username and password. 2. To test that the TOE restricts the ability to modify the User passcode to User. 3. To test that the TOE enforces the access control SFP on objects listed in Section 5.2.4 of the Security Target (Ref [6]). – Mobile User. 4. To test that the users able to update their Lockswitch mobile application screen lock once they have authenticated with the TOE
F003 – User-initiated session locking (Lockswitch mobile application)	FTA_SSL.2	1. To test that the TOE allows user-initiated locking of the user's own interactive session, by: a. clearing or overwriting display devices, making the current contents unreadable; b. disabling any activity of the user's data access/display devices other than unlocking the session. 2. To test that the TOE requires the following events to occur prior to unlocking the session; user draw phone passcode
F004 – Trusted Path	FTP_TRP.1	1. To test that the TOE provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure 2. To test that the TOE permit remote users to initiate communication via the trusted path 3. To test that the TOE require the use of the trusted path for initial user authentication and other services for which trusted path is required
F005 – Security Audit	FAU_GEN.1 FAU_SAR.1	1. To test that the TOE able to generate audit record of the following auditable events: a. User’s Activity i. Event date

Identifier	Security Function	Descriptions
		ii. Device associated with the user iii. User's login email iv. Activity type v. Type of module vi. Existing data and; vii. Change data b. Device Transaction i. Event date ii. Recorded date iii. Account iv. Device v. User vi. UUID vii. Group and; 2. To test that the TOE record within each audit record at least the following information: 3. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and 4. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, To test that the TOE provide the Administrator and User with the capability to read basic information from the audit records and provide the audit records in a manner suitable for the user to interpret the information.
F006 – Notification of Physical Attack	FPT_PHP.2	1. To test that the TOE provide detection of physical tampering that might compromise the controller. 2. To test that the TOE provide the capability to determine whether physical tampering with the controller. For [the TOE casing], the TSF shall monitor the devices and elements and notify [anyone] when physical tampering with the TSF's devices or TSF's elements has occurred.

68 All testing performed by the evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration Testing

69 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, and security architecture description.

70 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing a Basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapse time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other requirement for exploitation.

71 The penetration tests focused on:

a) SQL Injection

b) Cross Site Scripting

c) Cross-site Request Forgery (CSRF)

d) Missing Function Level Access Control

e) Insecure Direct Object References

f) Directory Traversal

g) Buffer Overflow

72 The results of the penetration testing noted that there was no residual vulnerability found. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in the Security Target (Ref [6]).

2.1.4.4 Testing Results

73 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in the Security Target and its functional specification. In addition, the documentation supplied as evidence for the EAL2 Common Criteria evaluation of the TOE was analysed to identify possible vulnerabilities.

3 Result of the Evaluation

74 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of Lockswitch Bluetooth Access Control System performed by Securelytics MySEF.

75 Securelytics MySEF, found that Lockswitch Bluetooth Access Control System upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) assurance Level 2 (EAL2).

76 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

77 EAL2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

78 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to an attacker possessing a Basic attack potential.

79 EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

80 The following recommendations are made:

a) The users should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

b) The users must maintain the confidentiality, integrity and availability of security relevant data for TOE initialization, start-up and operation if stored or handled outside the TOE

c) System Auditor should review the audit trail generated and exported by the TOE periodically

d) The users must ensure appropriate network protection is maintained, the network on which the TOE is installed must be both physically and logically protected.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July 2014.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[4] MyCC Scheme Policy (MyCC_P1), v1d, CyberSecurity Malaysia, 26 February 2016.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1c, 26 February 2016.

[6] Lockswitch Bluetooth Access Control System Security Target, Version 1.0, 10 July 2017

[7] Evaluation Technical Report Lockswitch Bluetooth Access Control System, T1703-3-ETR v1.0, 25 July 2017

A.2 Terminology

A.2.1 Acronyms

Table 2: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
TSF data	Data created by and for the TOE, which might affect the operation of the TOE.
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
TSFI	TOE Security Functions Interface
SFR	Security Functional Requirement
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register

Acronym	Expanded Term
MySEF	Malaysian Security Evaluation Facility
API	Application Programming Interface
CC	Common Criteria
EAL	Evaluation Assurance Level
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
OS	Operating System
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

A.2.2 Glossary of Terms

Table 3: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65

Term	Definition and Source
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---