MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

C130 Certification Report

PQTunnel v1.1.5

File name: ISCB-5-RPT-C130-CR-v1a
Version: v1a
Date of document: 21 October 2024
Document classification : PUBLIC

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

C130 Certification Report

PQTunnel v1.1.5

21 October 2024

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:	C130 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C130-CR-v1a
ISSUE:	v1a
DATE:	21 October 2024
DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 201601006881 (726630-U)

Printed in Malaysia

Foreword

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

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

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

This certification report is associated with the certificate of product evaluation dated 13 Mar 2024, 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/index.php/certification/product-certification/mycc/certified-products-and-systems-5.

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate 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	15 February 2024	All	Initial draft
v1	1 March 2024	All	Final version
v1a	21 October 2024	Page iv, vii, 4, 6,7,15 & 16	Update regarding the broken link on the website

Executive Summary

The Target of Evaluation (TOE) is PQTunnel v1.1.5 which is software application and a next-generation, Client-to-Client Virtual Private Network (VPN). The TOE provide connections based on Post-Quantum Cryptography (PQC) with Zero Trust Architecture to provide an E2EE secure tunnelling channels from the user's device to respective backend resources that are resistant to quantum attacks.

The TOE provides protection of data in transit across a shared or public network. The TOE employs quantum-resistant cryptographic algorithms that are recognised by National Institute of Standards and Technology (NIST).

The TOE provides security functions such as Identification and authentication, cryptographic support, security management, trusted path/channels, security audit and TOE access.

The scope of the evaluation is defined by the Security Target (Ref [6]) which identifies 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. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 1(EAL1). 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 Digiforen (M) Sdn Bhd and the evaluation was completed on 14 February 2024.

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 https://iscb.cybersecurity.my/index.php/certification/product-certification/mycc/certified-products-and-systems-5. It is the responsibility of the user to

ensure that PQTunnel v1.1.5 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

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE) is PQ Tunnel v1.1.5. This software application represent a next-generation Virtual Private Network (VPN) provides end-to-end secure tunnelling channels that are resistant to quantum attacks from the user's device to respective backend resources.

2 The TOE provides protection of data in transit across shared or public network.

3 Compared to traditional VPNs, the TOE utilizes National Institute of Standards and Technology (NIST) PQC-KEM (Post Quantum Cryptographic Key Encapsulation Mechanism) to assist in establishing a shared secret between two endpoints. This approach effectively protects against quantum computer attacks.

4 Moreover, the TOE prevent security incidents such as lateral movement through zero trust architecture and provide virtual IPs for each backend resources. The TOE can also limit the exposure in case of security exploitations due to the micro-segmentation of the backend resources and multi-layered identity authentication.

5 The key features of the TOE are listed as below:

- Support quantum-resistant secure channels for users to communicate remotely with their targeted endpoints;
- Support various deployment environment such as on-premises or on cloud;
- Provide direct, end-to-end connections between user devices and backend resources;
- Micro-segmentation of backend resources which reduces the impacted range by cyber-attacks such as malwares and ransomwares; and
- Two-Factor Authentication (2FA) which provide additional layer of security to access.

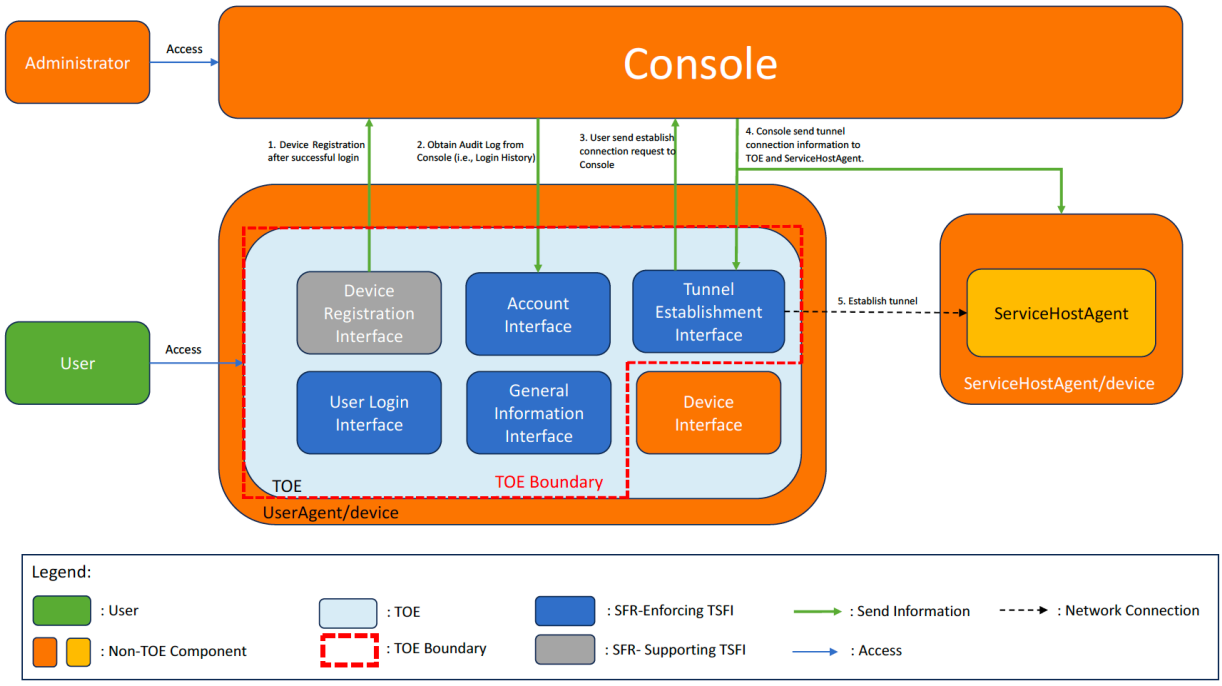

Figure 1: TOE Boundary

6 Figure 1 shows the implementation diagram of how the TOE is accessed and utilised to perform tunnel establishment. The TOE is installed on the user device (i.e., platform or UserAgent/device) such as desktop, laptop and so on. Next, the Console is accessible through a browser and is located on the cloud, it's used to manage the access control policy of the TOE. However, only the administrator has access to the Console and this evaluation do not include the Console into the scope. Lastly, the ServiceHostAgent (i.e., endpoint or host) is installed on backend resources (i.e., ServiceHostAgent/device) such as computer, server, databases, etc. to verify and accept connection establishment from the TOE.

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	C130
TOE Name	PQTunnel
TOE Version	v1.1.5
Security Target Title	Chelpis PQTunnel v1.1.5 Security Target
Security Target Version	v1.9
Security Target Date	29 January 2024
Assurance Level	Evaluation Assurance Level 1
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 1
Sponsor	Digiforen Technology Co. Ltd. 4th Floor, NSTC Cyber Security & Smart Technology R&D Building No. 6, Section 1, Gueiren 13th Road, Gueiren District, Tainan City 711, Taiwan.
Developer	Chelpis Quantum Tech Co. Ltd. 4F., No. 200, Sec. 2, Jinshan S. Rd., Da'an Dist., Taipei City 106, Taiwan (R.O.C).
Evaluation Facility	Digiforen (M) Sdn Bhd 1-4B, Incubator 3,

	Technology Park Malaysia, Lebuhraya Puchong-Sungai Besi, Bukit Jalil, 57000 Kuala Lumpur, Wilayah Persekutuan, Malaysia.

Table 1: TOE Identification

1.3 Security Policy

8 No Organisational Security Policy (OSP) declared for the TOE.

1.4 TOE Architecture

9 The TOE consist of logical and physical boundaries which are described in Section 1.7 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

10 The logical boundary of the TOE is summarized below:

- **Identification and authentication**
  The TOE users are required to provide their Account, Password and Domain before able to gain access to the TOE and initiate secure connections to backend resources. The TOE also require the user to utilise credentials with certain level of quality, and the login attempts are limited to 20 tries within 10 minutes.
- **Cryptographic support**
  The TOE provide the full lifecycle of cryptographic key generation, key destruction, and key operation for different operations for establishing and maintaining secure tunnel channels.
- **Trusted path/channels**
  The TOE provide secure path and channels for data in-transit during communications between local user and the TOE, and between the TOE and other trusted IT entities. This security is to prevent unauthorised disclosures and modifications for the data in-transit.

- **Security management**

  The TOE provide security management capability for the TOE user to reset their password, setup and reset the Two-Factor Authentication of the TOE through the Account Interface.

- **Security audit**

  The TOE allows the TOE user to view their login history including the device used by the TOE user, location, the date, and time of last accessed and the operations of the TOE user on the TOE and shown through the Account Interface. This information is obtained from the Console.

- **TOE access**

  The TOE allow the user to terminate their own interactive session. This is performed by the user's own action through pressing the "logout" button through the General Information Interface or Account Interface, or by pressing the "terminate" button through the Account Interface, under the "Operations" column.

1.4.2 Physical Boundaries

11 The TOE is a next-generation Virtual Private Network (VPN), a software application which provides end-to-end secure tunnelling channels that are resistant to quantum attacks from the user's device to respective backend resources.

12 The non-TOE comprise of the following:

- **Transport Layer Security.** Cryptography of the communication channel between users to the TOE; and from TOE to backend resources with TLS version 1.2 and 1.3, which is provided by:
  - https://pkg.go.dev/crypto/tls (go1.20.5)
  - https://boringssl.googlesource.com/boringssl

- **Secret Code Authentication Scheme**. Two-Factor Authentication that provides secret code by external authentication schemes, which includes:
  - Time-Based One Time Password (TOTP) from preferred authenticator application.
  - EZAuth which is an authenticator application developed by Chelpis that provides additional authentication method through a separate user device.

NOTE: The evaluation of the 2FA TOE component is performed on G2FA for TOTP and EZAuth Authenticator for EZAuth.

- **ServiceHostAgent.** Also known as Endpoint or Host, which are endpoints that the user wants to communicate with remotely. The agent is installed on ServiceHostAgent/device to be activated and allow tunnel establishment to occur.
- **ServiceHostAgent/device.** This represents the underlying platform (e.g., computer, server, databases, etc.) of the Endpoint or Host. After an administrator authenticates with the Console using a ServiceHostAgent, the computer is registered to the device list of that service server.
- **Console.** The console is a software for VPN management which provides management functions such as access control policy, audit logs, host managements, and so on. Console is managed by administrator.
- **Platform (i.e., UserAgent/device) for the TOE.** It represents any system (e.g., computer) the user logs into. After a user authenticates with the Console through the TOE on any computer, the computer is registered to the user's device list. The underlying platform for the TOE is as below:
  - Windows 10 (21H1) and above (x64/ arm64); or
  - MacOS Big Sur 11 and above (x64/ arm64).

  NOTE: The evaluation of the TOE component is performed on MacOS version 14.1.1, arm64.
- **Device Interface.** The device interface contains information related to the User's device, such as operating system and the virtual IP. This interface also outlines the TOE version, user device's public key and local event logs, which are not included in this evaluation.

1.5 Clarification of Scope

13 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

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

15 Potential consumers of the TOE are advised that some functions and services of the overall product have not been evaluated as part of this evaluation. Potential consumers

of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

16 This section is not applicable for EAL1.

1.7 Evaluated Configuration

17 This section describes the evaluated configurations of the TOE that are included within the scope of the evaluation.

18 As stated in Security Target (Ref [6]) the TOE is a software application and next-generation, Client-to-Client Virtual Private Network (VPN).

19 The secure acceptance procedure for the evaluated configuration of the TOE is described in document “Chelpis PQTunnel v1.1.5 Preparative Guidance, v1.9”.

20 The TOE is installed in MacOS version 14.1.1, arm64 with screen lock mechanism enabled and the timestamp using Apple time server that is time.apple.com.

21 Upon downloading the application, the user can check that the downloaded TOE is not modified by unauthorised parties by performing file checksum. The updated installer file checksum is “f6040e54” for MacOS.

22 The TOE is installed on devices that are accessible only to authorised personnel; and the endpoints in secure area accessible only to authorised personnel.

23 The TOE is installed and operated by the evaluation and uses the software within compliance of the guidance.

24 The TOE is delivered as a software application by the developer in its known state.

25 Before the user are allowed the functions of the TOE, they required to perform necessary configurations which are:

a) Whitelisting the domain used for the user by admin;
b) Setting up accounts to be used for the user by admin; and
c) Setting up services and policies for the user by admin

1.8 Delivery Procedures

26 This section in not applicable for EAL1.

2 Evaluation

27 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 1. 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

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

2.1.1 Life-cycle support

29 The evaluator found that the TOE provided for evaluation is labelled with its reference.

30 The evaluator check that the TOE references used are consistent.

31 The evaluator examine the configuration list to determine that it uniquely identifies each configuration item.

32 At the end, the evaluator confirmed that all the requirements for this class were fulfilled and passed.

2.1.2 Development

33 The functional specification shall describe the purpose and method of use for use for each SFR-enforcing and SFR-supporting TSFI.

34 The evaluator examined the presentation of the TSFI to determine that it identifies all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

35 The evaluator examined the rationale provided by the developer for the implicit categorization of interfaces as SFR non-interfering to determine that it is accurate.

36 The evaluator shall examine the functional specification to determine that it is a complete instantiation of the SFRs.

37 At the end, the evaluator confirmed that all the requirements for this class were fulfilled and passed.

2.1.3 Guidance documents

38 The evaluator 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.

39 The evaluator examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

40 The evaluator confirmed that the TOE guidance was fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

41 Testing at EAL 1 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by Digiforen (M) Sdn Bhd. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report (TPR).

2.1.4.1 Assessment of Developer Tests

42 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

43 At EAL 1, 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 EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

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

Test Title	Test Title	Description	Security Function	TSFI	Results
TEST GROUP A – Identification and Authentication					
1.	A1. Account Field	To test whether user able to perform identification and authentication functions to the TOE.	FIA_ATD.1, FIA_UID.2, FIA_UAU.2, FAU_SAR.1	1. User Login Interface 2. Account Interface	Passed
2.	A2. Password Field				
3.	A3. Domain Field				
4.	A4. Reset Password Less Than 12 Characters and Maximum 32 Characters	To test whether the TOE allows the user to reset password less than 12 characters and maximum 32 characters.	FIA_SOS.1		Passed
5.	A5. Authentication Attempts	To test whether the TOE locked the user after more than 20 times attempts within 10 minutes.	FIA_AFL.1		Passed
TEST GROUP B-Trusted Path/Channels					
6.	B1. Communication Protocol between the User to TOE to Backend	To test whether the communication protocol between the user to TOE and TOE to			Passed

Test Title	Test Title	Description	Security Function	TSFI	Results
		backend is using TLS version 1.2 and 1.3.	FTP_TRP.1, FTP_ITC.1	Tunnel Establishment Interface	
7.	B2. Trusted Path Establishment	To test whether trusted path establishment are using TLS version 1.2 and 1.3.			Passed
TEST GROUP C- Security Management					
8.	C1. Reset Password	To test whether the user able to perform management functions which is reset password.	FMT_SMR.1, FMT_SMF.1	Account Interface	Passed
9.	C2. Enable 2FA for TOTP	To test whether the user able to perform management functions which is enable 2FA for TOTP.			Passed
10.	C3. Enable 2FA for EZAuth	To test whether the user able to perform management functions which is enable 2FA for EZAuth.			Passed
11.	C4. Reset 2FA	To test whether the user able to perform management functions which is reset 2FA.			Passed
TEST GROUP D – Security Audit					
12.	D1. Audit Review	To test whether the user able to read audit log.	FAU_SAR.1	Account Interface	Passed

Test Title	Test Title	Description	Security Function	TSFI	Results
TEST GROUP E- TOE Access					
13.	E1. Logout Session from General Information Interface	To test whether the user able to terminate their interactive session by logout session from General Information Interface	FTA_SSL.4	1. Account Interface 2. General Information Interface	Passed
14.	E2. Terminate Session from Account Interface	To test whether the user able to terminate their interactive session by terminate session from Account Interface			Passed
15.	E3. End Session from Account Interface	To test whether the user able to terminate their interactive session by end session from Account Interface			Passed
TEST GROUP F- Cryptographic Support					
16	F1. UUID Validation	To test whether the UUID generated is version 4	FCS_CKM.1(5)	N/A	Passed
17	F2. Cryptographic Key Generation (Authentication) and Cryptographic Operation (Authentication)	To test whether cryptographic key generation (authentication) is using Curve P-256 and ECC key Pair Generation with 32 bytes key size and cryptographic operation (Authentication)	FCS_CKM.1(1)		Passed

Test Title	Test Title	Description	Security Function	TSFI	Results
		is using Curve P-256 and ECDSA with 32 bytes key size.			
18	F3. Key Destruction (Backend)	To test whether key destructed after the operation.	FCS_COP.1(1)		Passed
19	F4. Key Destruction (TOE)				Passed
TEST GROUP G-Cryptographic Support					
20.	G1. AES Keys Generation (BLAKE2s)	To test whether cryptographic key generation (AES keys generation) is using BLAKE2s and HKDF with 32 bytes key size	FCS_CKM.1(4)		Passed
21.	G2. AES Keys Generation (HKDF)				Passed
22.	G3. AEAD Operation	To test whether cryptographic key operation is using AEAD with 32 bytes key size	FCS_COP.1(4)	N/A	Passed
23.	G4. Key Destruction	To test whether key destructed after the operation.	FCS_CKM.4		Passed
TEST GROUP H-Cryptographic Support					
24.	H1. Cryptographic Key Generation (PQC Shared Secret) and Cryptographic Operation (PQC-KEM)	To test whether the cryptographic key generation (PQC Shared Secret) is using CRYSTALS-Kyber 768 Pair Generation with 2,400 bytes of key size and cryptographic operation	FCS_CKM.1(2) FCS_COP.1(2)	N/A	Passed

Test Title	Test Title	Description	Security Function	TSFI	Results
		(PQC_KEM) is using Kyber-768 with 32 bytes key size.			
25.	H2. Key Destruction	To test whether key destructed after the operation.	FCS_CKM.4		Passed
TEST GROUP I- Cryptographic Support					
26.	I1. Cryptographic Key Generation (Shared Secret)	To test whether the cryptographic key generation (Shared Secret) is using Curve25519 Pair Generation with 32 bytes of key size	FCS_CKM.1(3) FCS_COP.1(3)	N/A	Passed
27.	I2. Cryptographic Operation (Diffie- Hellman)	To test whether the cryptographic operation (Diffie-Hellman) is using X25519 with 32 bytes key size.			Passed
28.	I3. Key Destruction	To test whether key destructed after the operation.	FCS_CKM.4	N/A	Passed

Table 2: Functional Test

45 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.

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

2.1.4.3 Vulnerability Analysis

47 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.

48 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

49 The penetration tests focused on:

a) SQL Injection (SQLi)

b) ARP Spoofing

c) Sniffing

50 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

51 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

52 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 PQTunnel v1.1.5 which is performed by Digiforen (M) Sdn Bhd.

53 Digiforen (M) Sdn Bhd found that PQTunnel v1.1.5 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 1.

54 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

55 EAL 1 provides a basic level of assurance by a limited security target and analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behaviour.

56 The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TSF.

57 EAL 1 also provides assurance through unique identification of the TOE and the relevant evaluation documents.

58 This EAL provides a meaningful increase in assurance over unevaluated IT.

3.2 Recommendation

59 The Malaysian Certification Body (MyCB) is strongly recommended that:

a) Opinions and interpretations expressed herein are outside the scope of accreditation.

b) It is recommended that all guidance outlined in Preparative Guidance and Operational Guidance be followed to configure the TOE in the evaluated configuration.

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] Chelpis PQTunnel v1.1.5 Security Target, v1.9, 29th January 2024.

[7] Digiforen (M) Sdn Bhd MP-230728-82 Evaluation Technical Report, v1.1,14th February 2024.

A.2 Terminology

A.2.1 Acronyms

Table 3: 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 4: Glossary of Terms

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

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

--- END OF DOCUMENT ---