Certificate Report

Version 1.0

17 April 2022

CSA_CC_21005

For

X-PHY AI Cyber Secure SSD, FAMP1.00

From

Flexxon Pte Ltd

This page is left blank intentionally

Foreword

Singapore is a Common Criteria Certificate Authorising Nation under the Common Criteria Recognition Arrangement (CCRA). The current list of signatory nations and approved certification schemes can be found at the CCRA portal:

https://www.commoncriteriaportal.org

The Singapore Common Criteria Scheme (SCCS) is established for the info-communications technology (ICT) industry to evaluate and certify their IT products against the requirements of the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 (ISO/IEC 15408) and Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 (ISO/IEC 18045) in Singapore.

The SCCS is owned and managed by the Certification Body (CB) under the ambit of Cyber Security Agency of Singapore (CSA).

The SCCS certification signifies that the target of evaluation (TOE) under evaluation has been assessed and found to provide the specified IT security assurance. However, certification does not guarantee absolute security and should always be read with the particular set of threats sought to be addressed and assumptions made in the process of evaluation.

This certification is not an endorsement of the product.

Amendment Record

Version	Date	Changes
1.0	17 April 2022	Release

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

Executive Summary

This report is intended to assist the end-user of the product in determining the suitability of the product in their deployed environment.

The Target of Evaluation (TOE) is the X-PHY AI Cyber Secure SSD, FAMP1.00 and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS).

The TOE comprises of the following components:

- Flexxon X-PHY Cyber Secure SSD FAMP 1.00
- X-PHY Quick Start Guide 24 March 2022
- X-PHY User Application Guide Windows 24 Nov 2021

The TOE is defined as a solid-state drive (SSD) that protects its SSD data flow against all known ransomware and data cloning attacks. The TOE analyses various attributes in the data access pattern to detect known ransomwares and malicious data cloning behaviour. Upon detection of such malicious behaviour, the TOE shall lock its SSD from further read/write access.

The evaluation of the TOE has been carried out by AN Security, an approved CC test laboratory at the assurance level CC EAL2 augmented by ALC_FLR.2 and completed on 4 April 2022. The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed Issue
Identification and authentication	The TOE performs identification and authentication of the administrator prior to allowing access to the TOE's security management functionality. The TOE authenticates the administrator using 2-Factor Authentication (2FA). The TOE performs 2FA using administrator's password and One-Time-Password (OTP). On an administrator's desktop/laptop, a client application is run for the administrator to interact with the TOE's identification and authentication functionality. On a mobile phone, a mobile application is run for the same purpose i.e. for the administrator to interact with the TOE's identification and authentication functionality.
Security management	The TOE provides security management functionality to manage the following security function behaviour: • Identification and authentication o Manage identification and authentication data o Management subject security attributes • TSF protection o Management of users that gets informed about physical

	tamper ○ Management of SSD lock or unlock status ○ Enable or disable purge response to physical tamper.
User data protection	The TOE performs SSD data protection in two prongs during normal operation: • The TOE encrypts and decrypts user data stored in the SSD on-the-fly; SSD data confidentiality is protected at rest. • The TOE analyses various attributes of user PC's read/write access to the TOE's SSD. Based on the behaviour of these attributes, the TOE determines whether the user PC's read/write access behaviour is associated with that of a known ransomware or data cloning attack. Once the TOE determines that the read/write access behaviour is associated with that of a ransomware or data cloning attack, the TOE locks user PC's access to the SSD.
Trusted path	The administrator performs TOE security management via the administrator's mobile phone. The TOE connects to the administrator's mobile phone via Bluetooth. To protect the confidentiality and integrity of administrator's identification/authentication data and other TOE Security Functionality (TSF) data being exchanged between the mobile phone and the TOE, the TOE establishes a trusted path between the TOE and the administrator.
TSF protection	The TOE provides TSF protection in the following areas: • Physically, the TOE provides physical tamper detection/response by measuring physical properties of SSD disconnection and temperature. • Logically, TOE ○ performs firmware integrity check using digital signature during initialisation and firmware update; this ensures the TSF integrity and authenticity is preserved in both scenarios. ○ performs cryptographic Known-Answer-Test (KAT) during initialisation and operations to ensure the correctness of the cryptographic implementation.

	○ encrypts inter-chip communication to protect confidentiality of TSF data.

Table 1: TOE Security Functionalities

Please refer to the Security Target [1] for more information.

The assets to be protected by the TOE has been defined. Based on these assets, the TOE Security Problem Definition has been defined in terms of Assumptions, Threats and Organisation Policies. These are outlined in Chapter 4 of the Security Target.

This Certification covers the configurations of the TOE as outlined in Chapter 5.3 of this report.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate applies only to the specific version and release of the IT product in its evaluated configuration. This certificate is not an endorsement of the IT product by SCCS, and no warranty of the IT product by SCCS, is either expressed or implied.

Table of Contents

1 Certification

1.1 Procedure

The certification body conducts the certification procedure according to the following criteria:

- Common Criteria for IT Security Evaluation (CC) Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, ISO/IEC 15408
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 5, ISO/IEC 18045
- SCCS scheme publications

1.2 Recognition Agreements

The international arrangement on the mutual recognition of certificates based on the Common Criteria Recognition Arrangement had been ratified on 2 July 2014. The arrangement covers certificates with claims of compliance against collaborative protection profiles (cPPs) or evaluation assurance levels (EALs) 1 through 2 and ALC_FLR.

Singapore is authorised to issue CC certificates recognised widely through the Common Criteria Recognition Arrangement (CCRA) by the member nations. Hence, the certification for this TOE is fully covered by the CCRA.

The Common Criteria Recognition Arrangement Logo printed on this certificate indicates that this certification is recognised under the terms of this agreement by all signatory nations listed on the CC web portal (http://www.commoncriteriaportal.org).

2 Validity of the Certification Result

This Certification Report only applies to the version of the TOE as indicated. The Certificate is valid till 1**6 April 2027**[1].

In cases of changes to the certified version of the TOE, the validity may be extended to new versions and releases provided the TOE sponsor applies for Assurance Continuity (i.e. re-certification or maintenance) of the revised TOE, in accordance with the requirements of the SCCS.

The owner of the Certificate is obliged:

- When advertising the Certificate or the fact of the product's certification, to refer to and provide the Certification Report, the Security Target and user guidance documentation herein to any customer of the product for the application and usage of the certified product;
- To inform the SCCS immediately about vulnerabilities of the product that have been identified by the developer or any third party; and
- To inform the SCCS immediately in the case that relevant security changes in the evaluated life cycle has occurred or the confidentiality of documentation and information related to the TOE or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is no longer valid.

[1] Certificate validity could be extended by means of assurance continuity. Certificate could also be revoked under the conditions specified in SCCS Publication 3 [3]. Potential users should check the SCCS website (https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/csa-common-criteria/product-list) for the up-to-date status regarding the certificate's validity.

3 Identification

The Target of Evaluation (TOE) is the **X-PHY AI Cyber Secure SSD**. The following table identifies the TOE deliverables, which includes the guide for receipt and acceptance [2] [3] [4] [5] of the TOE.

Type	Name	Version	Form of Delivery
HW	X-PHY AI Cyber Secure SSD	FAMP 1.00	Courier
PDF	X-PHY Quick Start Guide 24 Mar 22	N.A	Download from website
	X-PHY User application Guide Windows 24 Nov 21		
	X-PHY Bluetooth Application Guide Apple 24 Sep 21		
	X-PHY Bluetooth Application Guide Android 24 Sep 21		

Table 2: Deliverables of the TOE

Additional identification information relevant to this Certification procedure as follows:

TOE	X-PHY AI Cyber Secure SSD FAMP1.00
Security Target	Flexxon X-PHY AI Cyber Secure SSD Security Target v1.2
CC Scheme	Singapore Common Criteria Scheme (SCCS)
Methodology	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5
Assurance Level/cPP	EAL 2 augmented with ALC_FLR.2
Developer	Flexxon Pte Ltd
Sponsor	Flexxon Pte Ltd
Evaluation Facility	An Security Pte Ltd
Certification Body	Cyber Security Agency of Singapore (CSA)
Certification ID	CSA_CC_21005
Certificate Validity	**17 April 2022** till **16 April 2027**

Table 3: Additional Identification Information

4 Security Policy

The TOE's Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE.

The TOE implements policies pertaining to the following security functional classes:

- Identification and authentication
- Security management

- User data protection
- Trusted path
- TSF protection

Specific details concerning the above-mentioned security policies can be found in chapter 6 of the Security Target [1].

5 Assumptions and Scope of Evaluation

5.1 Assumptions

The assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE environment and are listed in the tables below:

Security Objectives	Description

OE.Trusted_User	The operational environment must ensure that
	• TOE users are well-trained to
	  ○ operate the TOE securely in accordance with the operational guidance
	  ○ setup the IT environment in accordance with the preparative guidance.
	• TOE users are trusted i.e. does not harbour malicious intent.

OE.PasswordPolicy	The client application shall enforce password complexity policy for its user identification and authentication.
OE.User_mobile	The TOE user must ensure that the user mobile is secure and trusted.

Table 4: Objectives for the Operational Environment

Details can be found in 4.2 of the Security Target [1].

5.2 Clarification of Scope

The scope of evaluation is limited to those claims made in the Security Target [1].

5.3 Evaluated Configuration

The TOE is a solid-state drive (SSD) that protects its SSD data against ransomware and data cloning attacks; it is capable of detecting ransomwares and cloning wares of known behaviour.

The TOE analyses various attributes of ransomware and malicious data cloning behaviour. This allows the TOE to detect ransomwares and cloning wares with known behaviour. Upon detection of such malicious behaviour, the TOE shall lock its SSD from further read/write access.

The following illustrates the TOE usage.

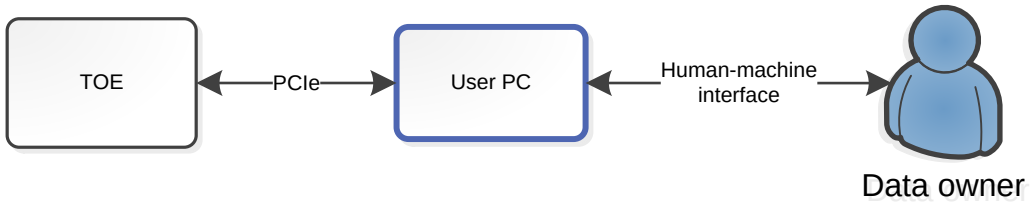

Figure 1: TOE usage during normal operation

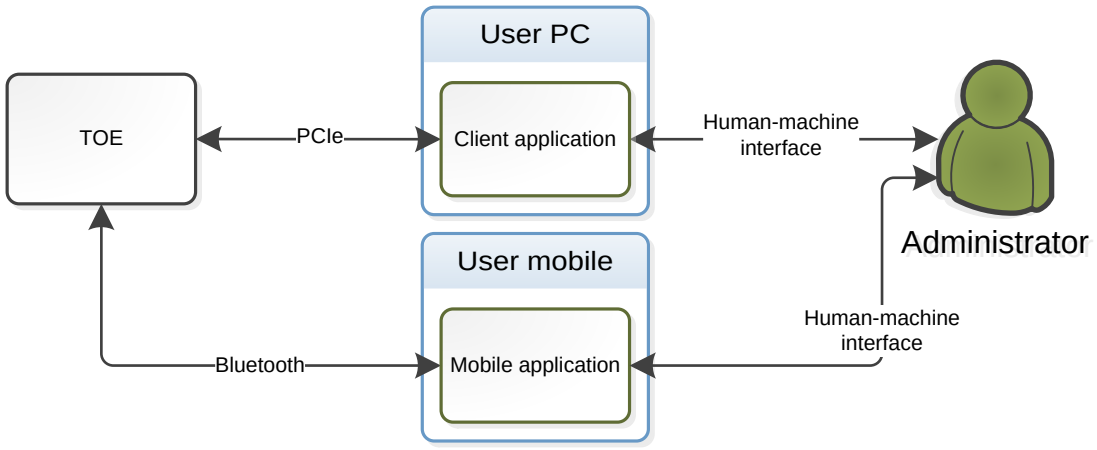

Figure 2: TOE usage during security management

The TOE also provides physical tamper detection/response by measuring physical properties of SSD disconnection. If the TOE detects any anomalies in those physical properties, the TOE shall either lock its SSD from further read/write access or purge its SSD data.

5.4 Non-Evaluated Functionalities

There are no non-evaluated functionalities within the scope as clarified in section 5.2

5.5 Non-TOE Components

The TOE requires additional components (i.e. hardware/software/firmware) for its operation. These non-TOE components include:

- Windows 10/8 Laptop/Desktop PC with PCIe M Key, PCIe version Gen 3 host interface
- Android/iOS Mobile Phone with Bluetooth version 5.0 host interface
- Google/Microsoft Authenticator application

More information is available in 1.3.3 of the Security Target [1].

6 Architecture Design Information

The major components of the TOE are the SSD controller, X-Trust controller, Authentication IC, Bluetooth Low Energy (BLE) module, Temperature sensor, Tamper pads, DDR and SSD.

The SSD controller performs self-test during TOE initialisation, manages all administrator and user commands, performs encryption and decryption of user data stored on the SSD, performs detection of ransomware and cloning activities data flow. The SSD controller will lock access to the flash memory upon detection of ransomware or cloning activities.

The X-Trust controller manages secure communication sessions between TOE and external applications, performs user identification and authentication, executes security management actions when physical tamper detection events occurs.

The Authentication IC validates authenticity of TOE with external applications.

The BLE module supports trusted communication between TOE and external mobile application via Bluetooth.

The tamper pads supports physical tamper detection of the TOE and notifies the X-Trust controller when any tamper event has been detected.

The DDR maps the SSD physical to logical locations to manage user data stored in the SSD. It also acts as a temporary buffer as user data is being read or written.

The SSD stores the user data.

7 Documentation

The evaluated documentation as listed in Table *2*: Deliverables of the TOE is being provided with the product to the customer. These documentations contain the required information for secure usage of the TOE in accordance with the ST.

8 IT Product Testing

8.1 Developer Testing (ATE_FUN)

8.1.1 Test Approach and Depth

The developer's tests cover all operational functions as described in the ST.

8.1.2 Test Configuration

The developer performed testing on the following TSFs: Identification & Authentication, Information Flow Control, TSF Protection, Security Management, Trusted Path. The TOE used for testing is configured according to the TOE guidance documents.

8.1.3 Test Results

All test results from all tested environment showed that the expected test results are identical to the actual test results.

8.2 Evaluator Testing (ATE_IND)

8.2.1 Test Approach and Depth

The evaluator confirms that the TSFIs have been sufficiently covered by the developer's tests. The CCTL was able to fully repeat the developer's tests that are deemed to be TSF relevant.

To gain more assurance in the correctness of the cryptographic operations, the evaluator augmented a test subset to verify the correctness of a cryptographic operation performed by the SSD Controller subsystem as part of independent testing to gain assurance of the security of the TOE.

8.2.2 Test Configuration

There is only one configuration stated in the preparative guidance and the TOE used for testing is configured according to the TOE guidance documents.

8.2.3 Test Results

The developer's test reproduced were verified by the evaluator to conform to the expected results from the test plan, the actual version of the TOE provides security functionalities that are correctly implemented as specified by the developer.

8.3 Penetration Testing (AVA_VAN)

8.3.1 Test Approach and Depth

The approach chosen by the evaluator is commensurate with the assurance component chosen (AVA_VAN) treating the resistance of the TOE to an attack with the Basic attack potential. i.e. amongst other that the evaluator used sources of information publicly available to identify potential vulnerabilities in the TOE. The evaluator analysed which potential vulnerabilities are not applicable to the TOE in its operational environment

For the potential vulnerabilities being applicable to the TOE in its operational environment and, hence, which were candidates for testing applicable to the TOE in its operational environment, the evaluator devised the attack scenarios where these potential vulnerabilities could be exploited. For each such attack scenario he firstly performed a theoretical analysis on the related attack potential. Where the attack potential was Basic or near to Basic, the evaluator conducted penetration tests for such attack scenarios. He analysed then the results of these tests with the aim to determine, whether at least one of the attack scenarios with the attack potential Basic was successful.

The approach chosen by the evaluator is appropriate for the assurance component chosen (AVA_VAN.2), treating the resistance of the TOE to an attack with **Basic** potential.

All findings were rectified. No residual risks were identified.

9 Results of the Evaluation

The Evaluation Technical Report (ETR) was provided by the CCTL in accordance with the CC, CEM, requirements of the SCCS. As a result of the evaluation, the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 2 + ALC_FLR.2 assurance package

10 Obligations & Recommendations for Usage of the TOE

- The documents as outlined in Table 3 - Guidance Document contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition, all aspects of Assumptions, Threats and OSPs as outlined in the Security Target [1] that are not covered by the TOE shall be fulfilled by the operational environment of the TOE.
- Potential users shall note that the detection of known ransomware and data cloning attacks do not happen instantaneously. Users may lose up to 20% of the files stored in the SSD.
- Potential user of the product shall consider the results of the certification within his/her system risk management process. As attack methods and techniques evolve over time, he/she should define the period of time whereby a re-assessment of the TOE is required and convey such request to the sponsor of the certificate.
- No additional recommendation was provided by the evaluators.

11 Acronyms

CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CCTL	Common Criteria Test Laboratory
CSA	Cyber Security Agency of Singapore
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirement
SCCS	Singapore Common Criteria Scheme
SFR	Security Functional Requirement
TOE	Target of Evaluation
TSF	TOE Security Functionality

12 References

[1] Flexxon Pte Ltd, “Flexxon X-PHY AI Cyber Secure SSD Security Target v1.2,” 2022.

[2] Flexxon Pte Ltd, “X-PHY Quick Start Guide 24 March 2022”.

[3] Flexxon Pte Ltd, “X-PHY User Application Guide Windows 24 Nov 2021”.

[4] Flexxon Pte Ltd, “X-PHY Bluetooth Application Guide Apple 24 Sept 2021”.

[5] Flexxon Pte Ltd, “X-PHY Bluetooth Application Guide Android 24 Sept 2021”.

[6] Cyber Security Agency of Singapore (CSA), “SCCS Publication 1 - Overview of SCCS, Version 5.0,” 2018.

[7] Cyber Security Agency of Singapore (CSA), “SCCS Publication 2 - Requirements for CCTL, Version 5.0,” 2018.

[8] Cyber Security Agency of Singapore (CSA), “SCCS Publication 3 - Evaluation and Certification, Version 5.0,” 2018.