

C134 Certification Report

Smart-Ex 03

File name: ISCB-5-RPT-C134-CR-v1

Version: v1

Date of document: 27 February 2025

Document classification : PUBLIC



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

C134 Certification Report

Smart-Ex 03

27 February 2025

ISCB Department

CyberSecurity Malaysia

Level 7, Tower 1,
Menara Cyber Axis, Jalan Impact,
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999 □ Fax: +603 8008 7000
<http://www.cybersecurity.my>

Document Authorisation

DOCUMENT TITLE: C134 Certification Report

DOCUMENT REFERENCE: ISCB-5-RPT-C134-CR-v1

ISSUE: v1

DATE: 27 February 2025

DISTRIBUTION: UNCONTROLLED COPY - FOR UNLIMITED USE AND
DISTRIBUTION

Copyright Statement

The copyright of this document, which may contain proprietary information, is the property of CyberSecurity Malaysia.

The document shall be held in safe custody.

©CYBERSECURITY MALAYSIA, 2025

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 200601006881 (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, 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 7 March 2025 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 <https://iscb.cybersecurity.my> and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Reproduction of this report is authorised 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 using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (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	6 February 2025	All	Initial draft
v1	27 February 2025	All	Final version

Executive Summary

The Target of Evaluation (TOE) is a Smart-Ex 03 smartphone, a mobile phone designed and developed by Pepperl+Fuchs SE. The product is designed to be used in explosion hazardous locations and for heavy duty use in industrial environments.

Smart-Ex 03 smartphone is a device that features a protection mechanism in the form of smartphone from the aspects of externally and internally. With high performance hardware such as thermal sensors located in specific area inside the smartphone as well as physical protections that prevent high impact damages that may compromise the smartphone integrity.

The scope of evaluation covers the smart battery sensors, physical protection of the device (smartphone casing and its sensor), TOE mobile applications, evaluated configuration of Android OS and evaluated configuration of the hardware components operated within the device.

The TOE provides security functions such as security audit, cryptographic function, user data protection, identification and authentication, security management, TOE access and physical tampering and fault tolerance.

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 functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Users are advised to review the intended operating environment and confirm that the stated security objectives can be effectively met by considering 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 SEF and the evaluation was completed on 6 February 2025.

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 <http://iscb.cybersecurity.my> and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at <http://www.commoncriteriaportal.org>

It is the responsibility of the user to ensure that Smart-Ex 03 meets their requirements. It is recommended that a potential user of the TOE refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Document Authorisation	ii
Copyright Statement	iii
Foreword	iv
Disclaimer	v
Document Change Log	vi
Executive Summary	vii
Index of Tables	x
Index of Figures	x
1 Target of Evaluation	1
1.1 TOE Description	1
1.2 TOE Identification.....	3
1.3 Security Policy	4
1.4 TOE Architecture	4
1.4.1 Logical Boundaries	4
1.4.2 Physical Boundaries	5
1.5 Clarification of Scope	6
1.6 Assumptions	7
1.7 Evaluated Configuration	8
1.8 Delivery Procedures.....	7
2 Evaluation	9
2.1 Evaluation Analysis Activities.....	9
2.1.1 Life-cycle support	9
2.1.2 Development	9
2.1.3 Guidance documents	10
2.1.4 IT Product Testing.....	10
3 Result of the Evaluation	22
3.1 Assurance Level Information.....	22
3.2 Recommendation	22

Annex A References	24
A.1 References	24
A.2 Terminology	24
A.2.1 Acronyms	24
A.2.2 Glossary of Terms	25

Index of Tables

Table 1: TOE Model	1
Table 2: TOE Identification	3
Table 3: Functional Test	19
Table 4: List of Acronyms	24
Table 5: Glossary of Terms	25

Index of Figures

Figure 1: TOE Boundary	2
------------------------	---

1 Target of Evaluation

1.1 TOE Description

- 1 The Target of Evaluation (TOE) is the Smart-Ex 03 smartphone, which operates on the Android Operating System (AOS). The TOE features a complex design of safety capabilities and designed to be used, handled and designed to operate in hazardous and harsh environments.
- 2 Besides its intrinsically safe electronic design, embedded sensors inside the smartphone monitor thermal incidents that may impact the smartphone integrity.
- 3 The TOE is equipped with an intelligent thermal management system that prevents overheating and maintains optimal performance even in hot environments as well as with a Smart-Battery to ensure optimal battery life.
- 4 The rugged design of the TOE includes special housing materials, strengthened glass and shock-absorbing materials, making the TOE highly resistant to physical shocks, falls, or rough handling. The TOE had undergone rigorous testing procedures, including drop tests, impact resistance evaluations, and temperature stress tests, to ensure their ability to withstand various adverse conditions and protects the user in hazardous environments.
- 5 In addition, the TOE consists of the following models, its country specific variants which are based on the same system architecture and software baseline.

Model	Platform	Kernel	Android Version
Smart-Ex 03 DZ1*	QCM6490	5.4.233	13
Smart-Ex 03 DZ2*	QCM6490	5.4.233	13
Smart-Ex 03*	QCM6490	5.4.233	13

Table 1: TOE Model

Note that, the notation “*” are meant as the TOE model is based on country specific variant that may vary in the aspect such as Android GMS services must not be installed in certain countries as per Google Licensing requirement and others that shall be advised by the TOE Developer.

The model that will be using for the evaluation will be Smart-Ex 03*. Note that, the other two models in the table above having the same software, hardware, firmware

and configuration that uses by the Smart-Ex 03*. Thus, due to the similar build up, both models are included in the scope of evaluation. The different labelling on the models is basically the different name used for marketing in different country and region.

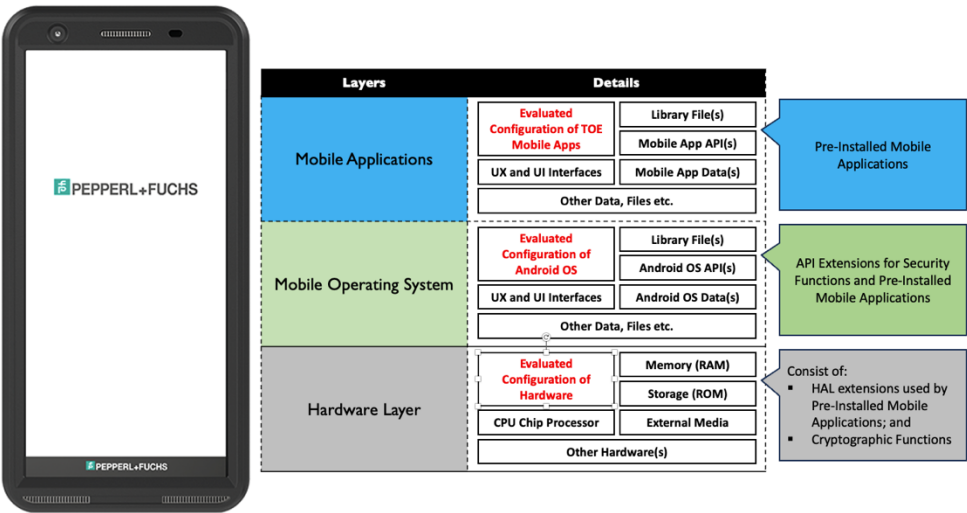


Figure 1: TOE Boundary

- 6 Figure 1 shows has highlighted in red font is the scope of the TOE. The TOE consists of two (2) main parts of operations, which are physical operations and logical operations. The description is provided in Section 1.4 in this document.

1.2 TOE Identification

7 The details of the TOE are identified in table below.

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C134
TOE Name	Smart-Ex
TOE Version	03
Security Target Title	Smart-Ex 03 Security Target
Security Target Version	v1.1
Security Target Date	2 February 2025
Assurance Level	Evaluation Assurance Level 2
Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL 2
Sponsor	Eurofins Product Service GMBH Storkower Str. 38c, 15526 Reichenwalde, Germany
Developer	Pepperl+Fuchs SE Lilienthalstraße 200 68307 Mannheim Germany
Evaluation Facility	Securelytics SEF A-19-06, Tower A ATRIA SOFO SUITES, Jalan SS 22/23, Damansara Utama, 47400 Petaling Jaya, Selangor, Malaysia

Table 2: TOE Identification

1.3 Security Policy

- 8 No Organisational Security Policy declared for the TOE.

1.4 TOE Architecture

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

1.4.1 Logical Boundaries

- **Security Audit**

Smart-Ex 03 smartphone as the TOE has the capability to collect, stored and maintained the security events audit log trails of the device components such as sensors, hardware and processor. inclusive of event logs generated by the configuration made on the Android OS, as well as hardware components within the TOE as a smartphone. In which, these components are important to ensure the TOE operates in a good condition, safely from any hazardous conditions and maintain its integrity from any internal or external damages.

- **Cryptographic Function**

Smart-Ex 03 smartphone has the capability of performing security functions related to cryptographic processes through the functionality of the Android OS as well as supported by the chip processes that enable several features such as secure boot and secure data protection storage.

- **User Data Protection**

Smart-Ex 03 smartphone as the TOE has the capability and capacity to protect the data stored inside the smartphone (as part of TOE secure operations) consist of audit log trails, collected data from sensors, data performance of hardware, configuration files of Android OS and configuration files of the hardware components.

- **Identification and Authentication**

Smart-Ex 03 smartphone has the capability to enforce access control based on identification and authentication by enabling security function such as: PIN code, Pattern, Password Based and Biometric fingerprint on the login screen, that enforce security capabilities in protecting the device lock screen security enabled by the TOE User.

- **Security Management**

Smart-Ex 03 smartphone as the TOE is being constructed with management functions that maintain the device conditions to ensure continues capability and capacity from the aspects of device integrity and data securely being protected in the mobile device through device monitoring that is accessible by both TOE User and TOE Developer (If being shared or allow access by TOE user).

The security management functions are performed and enforced by the TOE and TOE Mobile Apps (which are: eIS, eLOGKIT, eDIAGNOSTICS, eXTEND and ecomManagerService).

- **Physical Tampering and Fault Tolerance**

Smart-Ex 03 smartphone as the TOE equipped with smart battery sensors and intelligent thermal management systems, the TOE can effectively dissipate heat, prevent overheating and maintains optimal performance even in hot environments. Likewise, the TOE alerts the user on the high and low temperature (temperature acceptance (Ta) range accepted: $-20\text{ }^{\circ}\text{C} \leq \text{Ta} \leq +60\text{ }^{\circ}\text{C}$) through sensors located in the battery compartment as well as around the selected hardware chips in the smartphone. In which, this function mainly to ensure safe operation of Smart-Ex 03 in harsh environments it has been designed for. With such rugged design of the TOE, it includes reinforced frames, strengthened glass, and shock-absorbing materials, making the smartphone highly resistant to physical shocks, falls, or rough handling.

- **TOE Access**

Smart-Ex 03 smartphone protects the data from unauthorised access as well as prevent any means of accessing sensitive data inside the device without proper credentials. Protection has been applied through the secure configuration enforced by the Android OS supported by the chip processing.

1.4.2 Physical Boundaries

- 10 The TOE physical boundary is the physical perimeter of the device.
- 11 The TOE provides physical security of the smartphone by protecting it through complex design of the safety capabilities. It also features embedded hardware sensors inside the smartphone and its battery. These sensors can detect high temperatures.
- 12 The TOE are being operated using Android Operating System with all pre-installed (default) mobile applications known as TOE Mobile Apps (which are: eIS, eLOGKIT,

eDIAGNOSTICS, eXTEND and ecomManagerService) as well mobile applications as provided by the Android Open-Source Project (AOSP) and/or as part of GMS.

- 13 Mobile applications that are provided by Android Open-Source Project (AOSP) and/or as part of GMS are not in scope of the TOE. In which, that are being installed by TOE Developer to communicate with the smartphone hardware sensors for the purpose of monitoring, collecting device health data, to take defined actions such as generating audit trails and/or generates user-advice messages if determined thresholds are met.
- 14 The TOE also has a set of additional APIs provided to configure the devices. These are part of ecomManagerService. Some of these APIs impact the security of the device and are included as part of TOE Mobile Apps.
- 15 The TOE is also able to interact with and Enterprise Mobility Management (EMM) system (sometimes also referred to as Mobile Device Management (MDM) system) through Android Management API and Developer extensions following the Android OEM Configuration mechanism.
- 16 Android OEM Configuration refers to app framework that allows device manufacturers (OEMs) to configure, customize, and manage specific settings, features, or apps on their Android devices without requiring significant software modifications or updates. It enables OEMs to adapt Android to meet the specific needs of product developer.
- 17 All operations of the TOE are based on evaluated configuration of TOE Mobile Apps, evaluated configuration of Android OS and evaluated configuration of Hardware that are defined as scope of evaluation related to the operations of hardware, Android OS and pre-installed TOE mobile apps.
- 18 Data generated by these pre-installed TOE mobile apps will only be shared upon authorization of the TOE User of TOE Developer Services as Support, Diagnostics or Analytics.

1.5 Clarification of Scope

- 19 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.
- 20 Figure 1 and Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref[6]).
- 21 The excluded scope of evaluation is being stated below:

- User interface components which consist of capacitive touch display and hardware buttons
 - Mobile applications installed by TOE user and that are not pre-installed by TOE Developer.
 - Smartphone accessories including the protective case (Ex-protection) and peripherals.
- 22 Potential consumers of the TOE are advised that some functions and services of the overall product have not 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

Identifier	Assumption statement
A.TOE_USER	TOE User can access the files and folders of the TOE that been installed in the device, in which they can be trusted and shall not be hostile, are not careless (aware of the surrounding to prevent any social engineering attacks) and understood the importance of keeping information of data/files plus password in private (securely).
A.NOEVIL	TOE User that are responsible for configuring, installing and removing the TOE Mobile Apps, whilst managing the TOE Mobile Apps data and communication with the Developer Management System for updates or upgrades. It is assumed that this person, is not hostile and is competent. Note that, the Developer Management System is a system deployed by the TOE Developer to push updates on the underlying Android OS and push updates on the TOE Mobile Apps.
A.PASSWD	TOE User are recommended to enable complex password protected or biometric access protection on the smartphone lock screen.
A.CONFIG	It is assumed that the TOE's security functions are configured correctly in a manner to ensure that the TOE security policies will be enforced on all applicable based on the usage of the TOE device.

1.7 Evaluated Configuration

23 All operations of the TOE are based on evaluated configuration of TOE Mobile Apps, evaluated configuration of Android OS and evaluated configuration of hardware that are defined as scope of evaluation related to the operations of hardware, Android OS and pre-installed TOE mobile apps stated in the Security Target (Ref[6]).

- TOE Mobile Apps (Pre-installed Applications): These apps (eIS, eLOGKIT, eDIAGNOSTICS, eEXTEND, and ecomManagerService) are included within the scope of evaluation. They provide device monitoring and security logging. Refer to Section 1.5.2 of Security Target (Ref[6]) and for the logical scope and Section 6 of Security Target (Ref [6]) for the security functional requirement offered by the TOE Mobile Apps (Pre-Installed Applications). No third-party or user-installed apps are included in the evaluation.
- Android OS Configuration: The evaluated version of Android OS enforces access control, cryptographic security, audit logging and many more. Refer to Section 1.5.2 of Security Target (Ref[6]). for the logical scope and Section 6 of Security Target (Ref[6]). for the security functional requirement offered by the Android OS Configuration. The OS is pre-configured to work securely with the TOE Mobile Apps and hardware components.
- Hardware Configuration: The hardware (battery sensors, thermal monitoring, secure boot, reinforced casing) is included in the scope of evaluation. Refer to Section 1.5.2 of Security Target (Ref[6]). for the logical scope and Section 6 of Security Target (Ref[6]). for the security functional requirement offered by the Hardware Configuration. Features like secure boot, resistance to tampering, and smart sensors ensure physical and operational security.

2 Evaluation

- 24 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2. The evaluation was performed conformant to the MyCC Scheme Requirement (MyCC_REQ) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

- 26 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.
- 27 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Development

- 28 The evaluators analyzed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), and how the TOE security function (TSF) implements the security functional requirements (SFRs).
- 29 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behavior of the SFR-enforcing subsystems.

- 30 The evaluators examined the TOE security architecture description; they determined 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.
- 31 At the end, the evaluators confirmed that all the requirements for this class were fulfilled and passed.

2.1.3 Guidance documents

- 32 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.
- 33 The evaluators confirmed that the TOE guidance was fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

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

2.1.4.1 Assessment of Developer Tests

- 35 The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, 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). The results of the evaluators tests are consistent with the developers test results defined in their evaluation evidences submitted.

2.1.4.2 Functional Testing

- 36 At EAL2, provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance

documentation provided. It is intended that an EAL2 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

- 37 An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.

Test ID	Descriptions	Security Function	Results
F001- Identification and Authentication	1. To test that the TOE require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. 2. To test that the TOE require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. 3. To test that the TOE maintain the following list of security attributes belonging to individual users (login screen access credentials): · PIN code login screen · Pattern · Password Based · Biometric fingerprint login screen 4. To test that the TOE provide a mechanism to generate secrets that meet a defined quality metric configured by the TOE User. 5. To test that the TOE able to enforce the use of TSF generated secrets for encryption/decryption function, password management function, access control function,	FIA_UAU.2 FIA_UID.2 FIA_ATD.1 FIA_SOS.2	PASS

	biometric security function, access to configuration of hardware, access to configuration of OS, access to configuration of TOE Mobile Apps, PKI key management function.		
F002 – Identification and Authentication & TOE Access	1. To test that the TOE detect unsuccessful authentication attempts (value configured by TOE User) related to PIN code login screen, Pattern, Password Based, Biometric fingerprint login screen 2. To test that when the defined number of unsuccessful authentication attempts has been met, the TOE shall lockout and prevent to login on the screen with the timeout set by TOE User 3. To test that the TOE re-authenticate the user under the condition's session lockout of TOE Mobile Apps or exiting TOE Mobile Apps or exiting any configuration functions on the TOE. 4. To test that the TOE provide only obscured feedback to the device's display to the user while the authentication is in progress. 5. To test that before establishing a user session, the TOE shall display an advisory warning message regarding unauthorised use of the TOE.	FIA_AFL.1 FIA_UAU.6 FIA_UAU.7 FTA_TAB.1	PASS
F003 – Identification and Authentication	To test that the TOE prevent reuse of authentication data related to PIN	FIA_UAU.4	PASS

	code login screen and password based.		
F004 – TSF initiated session locking	1.To test that the TOE look an interactive session (time interval configured by TOE User) after: · clearing or overwriting display devices, making the current contents unreadable. · disabling any activity of the user’s data access/display devices other than unlocking the session 2. To test that the TOE require successful authentication on the lock screen with identified correct TOE User credential prior to unlocking the session. 3. To test that the TOE terminate an interactive session after a time interval configured by TOE User of inactivity.	FTA_SSL.1 FTA_SSL.3	PASS
F005–Security Management and User Data protection	1. To test that the TOE restrict the ability to disable or enable the functions in Table 12 and Table 13 to TOE User Security Target (Ref[6]). 2. To test that the TOE enforce the access control SFP(s) as stated in Table 12 and Table 13 Security Target (Ref[6]) to restrict the ability change_default, query, modify, delete, enable or disable the security attributes for TOE Mobile App to TOE User or TOE Developer.	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FDP_ACC.1 FDP_ACF.1 FDP_ITC.1 FMT_SMR.1	

	3. To test that the TOE enforce the access control SFP to provide permissive default values for security attributes that are used to enforce the SFP. 4. To test that the TOE allow the TOE User or TOE Developer to specify alternative initial values to override the default values when an object or information is created. 5. To test that the TOE capable of performing management functions such as all administrative actions related to the TOE Mobile Apps, configuration of security function of the OS and configuration of security functions of the hardware. 6. To test that the TOE enforce the access control SFP on list of subjects, objects, and operations components among subjects and objects covered by the SFP as stated in Table 12 Security Target (Ref[6]). 7. To test that the TOE enforce the access control SFP to objects based on the following: list of subjects and objects controlled under the indicated SFP as in Table 12 Security Target (Ref [6]). 8. To test that the TOE enforce the rules to determine if an operation among controlled subjects and controlled objects is allowed. The rules governing access among controlled subjects and controlled objects using controlled operations		
--	---	--	--

	on controlled objects as stated in Table 13 in Security Target (Ref[6]). 9. To test that the TOE explicitly authorise access of subjects to objects. 10. To test that the TOE explicitly deny access of subjects to objects 11. To test that the TOE enforce the access control SFP(s) based on Table 12 and Table 13 Security Target (Ref[6]) when importing user data, controlled under the SFP, from outside of the TOE. 12. To test that the TOE ignore any security attributes associated with the user data when imported from outside the TOE. 13. To test that the TOE maintain the roles TOE User and TOE Developer. 14. To test that the TOE able to associate users with roles.		
F006- Cryptographic Support (FCS)	1. To test that the TOE generate cryptographic keys in accordance with a specified cryptographic key generation algorithm; AES, SHA, ECDSA and specified cryptographic key sizes; AES (256-bit keys), SHA (256-bit keys), ECDSA (256-bit keys) that meets FIPS 140-2. 2. To test that the TOE destroy cryptographic keys in accordance with a specified cryptographic key destruction method; overwrite 3. To test that the TOE perform encrypt/decrypt in accordance with	FCS_CKM.1 FCS_CKM.4 FCS_COP.1	PASS

	a specified cryptographic algorithm; AES, SHA, ECDSA and specified cryptographic key sizes; AES (256-bit keys), SHA (256-bit keys), ECDSA (256-bit keys) that meets FIPS 140-2. 4. To test that the TOE perform hashing in accordance with a specified cryptographic algorithm; SHA and cryptographic key sizes; 256-bit, 384-bit, 512-bit that meets FIPS 180-4. 5. To test that the TOE perform generation and verification based on signing mechanism in accordance with a specified cryptographic algorithm; RSA and cryptographic key sizes 2048-bit or greater that meets FIPS PUB 186-4.		
F007-Passive detection of physical attack and Resistance to physical attack	1. To test that the TOE provide unambiguous detection of physical tampering that might compromise the TSF. 2.To test that the TOE provide the capability to determine whether physical tampering with the TSF's devices or TSF elements has occurred. 3.To test that the TOE resist protection casing being compromised or broken, hardware sensor to the physical protection casing, hardware consists of PCB motherboard, RAM, ROM and other hardware in the mobile device by	FPT_PHP.1 FPT_PHP.3	PASS

	responding automatically such that the SFRs are always enforced.		
F008 – TSF testing and Reliable time stamps	1. To test that the TOE run a suite of self-tests during initial startup to demonstrate the correct operation of the TSF. 2. To test that the TOE provide authorised users with the capability to verify the integrity of TSF data. 3. To test that the TOE provide authorised users with the capability to verify the integrity of TSF. 4. To test that the TOE able to provide reliable time stamps.	FPT_TST.1 FPT_STM.1	
F009 – Security Audit and User Data Protection	1.To test that the TOE able to generate an audit record of the following auditable events: · Start-up and shutdown of the audit functions · All auditable events for the minimum level of audit · All administrative actions, start-up and shutdown of the OS, insertion or removal of external media (e.g., SD card, SIM Card), enrolment/activation of eSIM, auditable events generated by TOE Mobile Apps and auditable events generated by the OS, Invocation of ECOMS SDK APIs as stated to Appendix A in Security Target (Ref[6]).	FAU_GEN.1 FAU_ARP.1 FAU_STG.1 FAU_STG.4 FAU_SAA.1 FDP_SDI.1 FDP_SDI.2	PASS

	2.To test that the TOE record within each audit report at least the following information: · Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event. · For each audit event type, based on the auditable event definition of the functional components included in Security Target (Ref[6]). 3.To test that the TOE take notification on the eIS and eXTEND that monitors the data from various thermal sensors upon detection of a potential security violation. 4. To test that the TOE able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs. 5.To test that TOE, enforce the following rules for monitoring audited events: · Accumulation or combination of subset of defined auditable events in Table 11 Security Target (Ref[6]) known to indicate a potential security violation. 6. To test that the TOE protect the stored audit records in the audit trail from unauthorized deletion.		
--	--	--	--

	7. To test that the TOE to detect unauthorized modifications to the stored audit records in the audit trail. 8. To test that the TOE overwrite the oldest stored audit records and circular log buffer size function if the audit trail is full. 9. To test that the TOE monitor user data stored in containers controlled by the TOE for integrity errors on all objects, based on the following attributes; TOE User data attributes related to the evaluated configuration of the TOE Mobile Apps, evaluated configuration of Android OS and evaluated configuration of hardware. 10. To test that the TOE monitor user data stored in containers controlled by the TSF for integrity errors on all objects, based on the following attributes: TOE user data attributes related to the security configuration, files, hardware, OS configuration and TOE Mobile apps configuration.		
--	---	--	--

Table 3: Functional Test

- 40 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

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

2.1.4.3 Vulnerability Analysis

- 42 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.
- 43 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack performed by an attacker possessing a Basic and Enhanced attack potential. The following factors have been taken into consideration during penetration tests:
- a) Time taken to identify and exploit (elapsed 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 equipment required for exploitation

2.1.4.4 Vulnerability testing

- 44 The penetration tests focused on:
- a) Improper Credential Usage
 - b) Inadequate Supply Chain Security
 - c) Insecure Authentication/Authorization
 - d) Insufficient Input/Output Validation
 - e) Insecure Communication
 - f) Inadequate Privacy Controls
 - g) Insufficient Binary Protections
 - h) Security Misconfiguration
 - i) Insecure Data Storage
 - j) Android Self-Test and Integrity Validation
 - k) Authentication Mechanism Bypass Test

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

2.1.4.5 Testing Results

- 46 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. Therefore, the certifiers confirmed that all the test conducted were PASSED as expected.

3 Result of the Evaluation

- 47 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 Smart-Ex 03 which is performed by Securelytics SEF.
- 48 Securelytics SEF found that Smart-Ex 03 upholds the claims made in the Security Target (Ref[6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2.
- 49 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

- 50 EAL 2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and interface specifications, guidance documentation and a description of the design of the TOE and the implementation to understand the security behaviours.
- 51 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.
- 52 EAL 2 also provides assurance through also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

- 53 The Malaysian Certification Body (MyCB) is strongly recommended (Opinions and interpretations expressed herein are outside the scope of certification) that:
- a) TOE users should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

- b) TOE users should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.
- c) TOE users and TOE developer 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.
- d) TOE users should review the audit trail generated by the TOE periodically.
- e) TOE developer should implement appropriate physical protection of the TOE to ensure access to the TOE internal parts are restricted and check the serial numbers of the tamper evident bags on delivery of the TOE.

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 5, April 2017.
- [3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
- [4] MyCC Scheme Requirement (MYCC_REQ), v1b, July 2023.
- [5] ISCB Evaluation Facility Manual (ISCB_EFM), v3, January 2023.
- [6] Smart-Ex 03 Security Target, v1.1, 2 February 2025.
- [7] Evaluation Technical Report- Smart-Ex 03 (T2303-4-ETR 1.0), 6 February 2024.

A.2 Terminology

A.2.1 Acronyms

Table 4: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body

Acronym	Expanded Term
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 5: 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-to-day 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 ---