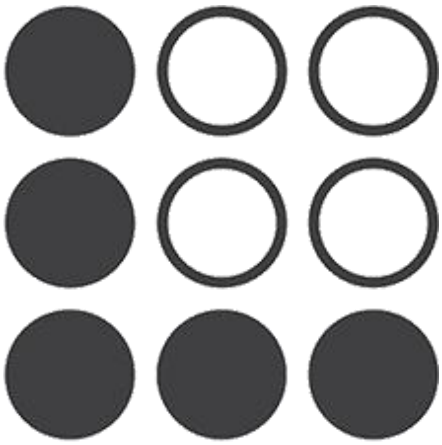

LOCKSWITCH BLUETOOTH ACCESS CONTROL SYSTEM

SECURITY TARGET

VERSION 1.0
10-JULY-17

Document management

Document identification

Document ID	Lockswitch_EAL2_ST
Document title	Lockswitch Bluetooth Access Control System Security Target
Document Version/Date	Version 1.0 (10-JULY-17)

Document history

Version	Date	Description
0.1	10-JAN-17	Released for internal review.
0.2	18-FEB-17	Revised Section 1 and Section 5 Add in Section 7 – TOE Summary Specification
0.3	01-JUNE-17	Revised Section 3, Section 4 and Section 5 based on Evaluation Observation Report (EOR) from the evaluator
1.0	10-JULY-17	Final Released

Table of Contents

1 Security Target Introduction (ASE_INT.1) 5

1.1 ST Reference 5
1.2 TOE Reference 5
1.3 Document Organization 5
1.4 TOE Overview 7
1.5 TOE Description 12

2 Conformance Claim (ASE_CCL.1) 16

3 Security Problem Definition (ASE_SPD.1) 17

3.1 Overview 17
3.2 Threats 17
3.3 Organisational Security Policies 17
3.4 Assumptions 18

4 Security Objectives (ASE_OBJ.2) 19

4.1 Overview 19
4.2 Security Objectives for the TOE 19
4.3 Security Objectives for the Environment 19
4.4 TOE Security Objectives Rationale 20
4.5 Environment Security Objectives Rationale 22

5 Security Requirements (ASE_REQ.2) 23

5.1 Overview 23
5.2 Security Functional Requirements 24
5.3 Security Requirements Rationale 33

6 TOE Security Assurance Requirements (ASE_REQ.2) 36

6.1 Overview 36
6.2 Justification for SAR selection 37

7 TOE Summary Specification (ASE_TSS.1) 38

7.1 Overview 38
7.2 Security Audit 38
7.3 Identification and Authentication 39
7.4 Security Management 39

7.5 Secure Communication 40
7.6 Tamper Protection 40

1 Security Target Introduction (ASE_INT.1)

1.1 ST Reference

ST Title	Lockswitch Bluetooth Access Control System Security Target
ST Identifier	Lockswitch_EAL2_ST
ST Version/Date	Version 1.0 (10-JULY-17)

1.2 TOE Reference

TOE Title	Lockswitch Bluetooth Access Control System which consists of: • Lockswitch Bluetooth Controller • Lockswitch Cloud • Lockswitch Mobile Application
TOE Version	• Lockswitch Bluetooth Controller (Hardware v5.4, Firmware v1.2.4) • Lockswitch Cloud v1.3.1 • Lockswitch Mobile Application (Android v1.3.4)

1.3 Document Organization

This document is organized into the following major sections:

- Section 1 provides the introductory material for the ST as well as the TOE description (ASE_INT.1).
- Section 2 provides the conformance claims for the evaluation (ASE_CCL.1).
- Section 3 provides the definition of the security problem that the TOE has been designed to address (ASE_SPD.1).
- Section 4 defines the security objectives for the TOE and the environment (ASE_OBJ.2).
- Section 5 contains the security functional and assurance requirements derived from the Common Criteria Part 2 and 3 respectively, which are in turn satisfied by the TOE and the development lifecycle (ASE_REQ.2).
- Section 6 contains the security assurance requirements derived from the Common Criteria, Part 3 (ASE_REQ.2).

- Section 7 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE (ASE_TSS.1).

1.4 TOE Overview

1.4.1 TOE Usage and Major Security Functions

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.

The TOE consists of three (3) parts:

1. **Lockswitch Bluetooth Controller** - 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:

    - Battery backed real time clock and non-volatile memory for event recording and storage.
    - OTA firmware update through Bluetooth connection.
    - Configurable output settings for connection to locking devices such as EM Lock, Door strikes, Drop bolts and Electronic Latches.
    - Optical and acoustic indicators to show operation, connection and relay status. Built in optical and motion tamper detection.
    - It comes with wide input voltage range and low power consumption.

Figure 1 - Lockswitch Bluetooth Controller

2. **Lockswitch Mobile Application** – 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:

    - Automatically push all pending events to server and update accessibility changes whenever possible.
    - Does not require data connection to operate as long as accessibility settings have been updated.
    - User automatically locked out on expiry of mandatory sync time.
    - Easy to operate with no local configurations required.
    - Easily view and navigate through all devices.
    - Quick access using PIN or fingerprint validation when switching between tasks.
    - Single app for Lockswitch device initialisation and operation. Capabilities depends on the login user which can be managed by the administrator
    - Optimised design to ensure low data usage and minimal battery drain for the smartphone device.

3. **Lockswitch Cloud** - 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:

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

- All connections from mobile app and browser to server are done through secure channels via HTTPS.
- Flexible scheduling to control who can access which device when and for how long.
- Able to assign individual device rights and accessibility to every single user.
- Full event and audit trail records with data export functions.
- Single portal to manage and configure all device and users.

The following table highlights the range of security functions implemented by the TOE.

Security functions	Descriptions
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.

1.4.2 TOE Type

The TOE is consists of three (3) separate components; Lockswitch Bluetooth Controller, Lockswitch Mobile Application and Lockswitch Cloud. The TOE provides security functionality such as Security Audit, Identification and Authentication, Security Management, Secure Communication and Tamper Protection. The TOE can be categorised as ***Access Control Devices and Systems*** in accordance with the categories identified on the Common Criteria Portal (www.commoncriteriaportal.org) that lists all the certified products.

1.4.3 Supporting hardware, software and/or firmware

Minimum System Requirements	
Lockswitch Bluetooth Controller	
Hardware Specification	• 2 Form C Relay rated up to 24V,1A • 1 OC Output rated up to 24V, 250mA • 2 Inputs for Door sensor and Lock Bypass status with built in ESD protection. • 16bit, 32MHz RISC processor. • Bluetooth Low Energy 4.1. • 1000 transactions storage. • Mounted on single gang electrical box or DIN rail using adaptors. • UL94 Polycarbonate enclosure with pluggable terminal blocks. • Power Requirements: 7-24Vdc, 100mA • Dimension: 86mm x 86mm x 26mm • Interior Use only
Lockswitch Mobile Application	
Operating Systems for Mobile Devices	• Android v4.4.4 Kit Kat
Lockswitch Cloud	
Web Browser	Modern HTML 5 browser which include: • Microsoft Internet Explorer 11 • Microsoft Edge 14 • Mozilla Firefox 48 • Google Chrome 52

	• Apple Safari 10.0.1 • Opera 41
Operating System	Linux with kernel 3.10 which include: • Ubuntu Precise 12.04 (LTS), Ubuntu Trusty 14.04 (LTS), Ubuntu Wily 15.10, Ubuntu Xenial 16.04 (LTS) • Red Hat Enterprise Linux 7 • CentOS 7.X • Fedora version 22, 23, and 24 • Debian 7.7 Wheezy (backports required), Debian 8.0 Jessie • Oracle Linux 6 and 7 • openSUSE 13.2, SUSE Linux Enterprise 12

1.5 TOE Description

1.5.1 Physical scope of the TOE

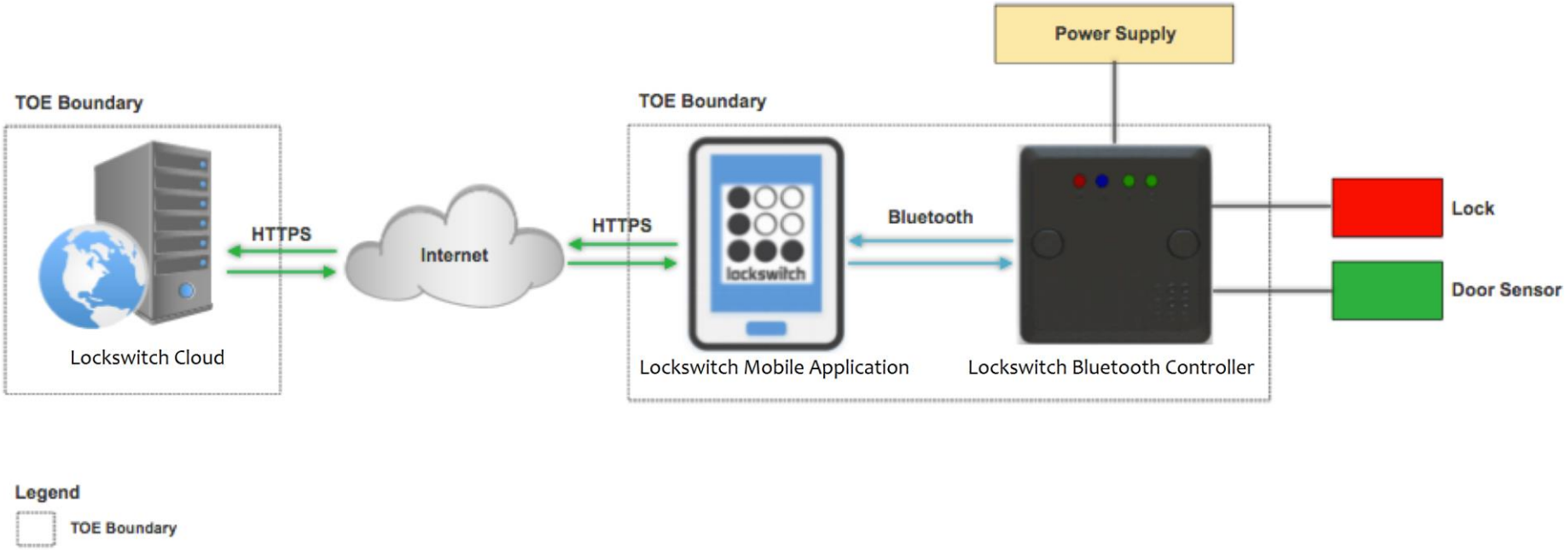

Figure 2 – TOE Deployment Architecture

Below are the descriptions of the components stated in Figure 2 above.

Component	Descriptions
Lockswitch Bluetooth Controller	Lockswitch Bluetooth Controller is mounted on the secured side either on the casing of the door or on the wall near the door. It uses power supply to power up the device and has a built-in battery for real time clock. Lockswitch Bluetooth Controller is connected to an electronic lock (locking devices such as EM Lock, Door strikes, Drop bolts and Electronic Latches) and magnetic door sensor. For more detail hardware specification, refer to Section 1.4.3
Lockswitch Mobile Application	Lockswitch Mobile Application is installed in an Android platform smartphone and has the ability to control the Lockswitch Bluetooth Controller either to lock or unlock the door via Bluetooth connection. Lockswitch Mobile Application also communicate with Lockswitch Cloud via HTTPS connections to perform TOE operations. For more detail on operating system specification, refer to Section 1.4.3
Lockswitch Cloud	Lockswitch Cloud is hosted either in Lockswitch cloud server environment or hosted into customer's privately hosted servers. For more detail on operating systems specification, refer to Section 1.4.3
Power Supply	The power supply is used to power up the Lockswitch Bluetooth controller. For more detail specification, refer to Section 1.4.3
Lock	A locking device which operates by means of electric current. Example of locking device are EM Lock, Door strikes, Drop bolts and Electronic Latches.
Door Sensor	A magnetic door sensor attached to a wall/door.

1.5.2 Logical scope of the TOE

The logical boundary consists of the security functionality of TOE is summarized below.

- **Security Audit:** The TOE (Lockswitch Cloud) generates audit records for security events. Only the administrator has the ability to view/export the audit logs. There are two types of audit event log:
    - Activity – The Activity audit event is catered for the Lockswitch Cloud user's activities (Administrator/User) audit log. It captures events such as event date, device associated with the user, user's login email, activity type, type of module, existing data and change data.
    - Transaction – The Transaction audit event is catered for the device (Lockswitch Controller) audit log. It captures events such as event date, recorded date, account, device, user, UUID (Universal Unique Identifier), group and descriptions.

  The exported audit logs can be either in PDF or CSV file format.

- **Identification and Authentication:** All users are required to perform identification and authentication with the TOE before any information flows are permitted.
    - Lockswitch Cloud - Administrator and user must be authenticated to the server prior to performing any TOE functions by entering a registered email and password.
    - Lockswitch Mobile Application – Supervisor and Operator must be authenticated to the application by entering the server domain name, a registered email and password before performing any TOE functions. Upon the smartphone screen lock, these users are required to enter a pin code or fingerprint validation before the TOE allows the users to continue performing any action. Each user utilizes one device policy to prevent sharing of user IDs and passwords. The credential is unique and only applicable on a single device.

- **Security Management**: The TOE provides a wide range of security management functions. For Lockswitch Cloud, 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 manage the TOE device (Lockswitch Bluetooth Controller), manage user account and view/export the audit logs.

- **Secure Communication:** The TOE can protect the user data from disclosure and modification using Secure Socket Layer (SSL) as a secure communication between:
    - Remote Administrator/users and Lockswitch Cloud
    - Lockswitch Mobile Application and Lockswitch Cloud

  The TOE also able to protect the user data from disclosure and modification using Bluetooth encryption as a secure communication between the smartphone and Lockswitch Bluetooth Controller

- **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.

2 Conformance Claim (ASE_CCL.1)

The ST and TOE are conformant to version **3.1 (REV 4)** of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the TOE and ST:

- **Part 2 conformant.** Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1 (REV 4), September 2012

- **Part 3 conformant, EAL2.** Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1 (REV 4). Evaluation is EAL2, September 2012.

3 Security Problem Definition (ASE_SPD.1)

3.1 Overview

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through:

a) a series of ***threats*** that the TOE has been designed to mitigate,

b) specific ***assumptions*** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and

c) any relevant ***organisational security policies*** are any statements made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

Identifier	Threat statement
T.MANAGEMENT	An unauthorized user modifies management data that they are not authorised to access resulting in a loss of integrity of the data that the TOE uses to enforce the security functions.
T.UNAUTHORISED_ACCESS	A user may gain unauthorized access to the TOE and residing data by sending impermissible information through the TOE (such as Brute Force Attacks) resulting the exploitation of protected resources
T.CONFIG	An unauthorized person may read, modify, or destroy TOE configuration data.
T.TOECOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information or information properties sent between distributed components of the TOE.

3.3 Organisational Security Policies

No organisational security policies have been defined regarding the use of the TOE.

3.4 Assumptions

Identifier	Assumption statement
A.PLATFORM	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.
A.ADMIN	One or more competent, trusted personnel who are not careless, wilfully negligent, or hostile, are assigned and authorized as the TOE Administrators, and do so using and abiding by guidance documentation.
A.USER	Mobile device users are not wilfully negligent or hostile, and use the device within compliance of a reasonable Enterprise security policy.
A.TIMESTAMP	The platforms on which the TOE operate shall be able to provide reliable time stamps.
A.PHYSICAL	It is assumed that the appliance hosting the operating system and database are in a secure operating facility with restricted physical access and non-shared hardware.

4 Security Objectives (ASE_OBJ.2)

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in Section 3. There are security objectives for the TOE to address and additional objectives that provide specific direction for the intended in environment in which the TOE is to operate.

4.2 Security Objectives for the TOE

Identifier	Objective statements
O.ACCESS	The TOE must ensure that only authorised users are able to access protected resources or functions and to explicitly deny access to specific users when appropriate
O.CONFIG	TOE shall prevent unauthorized person to access TOE functions and configuration data. Only authorized TOE Administrator shall have access to TOE management interface.
O.MANAGE	The TOE must allow administrator to effectively manage the TOE, while ensuring that appropriate controls are maintained over those functions.
O.USER	The TOE must ensure that all users are identified and authenticated before accessing protected resources or functions.
O.NOAUTH	The TOE shall protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.
O.TOECOM	The TOE must protect the confidentiality of its dialogue between distributed components.

4.3 Security Objectives for the Environment

Identifier	Objective statements
OE.PLATFORM	The TOE relies upon the trustworthy Mobile platform and hardware to provide policy enforcement as well as cryptographic services and data protection.
OE.ADMIN	The owners of the TOE must ensure that the administrator who manages the TOE is not hostile, competent and apply all administrator guidance in a trusted manner.
OE.USER	Users of the mobile device are trained to securely use the mobile device and apply all guidance in a trusted manner.

Identifier	Objective statements
OE.TIMESTAMP	Reliable timestamp is provided by the operational environment for the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that the appliance hosting the operating system and database are in a secure operating facility with restricted physical access and non-shared hardware.

4.4 TOE Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats and OSPs.

OBJECTIVES \ THREATS/ ASSUMPTIONS/OSPs	T.MANAGEMENT	T.UNAUTHORISED_ACCESS	T.CONFIG	T.TOECOM	A.PLATFORM	A.ADMIN	A.USER	A.TIMESTAMP	A.PHYSICAL
O.ACCESS	✔	✔							
O.CONFIG			✔						
O.MANAGE	✔								
O.USER	✔	✔							
O.TOECOM				✔					
O.NOAUTH		✔							
OE.PLATFORM					✔				
OE.ADMIN						✔			
OE.USER							✔		
OE. TIMESTAMP								✔	
OE. PHYSICAL									✔

The following table demonstrates that all security objectives for the TOE trace back to the threats and OSPs in the security problem definition.

Threats/OSPs	Objectives	Rationale
T.CONFIG	O.CONFIG	The objective ensures that the TOE only allowed authorized person such as TOE Administrator to access TOE functions and configuration data.
T.MANAGEMENT	O.USER	The objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions.
	O.MANAGE	This objective ensures that the TOE provides the tools necessary for the authorized system admin to manage the security-related functions and that those tools are usable only by users with appropriate authorizations.
	O.ACCESS	The objective ensures that the TOE restricts access to the TOE objects to the authorized users and deny access to specific users when appropriate
T.UNAUTHORISED_ACCESS	O.ACCESS	The objective ensures that the TOE restricts access to the TOE objects to the authorized users and deny access to specific users when appropriate
	O.USER	The objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions.
	O.NOAUTH	The objective ensures that the TOE protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.
T.TOECOM	O.TOECOM	The objective ensures that the TOE protect the confidentiality of its dialogue between distributed components.

4.5 Environment Security Objectives Rationale

The following table demonstrates that all security objectives for the operational environment all trace back to assumptions or OSPs in the security problem definition.

Assumptions	Objective	Rationale
A.PLATFORM	OE.PLATFORM	This objective ensures that the underlying platforms are trustworthy and hardened to protect against known vulnerabilities and security configuration issues.
A.ADMIN	OE.ADMIN	This objective ensures that those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
A.USER	OE.USER	This objective ensures that those responsible for the TOE are competent and trustworthy individuals, capable of operating the TOE and the security of the information it contains in a secure manner.
A.TIMESTAMP	OE.TIMESTAMP	This objective ensures that reliable timestamps are provided by the operational environment for the TOE.
A.PHYSICAL	OE.PHYSICAL	This objective ensures that the appliance that hosts the operating system and database are hosted in a secure operating facility with restricted physical access with non-shared hardware.

5 Security Requirements (ASE_REQ.2)

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 (REV 4) of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

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

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

5.2 Security Functional Requirements

5.2.1 Overview

The security functional requirements are expressed using the notation stated in Section 5.1 above and itemised in the table below.

Identifier	Title
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FIA_ATD.1a	User attribute definition (Lockswitch Cloud)
FIA_ATD.1b	User attribute definition (Lockswitch Mobile Application)
FIA_UID.2	User identification before any action
FIA_UAU.2	User authentication before any action
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1a	Management of TSF data (Lockswitch Cloud)
FMT_MTD.1b	Management of TSF data (Lockswitch Mobile Application)
FMT_MOF.1	Management of security functions behaviour (Lockswitch Cloud)
FMT_SMF.1	Specification of Management Functions (Lockswitch Cloud)
FMT_SMR.1	Security Roles
FTA_SSL.2	User-initiated session locking (Lockswitch Mobile Application)
FTP_TRP.1	Trusted Path
FPT_PHP.2	Notification of physical attack (Lockswitch Bluetooth Controller)

5.2.2 FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
FAU.GEN.1.1	The TSF shall be able to generate an audit report of the following auditable events: ~~a) Start-up and shutdown of the audit functions;~~ b) All auditable events for the [***not specified***] level of audit; and c) [**Specifically defined auditable events listed in the Notes section below**].
FAU.GEN1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**none**].
Dependencies:	FPT.STM.1 Reliable time stamps
Notes:	Auditable events within the TOE: • Activity ○ Event date ○ Device associated with the user ○ User's login email ○ Activity type ○ Type of module ○ Existing data and; ○ Change data • Transaction ○ Event date ○ Recorded date ○ Account ○ Device ○ User ○ UUID (Universal Unique Identifier) ○ Group and; ○ Descriptions

5.2.3 FAU_SAR.1 Security Audit Review

Hierarchical to:	No other components.
FAU_SAR.1.1	The TSF shall provide [**administrator**] with the capability to read [**all audit information**] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies:	FAU_GEN.1 Audit data generation
Notes:	None.

5.2.4 FDP_ACC.1 Subset access control

<table>
<tr><td>Hierarchical to:</td><td colspan="3">No other components.</td></tr>
<tr><td>FDP_ACC.1.1</td><td colspan="3">The TSF shall enforce the [access control SFP] on [objects listed in the table below].</td></tr>
<tr><td>Dependencies:</td><td colspan="3">FDP_ACF.1 Security attribute based access control</td></tr>
<tr><td>Notes:</td><td colspan="3">Lockswitch Cloud
<table>
<tr><th>Subject</th><th>Object</th><th>Operation</th></tr>
<tr><td rowspan="6">Administrator</td><td>Account</td><td>View/Update/Reset/Unlink Mobile</td></tr>
<tr><td>Device</td><td>View/Add/Edit/Delete</td></tr>
<tr><td>Device Trigger Pattern</td><td>Add/Edit/Delete/Auto/Manual</td></tr>
<tr><td>User</td><td>Add/Edit (Set Device, Change Role, Unlink)/Delete</td></tr>
<tr><td>Activity</td><td>View/Clear Filters/Export (PDF/CSV)</td></tr>
<tr><td>Transaction</td><td>View/Clear Filters/Remap/Export (PDF/CSV)</td></tr>
<tr><td rowspan="2">User</td><td>Account</td><td>Update/Reset</td></tr>
<tr><td>Transaction</td><td>View/Clear Filters/Remap/Export (PDF/CSV)</td></tr>
</table></td></tr>
</table>

	Lockswitch Mobile Application **Subject** / **Object** / **Operation** Supervisor / List of devices / View Device Location / View Device Operation / Open/Lock/Activate Operator / List of devices / View Device Location / View Device Operation / Open/Lock

5.2.5 FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**access control SFP**] to objects based on the following: [**as listed in the Notes section of FDP_ACC.1**].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**a) First Time login to Lockswitch Cloud, Administrators/Users must set their password before performing any action for the first time** **b) Administrators/Users must enter their email address and password before performing any action on the Lockswitch Management Server** **c) Supervisor and Operator must enter their Domain Server, email address and password before performing any action on the Lockswitch Mobile Application. The credential is unique and only applicable on a single device** **d) Supervisor and Operator can update their Lockswitch Mobile Application pin code once they have authenticated with the TOE**]
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Notes:	None.

5.2.6 FIA_ATD.1a User attribute definition (Lockswitch Cloud)

Hierarchical to:	No other components.
FIA_ATD.1a.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**Email Address, Password**]
Dependencies:	No dependencies.
Notes:	None.

5.2.7 FIA_ATD.1b User attribute definition (Lockswitch Mobile Application)

Hierarchical to:	No other components.
FIA_ATD.1b.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**Domain Name, Email Address, Password, Pin Code**]
Dependencies:	No dependencies.
Notes:	None.

5.2.8 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.9 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies
Notes:	None.

5.2.10 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [**access control SFP**] to restrict the ability to [***change_default, modify, delete]*** the security attributes [**Administrator Account, Device Configuration, Users Account**] to [**Administrators**].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.11 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [**access control SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [**none**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

5.2.12 FMT_MTD.1a Management of TSF data (Lockswitch Cloud)

Hierarchical to:	No other components.
FMT_MTD.1a.1	The TSF shall restrict the ability to [***manage***] the [**TSF data on the Lockswitch Cloud**] to [**Administrators]**
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.13 FMT_MTD.1b Management of TSF data (Lockswitch Mobile Application)

Hierarchical to:	No other components.
FMT_MTD.1b.1	The TSF shall restrict the ability to [***modify***] the [**User pin code**] to [**Supervisor, Operator**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.14 FMT_MOF.1 Management of security functions behaviour (Lockswitch Cloud)

Hierarchical to:	No other components.
FMT_MOF.1.1	The TSF shall restrict the ability to [***determine the behaviour of, modify the behaviour of***] the functions [**Lockswitch Bluetooth Controller Alarm Trigger Pattern**] to [**Administrator**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.15 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**a) Account Management,** **b) Device Management,** **c) User Management,** **d) Unlink Operator**].
Dependencies:	No dependencies.
Notes:	None.

5.2.16 FMT_SMR.1 Security Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**Administrator, User, Supervisor and Operator**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.17 FTA_SSL.2 User-initiated locking (Lockswitch Mobile Application)

Hierarchical to:	No other components.
FTA_SSL.2.1	The TSF shall allow 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.
FTA_SSL.2.2	The TSF shall require the following events to occur prior to unlocking the session: [**User to enter a pin code or fingerprint scanning**].
Dependencies:	FIA_UAU.1 Timing of authentication
Notes:	None.

5.2.18 FTP_TRP.1 Trusted Path

Hierarchical to:	No other components.
FTP_TRP.1.1	The TSF shall 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***].
FTP_TRP.1.2	The TSF shall permit [***remote users***] to initiate communication via the trusted path
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [***initial user authentication***, [**other services for which trusted path is required**]].
Dependencies:	No dependencies
Notes:	Secure Socket Layer (SSL) as a secure communication between: - Remote Administrator/users and Lockswitch Management Server - Lockswitch Mobile Application and Lockswitch Management Server

	Bluetooth encryption as a secure communication between the smartphone and Lockswitch Controller

5.2.19 FPT_PHP.2 Notification of physical attack (Lockswitch Bluetooth Controller)

Hierarchical to:	FPT_PHP.1 Passive detection of physical attack
FPT_PHP.2.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.2.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.
FPT_PHP.2.3	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.
Dependencies:	FMT_MOF.1 Management of security functions behaviour
Notes:	The TSF shall detect physical tampering performed by opening the cover or forcedly removing the device

5.3 Security Requirements Rationale

5.3.1 Dependency rationale

Below demonstrates the mutual supportiveness of the SFR's for the TOE by demonstrating how the SFR dependencies are fulfilled by the TOE, and by justifying those dependencies that are not fulfilled.

The SARs relevant to the TOE constitute an evaluation assurance level EAL2 as defined in Common Criteria and include no extensions or augmentations. Therefore, as a complete evaluation assurance level, they are a mutually supportive set and require no further justification.

SFR	Dependency	Inclusion
FAU_GEN.1	FPT.STM.1 Reliable time stamps	FPT_STM.1 has not been included as the TOE obtains all audit timestamps from the underlying platform. This has been addressed in Section 3.4 by A.TIMESTAMP.
FAU.SAR.1	FAU.GEN.1 Audit data generation	FAU.GEN.1
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3
FIA_ATD.1a	No dependencies	NA
FIA_ATD.1b	No dependencies	NA
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UID.2	No dependencies	N/A
FMT_MSA.1	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_SMR.1 FMT_MSA.1

SFR	Dependency	Inclusion
FMT_MTD.1a	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_MTD.1b	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FTA_SSL.2	FIA_UAU.1 Timing of authentication	FIA_UAU.2
FTP_TRP.1	No dependencies	N/A
FPT_PHP.2	FMT_MOF.1 Management of security functions behaviour	FMT_MOF.1

5.3.2 Mapping of SFRs to security objectives for the TOE

Security objective	Mapped SFRs	Rationale
O.USER	FIA_UAU.2	The requirement helps meet the objective by authenticating user before any TSF mediated actions.
	FIA_UID.2	The requirement helps meet the objective by identifying user before any TSF mediated actions
O.ACCESS	FAU_GEN.1	The TOE allows set of rules to be applied to indicate authorised and unauthorised access of every user.
	FAU_SAR.1	The TOE maintains a profile of system usage and suspicion rating to each profile along with threshold condition to indicate possible security violation.
	FIA_ATD.1a/b	The requirement helps meet the objective by ensuring user security attributes are maintained.
	FMT_SMF.1	The requirement helps meet the objective by providing management functions of the TOE for authenticated user.

Security objective	Mapped SFRs	Rationale
	FMT_SMR.1	The requirement helps meet the objective by providing user timing of identification.
O.MANAGE	FMT_MTD.1a	The requirement helps meet the objective by restricting the ability to modify the user password.
	FMT_MSA.1	The requirement helps to meet the objective by restricting the ability to modify the security attributes for the administrator.
O.CONFIG	FMT_MTD.1a	The requirement helps meet the objective by restricting user access to management functions.
	FMT_MTD.1b	The requirement helps meet the objective by restricting user access to management functions.
	FMT_MSA.1	The requirement helps meet the objective by restricting user access to security attributes.
	FMT_MSA.3	The requirement helps meet the objective by restricting access to provide default values for security attributes that are used to enforce the SFP.
	FMT_SMR.1	The requirement helps meet the objective by defining the security roles used within the TOE.
	FDP_ACC.1	The requirement provides access control functionality to ensure that access to security functionality is controlled.
	FDP_ACF.1	The requirement provides access control functionality to ensure that access to security functionality is controlled.
	FTA_SSL.2	This requirement helps meet the objective by user-initiated locking sessions.
	FMT_MOF.1	This requirement helps meet the objective by restricting the modification of the TOE behaviour to Administrator
O.TOECOM	FTP_TRP.1	The requirement ensures that data sent by users is protected from modification or disclosure.
O.NOAUTH	FPT_PHP.2	The requirement ensures that the TOE provide notification of physical attack to Administrator

6 TOE Security Assurance Requirements (ASE_REQ.2)

6.1 Overview

EAL2 requires evidence relating to the design information and test results, but does not demand more effort on the part of the developer than is consistent with good commercial practice.

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

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 penetration attackers with a basic attack potential.

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

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_CMC.2 Use of a CM system
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements

Assurance class	Assurance components
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.2 Independent testing - sample
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.2 Justification for SAR selection

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 2 (EAL2).

TOE has a low to moderate level of assurance in enforcing its security functions when instantiated in its intended environment, which imposes no restrictions on assumed activity on applicable networks. EAL2 is sufficient to demonstrate that the TOE is resistant to attackers with a Basic attack potential.

7 TOE Summary Specification (ASE_TSS.1)

7.1 Overview

This section provides the TOE summary specification, a high-level description of how the TOE implements the claimed security functional requirements. The TOE provides the following security functions:

- Security Audit;
- Identification and Authentication;
- Security Management;
- Secure Communication; and
- Tamper Protection

7.2 Security Audit

The TOE (Lockswitch Cloud) will create audit records (which contain the data and time of the event, type of event, subject identity and outcome of the event) for the following auditable events (FAU_GEN.1):

- Activity
  - Event date
  - Device associated with the user
  - User's login email
  - Activity type
  - Type of module
  - Existing data and;
  - Change data
- Transaction
  - Event date
  - Recorded date
  - Account
  - Device
  - User
  - UUID (Universal Unique Identifier
  - Group and;
  - Descriptions

The TOE's (Lockswitch Cloud) Administrators have the capability to review these audit records via the Lockswitch Cloud web interface (FAU_SAR.1). Timestamps for Lockswitch Cloud are generated for audit logs by utilising the underlying operating system. The TOE does not generate its own timestamps for use in audit records; these are supplied by the underlying operating system.

7.3 Identification and Authentication

The TOE implement access control and authentication measures to ensure that TOE data and functionality is not misused by unauthorised parties (FDP_ACC.1). All TOE users must provide authentication data to the TOE to affirm their identity and role prior to being granted access to any TOE functions or interfaces.

- Lockswitch Cloud – Lockswitch Cloud maintains two types of users which are Administrator and User (FMT_SMR.1). These users may access the Lockswitch Cloud via the web interface that the platform provides. Administrator and user must be authenticated to the server prior performing any TOE functions by entering a registered email and password (FIA_ATD.1a, FIA_UAU.2.1, FIA_UID.2.1, FDP_ACF.1). Upon first time login to Lockswitch Cloud, Administrators and Users must set their new password before performing any action (FDP_ACF.1).

- Lockswitch Mobile Application – Lockswitch Mobile Application maintains two types of users which are Supervisor and Operator (FMT_SMR.1). These users must be authenticated to the application by entering the server domain name, a registered email and password before performing any TOE functions (FIA_ATD.1b, FIA_UAU.2, FIA_UID.2, FDP_ACF.1). Lockswitch Mobile Application user can initiate locking of their own interactive sessions (FTA_SSL.2). Upon the smartphone screen lock, Supervisor and Operator will not be able to read the content of the TOE and perform any activity or data access. These users are required to enter a pin code or fingerprint validation before the TOE allows the users to continue performing any action (FTA_SSL.2). Supervisor and Operator can update/modify their Lockswitch Mobile Application pin code once they have authenticated with the TOE by clicking on the 'Forgot' button (FDP_ACF.1, FMT_MTD.1b). Each user utilizes one device policy to prevent sharing of user IDs and passwords. The credential is unique and only applicable on a single device (FDP_ACF.1).

7.4 Security Management

The TOE provides a suite of management functions only to Administrators. These functions allow for the configuration of Lockswitch Cloud and Lockswitch Mobile Application to suit the environment in which it is deployed. Additionally, management roles may perform the following tasks (FMT_SMF.1, FMT_MTD.1a, FMT_MSA.1 and FMT_MSA.3):

- Account Management,

- Device Management,
- User Management,
- Unlink Operator

Both Lockswitch Cloud and Lockswitch Mobile Application implement access control and authentication measures to ensure that TOE data and functionality is not misused by unauthorised parties (FDP_ACC.1 and FDP_ACF.1).

7.5 Secure Communication

The TOE establishes a trusted path (FPT_TRP.1) using the Secure Socket Layer (SSL)/Transport Layer Security (TLS) as a secure communication between:

- Remote Administrator/users and Lockswitch Cloud
- Lockswitch Mobile Application and Lockswitch Cloud

The Secure Socket Layer (SSL) session is based on mutual authentication of the TOE, and the remote instance, using installed digital certificates.

The TOE also able to protect the user data from disclosure and modification using Bluetooth encryption as a secure communication between the smartphone and Lockswitch Bluetooth Controller

7.6 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 (FPT_PHP.2). There are two sensors used in the Lockswitch Bluetooth Controller to perform tamper detection.

- Infrared Sensor positioned at the screw hole where it can detect if someone trying to remove the device by unscrewing
- Motion Sensor is used to detect the changes on orientation and position of Lockswitch Device.

A dedicated output signal line is allocated to connect to external alarm/reporting system. This signal will be triggered upon tampering is detected. The Administrator has the ability to manage the behaviour of the TOE (Lockswitch Bluetooth Controller) alarm trigger pattern (FMT_MOF.1) via the Lockswitch Cloud.