EUCC Certification Report

CERTIFICATION REPORT INFORMATION	
Certification Report Reference	**FCS506_05 EUCC Quantum_PHIOTX Certification Report_1.0**
Project (TOE) Identification	TOE Name: PhioTX-V TOE version: 4.5.6 Common Criteria for Information Technology Security Evaluation, Parts: 1 - 5, CC:2022, Revision 1. Common Criteria for Information Technology Security Evaluation. Evaluation Methodology, CEM:2022, Revision 1. EAL 2
Evaluation Technical Report (ETR) Reference	PHIOTX-ETR PHIOTX ETR Report, Version 1.2, 02/10/2026
CB identification	DEKRA Testing and Certification S.A.U. EUCC CB Body Number at ENISA: CB 3095
Author	Dariusz Rogowski
Date	06/11/2026
EUCC APPLICANT INFORMATION	
Applicant identification	Quantum Xchange, Inc.
Manufacturer	Quantum Xchange, Inc.
ITSEF INFORMATION	
ITSEF Identification	DEKRA Testing and Certification S.A.U. (ITSEF-2024-01) C/ Severo Ochoa, 2 y 6. Parque Tecnológico de Andalucía; 29590 Campanillas (Málaga) Body Number at ENISA: ITSEF 3095

CONTENT

1. EXECUTIVE SUMMARY 3

2. BIBLIOGRAPHY AND ACRONYMS 6

BIBLIOGRAPHY 6

ACRONYMS 7

3. EVALUATED ICT PRODUCT 8

4. SECURITY SERVICES 10

5. ASSUMPTIONS AND CLARIFICATION OF SCOPE 12

6. ARCHITECTURAL INFORMATION 15

7. SUPPLEMENTARY CYBERSECURITY INFORMATION 16

8. ICT PRODUCT TESTING 17

9. CERTIFICATE HOLDER'S LIFECYCLE MANAGEMENT PROCESSES AND PRODUCTION FACILITIES 19

10. EVALUATION RESULTS 21

EVALUATED CONFIGURATION 21

SUMMARY OF EVALUATION ACTIVITIES 21

USAGE OF THE TOE 24

11. INFORMATION OF THE CERTIFICATE 25

12. SUMMARY OF THE SECURITY TARGET OF THE ICT PRODUCT 26

13. MARK AND LABEL 27

1. Executive Summary

This document is the Certification Report of the certification of the **PhioTX-V version 4.5.6** developed on the basis of the Evaluation Technical Report [ETR] **PHIOTX ETR**, **Version 1.2.**

This report is published together with the corresponding TOE EUCC certificate.

The TOE is the Phio Trusted Xchange™ PhioTX-V (hereafter referred to as Phio TX), a virtualized network device whose function is to distribute quantum-safe symmetric keys as an enterprise service.

The TOE is a Key Management Entity (KME), as defined in [ETSIQKD], a central component in a Quantum Key Distribution (QKD) network. It is responsible for managing cryptographic keys and cooperating with other KMEs across a network to ensure secure key distribution with post-quantum cryptography protection.

The TOE separates the key-management plane from the data plane, supports multiple post-quantum KEM algorithms (including ML-KEM, BIKE, Classic-McEliece, FrodoKEM, HQC, SNTRUP), and can be configured in “Hives” to share symmetric cryptographic keys.

The TOE is a software-only security product delivered as a virtual appliance and supporting software packages, intended to be deployed in a customer-controlled IT environment. Specifically, the TOE is provided as a preconfigured virtual machine image (OVA format). The TOE does not rely on dedicated proprietary hardware and does not include any physical components. It operates on standard virtualization infrastructures and commodity hardware provided by the end user.

The evaluation was performed using the TOE sample identified as phiotx_4.5.6_vm-vga_deb_x86_64.ova, deployed in a KVM virtual machine. This deployment constitutes the evaluated TOE configuration. The assurance provided by this certification applies exclusively to that configuration and to the security functionality specified in the Security Target [ST].

The major security features of the TOE are: Security audit, Cryptographic support, Identification and authentication, Security management, Protection of the TSF, TOE access, Trusted path/ channels. A detailed description of the security functionality is included in section **6. Security Requirements** [ST].

The following provides a summary of threats and organizational security policies (OSPs) addressed by the evaluated ICT product as documented in the [ST]:

- **Threats:**

The identified threats are:

  - Unauthorized Administrator Access: Threat agents may attempt to gain Administrator access to the Network Device.

- Weak Cryptography: Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space.
- Untrusted Communication Channels: Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic.
- Weak Authentication Endpoints: Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext.
- Update Compromise: Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device.
- Undetected Activity: Threat agents may attempt to access, change, and/ or modify the security functionality of the Network Device without Administrator awareness.
- Security Functionality Compromise: Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data.
- Password Cracking: Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device.
- Security Functionality Failure: An external, unauthorized entity could make use of failed or compromised security functionality.
- KME Link Disclosure: Threat agents may attempt to eavesdrop the communication links between the TOE and other Key Management Entities (KMEs) in a Quantum Key Distribution (QKD) network.
- Crypto Key Compromise: An attacker may gain unauthorized access to the cryptographic keys distributed to Secure Application Entities (SAEs) or inter KME communication keys.

- **Organizational Security Polices (OSPs):**

- The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

The evaluated ICT product usage is recommended given that there are not exploitable vulnerabilities for the evaluated ICT product under its operational environment. The following usage recommendations are given:

- It is mandatory to strictly follow the steps indicated in the installation documentation in order to download and install the correct version of the evaluated ICT product in a proper manner.
- The user guidance must be read and understood in order to operate the evaluated ICT product in an adequate manner according to the [ST].

- The fulfilment of the assumptions indicated in the section Assumptions and Clarification of Scope of this document is a key point as it implies evaluated ICT product environment configurations that leave some potential vulnerabilities out of the scope.

The evaluation was conducted by the ITSEF DEKRA Testing and Certification S.A.U. and was finished on 02/10/2026 with **PASS** verdict.

The evaluation was conducted in accordance with the Common Criteria (CC) standard, version 2022, Revision 1 [CC2022].

The evaluation activities performed during the evaluation correspond to an assurance level of **EAL2** and with **AVA_VAN.2** as specified in [CC2022p3] and [CEM2022].

The certification results apply only to the product version specified in the certificate, subject to the conditions set out in this Certification Report.

The patch management is out of the scope of the evaluation.

Considering that all evaluation activities have been conducted in accordance with the Common Criteria requirements and have resulted in PASS, the Technical Reviewers' Team issues the following recommendation regarding the certification decision:

Recommendation on Certification Decision		
Recommendation of the Technical reviewer's team	**POSITIVE**	Certificate validity period: 5 years

2. Bibliography and Acronyms

Bibliography

[CC2022p1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 2022, Revision 1

[CC2022p2] Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 2022, Revision 1

[CC2022p3] Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 2022, Revision 1

[CC2022p4] Common Criteria for Information Technology Security Evaluation. Part 4: Framework for the specification of evaluation methods and activities. Version 2022, Revision 1

[CC2022p5] Common Criteria for Information Technology Security Evaluation. Part 5: Pre-defined packages of security requirements. Version 2022, Revision 1

[CEM2022] Common Methodology for Information Technology Security Evaluation. Version 2022, Revision 1

[CSA] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[EUCC] COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)

[SotA] EUCC SCHEME DRAFT STATE-OF-THE-ART DOCUMENT. ACCREDITATION OF ITSEFs FOR THE EUCC SCHEME. Version 1.6c, July 2025

[ST] Phio TX version 4.5.6, Common Criteria Security Target, version 1.7, 28/09/2026

[AGD] Phio TX Administration Guide, Version 4.5-12.

[VUL1] EUCC Vulnerability Management Policy (VM-01), Version: 1.0, 2026-03-13.

[VUL2] EUCC Public Vulnerability Disclosure Method (VM-02), Version: 1.2, 2026-03-14.

[VUL3] EUCC Vulnerability Intake and Impact Analysis Procedure (VM-03), Version: 1.0, 2026-03-13.

[VUL4] EUCC Composite Product Notification Procedure (VM-04), Version: 1.0, 2026-03-13.

[VUL5] EUCC Vulnerability Information Transmission Procedure (VM-05), Version: 1.0, 2026-03-13.

[VUL6] https://quantumxc.com/vulnerability-disclosure

[ETR] PHIOTX-ETR Report, Version 1.2, 02/10/2026.

[ETSIQKD] "ETSI GS QKD 014-Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API, V1.1.1, 2019-02.

Acronyms

CC	Common Criteria
CEM	Common Evaluation Methodology
CB	Certification Body
ETR	Evaluation Technical Report
ITSEF	Information Technology Security Evaluation Facility
KME	Key Management Entity
ML-KEM	Module Lattice-based Key Encapsulation Mechanism
NCCA	National Cybersecurity Certification Authority
OSP	Organizational Security Policy
PP	Protection Profile
QKD	Quantum Key Distribution
SAE	Secure Application Entity
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface

3. Evaluated ICT product

3.1 Evaluated ICT product	
Name of the evaluated ICT product	PhioTX-V version 4.5.6
Enumeration of the ICT product's components that are part of the evaluation	1. phiotx_4.5.6_vm-vga_deb_x86_64.ova 2. PhioTX Install and Admin Guide.pdf
Version number of the ICT product's components	Version 4.5.6 for the above item 1 Version 4.5-12 for the above item 2
ST reference	Phio TX version 4.5.6, Common Criteria Security Target, version 1.7, 28/09/2026
CC / CEM Version and Assurance Level	[CC2022] / [CEM2022] EAL2
Identification of additional requirements to the operating environment of the certified ICT product	A single configuration is included in the scope of the evaluation, deployed on a preconfigured virtual machine image (OVA). Common Criteria Mode [AGD]: The EUCC mode is disabled by default and can be activated by specifying an appropriate value in the YAML configuration file. This mode is essential for enhancing security features to ensure compliance with [ST] requirements.
Name and contact information of the holder of the EUCC certificate	Quantum Xchange, Inc. 3 Bethesda Metro Center Suite 700, Bethesda, MD 20814, USA Contact person: Andrey Vovk andrey.vovk@quantumxc.com
Patch management procedure included into the certificate	N/A
Vulnerability handling and Disclosure procedures / assurance continuity	EUCC Vulnerability Management Policy (VM-01) [VUL1] with supporting documents: [VUL2], [VUL3], [VUL4], [VUL5]. https://quantumxc.com/vulnerability-disclosure [VUL6]

Link to the website of the holder of the EUCC certificate where supplementary cybersecurity information for the certified ICT product in accordance with Article 55 of Regulation (EU) 2019/881 is provided	– Cybersecurity information – https://quantumxc.com/cybersecurity-information/ – Security advisories – https://quantumxc.com/security-advisories/ – Vulnerability disclosure – https://quantumxc.com/vulnerability-disclosure/

3.2 TOE Deliverables	
Component	**Description**
phiotx_4.5.6_vm-vga_deb_x86_64.ova	A binary OVA virtual machine image file containing the preconfigured TOE.
phiotx_4.5.6_vm-vga_deb_x86_64.ova.sha256	A text file containing a 256-bit cryptographic hash used to verify that a downloaded or transferred file has not been altered or corrupted.
phiotx_4.5.6_vm-vga_deb_x86_64.ova.sha512	A text file containing a 512-bit cryptographic hash used to verify that a downloaded or transferred file has not been altered or corrupted.
phiotx_4.5.6_open-source_deb_x86_64.tar.gz	An archive file contains third-party libraries used by the TOE.
phiotx_4.5.6_open-source_deb_x86_64.tar.gz.sha256	A text file containing a 256-bit cryptographic hash used to verify that a downloaded or transferred file has not been altered or corrupted.
phiotx_4.5.6_open-source_deb_x86_64.tar.gz.sha512	A text file containing a 256-bit cryptographic hash used to verify that a downloaded or transferred file has not been altered or corrupted.
PhioTX Install and Admin Guide.pdf	Phio TX Administration Guide [AGD] used for secure installation, configuration and operation of the TOE.

4. Security Services

The TOE provides the following security services [ST]:

- Security audit:
  - Transmits audit data to external entities using a trusted channel.
  - Stores audit data locally on the TOE.
  - Overwrites oldest records in local storage when full to maintain continuous logging.
- Cryptographic support:
  - Generates, establishes, and destroys cryptographic keys.
  - Performs encryption, decryption, signature, and hashing operations.
  - Utilizes cryptography for securing communication channels and firmware updates.
- Identification and authentication:
  - Provides password-based authentication for administrators.
  - Authentication required before any Command Line Interface (CLI) interaction.
  - Configuration includes management of password policies and number of authentication failures.
- Security management:
  - Trusted Update mechanism.
  - Restriction of TSF management to the Security Administrator.
  - Local and remote administration of the TOE by the Security Administrator.
- Protection of the TSF:
  - Prevents disclosure of pre-shared, symmetric, private key and passwords.
  - Conducts self-tests on start-up to ensure software integrity.
  - Enables administrators to manage firmware/software updates using digital signatures for integrity check.
  - Provides reliable time stamps by its internal system clock.
- TOE access:
  - Displays a Security Administrator-specified advisory banner before establishing an administrative user session.
  - Allows administrators to initiate termination of their own interactive sessions.
  - Automatically terminates interactive sessions after a Security Administrator-defined period of inactivity.
- Trusted path/ channels:

- Supports secure communication channels for trusted interactions with the audit server.
- Provides a secure channel for remote administrators using SSH.
- Channels used between the TOE and other KMEs are post-quantum protected.

The vulnerability handling policy of the manufacturer is described in EUCC Vulnerability Management Policy (VM-01) [VUL1] and the following supporting documents: [VUL2], [VUL3], [VUL4], [VUL5]. There is also the Vulnerability Disclosure website https://quantumxc.com/vulnerability-disclosure [VUL6] describes how to report vulnerabilities.

The assurance continuity policy will follow [EUCC] regulation.

The patch management is out of the scope of the evaluation.

5. Assumptions and Clarification of Scope

The TOE is assured to provide effective security measures in a cooperative, non-hostile environment, provided that it is correctly installed, managed, and used. The following specific conditions are assumed to exist in the operational environment where the TOE is employed:

Assumption	Description
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, this ST does not include any requirements on physical tamper protection or other physical attack mitigation. This ST does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general-purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/ generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by this [ST].

A.TRUSTED_ADMINISTRATOR	The Security Administrator for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/ credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', 'trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification). The Security Administrator shall not create or delete users in the TOE's Operating System, as specified the installation and user guides.
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

A.OPERATIVE_SYSTEM	It is assumed that the underlying Operating System is outside the scope of the TOE and that the Security Administrator does not perform direct administrative, configuration, or user management actions on the Operating System (including user management, modifying OS configurations, or managing system services), strictly adhering to the operational procedures specified in the TOE installation and user guidance documentation.

The TOE is available as a virtual machine image for the following platforms:

- VMware as an OVA.
- KVM as a qcow2 disk image.
- Amazon Web Services as an AMI.
- Microsoft Azure as a VHD.

The minimum system requirements for all the above platforms are the same and following:

- CPU: 1 vCPU, x86_64
- RAM Memory: 512 MB
- Hard Disk: 8 GB

The TOE is not intended to counter threats outside the assumptions and operational environment defined in the Security Target [ST].

The certification applies exclusively to the evaluated TOE configuration and to the security functionality explicitly described in the [ST]. The evaluated TOE configuration consists of the TOE sample phiotx_4.5.6_vm-vga_deb_x86_64.ova as deployed in a KVM virtual machine for the evaluation.

6. Architectural Information

The basic design of the TOE in terms of SFR-enforcing and SFR-supporting subsystems provides a high-level description of the TOE architecture and its compliance with the security functionality [ST].

The TOE security functionality is deployed into the following subsystems:

SFR-enforcing subsystems:

- Core Services Subsystem: The central and most critical component of the Phio TX platform. It provides the full lifecycle management of cryptographic keys, the orchestration of quantum and post-quantum secure communication between nodes, and the enforcement of operational and security controls across the entire system.
- Operating System Subsystem: It provides the secure execution environment in which the TOE's core services operate, with emphasis on three foundational functions that underpin trusted operations: random number generation, trusted timestamping, and secure remote administration via the SSH library.
- Boot Chain Subsystem: It governs the secure initialization sequence of the Phio TX platform. It ensures that cryptographic assurance, software integrity, entropy availability, and network readiness are sequentially validated and established before any operational or cryptographic service becomes active.
- Monitoring and Reporting Subsystem: The centralized observability and control-plane service for Phio TX. It aggregates security and operational events from all platform services, maintains system and service telemetry, and provides external visibility through standards-based monitoring interfaces.
- Access and configuration subsystem: It provides administrative shell access by wrapping and supervising the OpenSSH daemon with built-in brute-force protection, connection limiting, firewall integration and centralized auditing.

SFR-supporting subsystems:

- Database (File System) Subsystem: It is the Phio TX configuration and state persistence component responsible for maintaining all validated system configurations, runtime flags, and operational metrics required by the platform's trusted services. It provides a unified, integrity-protected data layer shared across subsystems.
- Networking and Firewall Subsystem: The Network Subsystem is the early-boot networking and firewall manager that establishes interface state, IP addressing (static/DHCPv4/v6), routing (including default gateway), and resolver configuration, while continuously monitoring link and route changes to keep the platform reachable and policy-compliant.

7. Supplementary Cybersecurity Information

Quantum XChange provided the following public webpages to address Article 55 of Regulation (EU) 2019/881 for PhioTX-V, version 4.5.6.

- Cybersecurity information - https://quantumxc.com/cybersecurity-information/
- Security advisories - https://quantumxc.com/security-advisories/
- Vulnerability disclosure - https://quantumxc.com/vulnerability-disclosure/

Article 55(1)(a) - Guidance for secure configuration, installation, deployment, operation and maintenance.

- The cybersecurity information page identifies the TOE as PhioTX-V, version 4.5.6, and links to the evaluated Administration Guide, revision 4.5-12. The guide provides end users with guidance on secure configuration, installation, deployment, operation and maintenance. https://quantumxc.com/cybersecurity-information/

Article 55(1)(b) - Security support period, including cybersecurity-related updates.

- The website states that security support, including updates and patches, is available through **16 March 2029**. The support period is clearly disclosed. https://quantumxc.com/cybersecurity-information/

Article 55(1)(c) - Contact information and accepted methods for reporting vulnerabilities

- Quantum XChange publishes its PSIRT email address (security@quantumxc.com) and accepts vulnerability reports by email from end users and security researchers. Its Vulnerability Disclosure page explains what to include in a report.

Article 55(1)(d) - Public vulnerability repositories and relevant cybersecurity advisories.

- The manufacturer's cybersecurity information page links to its public Security Advisories page, which serves as the repository for publicly disclosed vulnerabilities and relevant advisories for the product. The reference required under Article 55(1)(d) is provided.

  - Cybersecurity information - https://quantumxc.com/cybersecurity-information/
  - Security advisories - https://quantumxc.com/security-advisories/

The certificate holder is responsible for keeping this information electronically available and updated as necessary at least until certificate expiry, in accordance with Article 55(2).

8. ICT Product Testing

The certificate is issued by **DEKRA Testing and Certification S.A.U. EUCC CB (3095)**, under the authority of the Spanish NCCA (ANCC CCN-Centro Criptológico Nacional).

The evaluation was performed by **the ITSEF DEKRA Testing and Certification S.A.U.**

The evaluation activities performed for an assurance level of **EAL2** as specified in [CC2022p3] and [CEM2022], are summarized in the following table:

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP.2 Security-enforcing functional specification ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedure
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system ALC_CMS.2 Parts of the TOE CM coverage ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

No state-of-the-art documents or additional security evaluation criteria were applied in this evaluation.

The [ST] does not claim conformance to any PP.

Independent testing was performed by the evaluator to verify that the TOE operates as specified, following an SFR-oriented approach. The evaluator, as part of the independent tests, repeated a sample of the developer tests, following his procedures to gain confidence in the results obtained. Next, the evaluator devised, based on the developer tests, their own test scenarios to operate the TOE in a different manner. The main objective of the tests was to check that the security functional requirements defined in [ST] are implemented as expected, and whether the subsystems behave as defined in the TOE design documentation, and whether TSFIs definitions are consistent with the TOE functional specification.

In addition, a vulnerability analysis was conducted based on publicly available sources, the TOE documentation, and its evaluated configuration. An independent search for potential vulnerabilities did not identify any applicable vulnerabilities or plausible attack paths exploitable with a Basic attack potential. During the evaluation activities development, it has been recorded several aspects of concerns which have been considered in the penetration tests design. All potential vulnerabilities identified were tested through the penetration testing which confirmed the TOE is resilient against attackers with the BASIC attack potential.

9. Certificate Holder's Lifecycle Management Processes and Production Facilities

The lifecycle management processes employed by the TOE's manufacturer cover: TOE unique reference, Configuration Management System, Configuration Items (CIs) list, and delivery procedure.

TOE unique reference

- TOE identification: The TOE (PhioTX-V 4.5.6) adheres to a structured semantic versioning convention denoted as A.B.C, where each segment of the version number corresponds to a specific category of change: A - Major release, B - Feature update, C - Security patch/ maintenance.
- Documentation identification: Each document produced by Quantum Xchange has a title and document version that identifies it. This information is displayed on the cover page.

Configuration Management System

- Identification of Configuration Items: Source Code - All source code Configuration Items (CIs) are managed within the Cloud GitHub Quantum Xchange organization; Documentation - All documentation configuration items (e.g., Security Target, design documents, guidance documents, test documentation) are managed using the Box (box.com) cloud-based CM system.
- Assignment of Identifiers and Entry into the CM System: Source Code - New CIs enter CM when committed to the GitHub repositories; Documents - A document CI is entered into CM when it is uploaded or updated within the controlled Box folder structure.
- Identification of superseded CI versions: Source Code - A CI version is superseded when a subsequent commit modifies the same repository/ path; Documents - A document version is superseded automatically when a newer version is uploaded to the Box.

Configuration Items list

- TOE items: A list includes virtual machine image file containing the preconfigured TOE, text files with cryptographic hashes, third-libraries archive file, the Administration Guide [AGD].
- Evaluation evidence items: A list includes evaluation evidence documents - ST (ASE), ADV, ALC, ATE, AGD, security testing plan and results.

Delivery procedure

- Delivery method: Distribution Channel - The TOE is distributed via the internet using the secure Box.com platform. Confidentiality, Integrity and Authenticity during transport is assured through the use of HTTPS (provided by the Box.com platform); Access

Control – Access to the download is restricted. Customers are provided with personal expiring links.

- Delivery Contents: The TOE is packaged as a software distribution bundle containing: the executable or installable package for the specific platform, cryptographic checksum files (SHA-256 and SHA-512) corresponding to the package; release notes and required open-source license and notice documentation.
- User Verification Procedure: Verification of the delivery source (Box.com) – Prior to downloading any artifact from Box.com, the user shall verify that the download link has been received through an authenticated and trusted communication channel, TLS server certificate is valid, there are no browser warnings indicating certificate errors; Integrity verification using cryptographic hashes – After download, the user shall verify the integrity of the TOE package by computing the cryptographic hash and comparing the results with the corresponding hash value provided by the developer.

10. Evaluation Results

The ITSEF produced and provided the Evaluation Technical Report [ETR] and companion partial reports of each activity (ASE, ADV, ALC, AGD, ATE and AVA) according to the requirements of the [EUCC] and the Common Criteria [CC2022] and the Common Evaluation Methodology [CEM2022].

The evaluation of the ICT product, has confirmed that it meets the requirements for assurance level 'Substantial' as defined in Article 4 of the EUCC Implementing Regulation and Article 52 of Regulation (EU) 2019/881 [EUCC].

The AVA_VAN.2 component indicates that the product was evaluated to resist attacks from attackers with a BASIC attack potential.

Based on the review of the evaluator's analysis and conclusions for the ASE, ALC, AGD, ADV, ATE, and AVA activities, it can be confirmed that the evaluation was conducted in accordance with the Common Criteria [CC2022] requirements and the Common Evaluation Methodology [CEM2022].

Evaluated Configuration

The TOE evaluated configuration included phiotx_4.5.6_vm-vga_deb_x86_64.ova (a virtual machine image file with the preconfigured TOE) and Administration Guide [AGD].

The evaluator configured the TOE and test environment according to the preparative procedures [AGD]. The testing was performed using the virtual machine image phiotx_4.5.6_vm-vga_deb_x86_64.ova, deployed in a KVM virtual machine. This deployment constitutes the evaluated TOE configuration. The evaluator defined and performed test cases considering security requirements defined in [ST] and external interfaces defined in the TOE functional specification documentation.

This configuration is established by following the guidance provided with the TOE and ensuring that all security objectives for the operational environment specified in the [ST] are fulfilled.

As detailed in the [ETR], the evaluator tested the TOE using this reference configuration.

Summary of Evaluation Activities

The evaluation resulted in a PASS verdict for all assurance components listed in section 7 of [ETR] and claimed in the Security Target [ST]. A summary of the evaluation activities is provided below.

ASE:

The findings are well-documented and internally consistent, demonstrating a thorough understanding of the Security Target and its components. The identified threats, security objectives, and security requirements are appropriately addressed, and the TOE description is both accurate and adequate for the evaluation level. Consequently, the ASE activities fulfil the assurance requirements for EAL2. No issues or deviations were identified that could impact the assurance of the TOE.

ALC:

The evaluation results demonstrate that the TOE's lifecycle processes, covering configuration management, delivery, and related controls, are clearly defined, properly implemented, and aligned with the required assurance level. The submitted evidence supports traceability of changes and the secure handling of the TOE throughout its lifecycle. The lifecycle management processes demonstrate a unique TOE reference, configuration management and delivery are clearly defined, and appropriately implemented to ensure there is no ambiguity in terms of which instance of the TOE is being evaluated. Therefore, the ALC activities satisfy the assurance requirements for EAL2 with no issues or deviations identified that could compromise the TOE's security.

AGD:

The evaluation has demonstrated that the guidance documentation is clear, complete, and sufficient to support the secure installation, configuration, and operation of the TOE within its intended environment. The guidance effectively helps prevent common misconfigurations and promotes correct usage. The Administration Guide [AGD] provides the sound Common Criteria Compliance and Secure Configuration guidelines to maintain the TOE's certification compliance, and Common Criteria Mode to ensure conformance with the [ST] requirements. Accordingly, the AGD activities fulfil the assurance requirements for EAL2 with no issues or deviations identified.

ADV:

The findings confirm that the design documentation provides sufficient detail to understand the TOE's architecture and security-enforcing and -supporting functions. The evidence demonstrates clear traceability between the security requirements and the TOE design. The basic design documentation demonstrates that the TOE is adequately described by its functional specification which identifies the TOE's interfaces and behaviour in a clear and understandable manner. The security architecture provides a sound description of the TSFs structured such that it cannot be tampered with or bypassed, and the TOE design is described in terms of subsystems. Accordingly, the ADV activities meet the assurance requirements for EAL2 with no issues or deviations identified.

ATE:

The testing evidence provided by the developer has been thoroughly reviewed and verified as complete, demonstrating correct implementation of the TOE's specified security functions. This includes validation of cryptographic operations, user data protection, and other security measures to ensure compliance with the defined requirements.

The evaluator performed ATE evaluation activities by checking the coverage of TSFIs tested by the manufacturer (ATE_COV), repeating functional tests performed by the developer (ATE_FUN), and independent testing of a subset of the TSFIs (ATE_IND).

The test repetition has demonstrated the test plan and report provided by the developer contained enough information to repeat all tests, and the results obtained were the same as the expected ones.

The independent cases were devised with the use of the specific criteria, e.g.: critical parameters in the TSFIs and subsystems interactions; exhaustive tests over the most important TSFIs; incorrect behaviour suspicion with specific input values. The results of all tests confirmed the TOE operates as intended, with no failures or security vulnerabilities identified.

As a result, the independent testing confirms that the TOE complies with all relevant security requirements specified for the evaluation. The testing process, encompassing both the developer's evidence and the evaluator's independent tests, has been comprehensive and thorough. No issues or deviations were identified during the evaluation, and the testing activities fully satisfy the assurance requirements for EAL2.

AVA:

The evaluator performed a vulnerability analysis to identify publicly known vulnerabilities and assess whether any could be exploited with a BASIC attack potential. This includes a thorough analysis of both the TOE itself and third-party libraries it relies on. The evaluation considered publicly known vulnerabilities, such as those listed in security databases or related to the software components used by the TOE.

The evaluator analysed the [ST], guidance documentation, functional specification, TOE design and security architecture description during evaluation evidence activity to identify areas of concern for potential vulnerabilities. The testing process included penetration tests based on commonly known methods and techniques to test the TOE's resistance against potential exploitation.

Consequently, the AVA activities were performed in full compliance with the assurance requirements for EAL2, providing a reasonable level of confidence in the TOE's resilience against attackers with the BASIC attack potential.

Usage of the TOE

The use of the certified ICT product is recommended, as no exploitable vulnerabilities have been identified within the defined operational environment. The following usage recommendations apply:

- The installation procedures provided in the documentation [AGD] shall be strictly followed to ensure the correct download and proper installation of the evaluated version of the ICT product.
- The user guidance [AGD] shall be carefully read and understood to ensure that the product is operated in accordance with the Security Target [ST].
- Compliance with the assumptions specified in section Assumptions and Clarification of Scope is essential, as these define the evaluated operational environment and imply that certain potential vulnerabilities are considered out of scope.

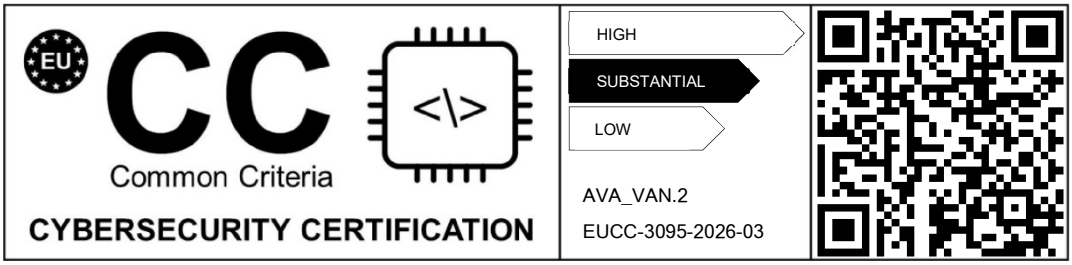
11. Information of the Certificate

Date of Issuance	10/11/2026
Period of Validity	Valid for five years from the date of issuance *The certificate is valid for five (5) years from the date of issuance, inclusive, and remains valid until the end of 9/11/2031, unless suspended or withdrawn earlier*
Unique Identifier of the Certificate	EUCC-3095-2026-03 version 1.0
Scheme Name	(EU) 2024/482 - EUCC
Certification Body Accreditation Reference Number	DEKRA Testing and Certification S.A.U. EUCC CB ENAC´s Accreditation number **134/C-PR337** ENISA´s Body number: **3095**
Certificate Authorising Participant	ANCC CCN-Centro Criptológico Nacional

12. Summary of the Security Target of the ICT Product

For publication purposes, the Security Target of the TOE [ST] “Phio TX version 4.5.6, Common Criteria Security Target, version 1.7, 28/09/2026” is provided as a separate document together with this Certification Report.

13. Mark and Label



Signature: Dariusz Rogowski **EUCC CB Technical Reviewer** DEKRA Testing and Certification S.A.U.	Signature: Alejandro Muñoz del Rey **EUCC CB Technical Manager** DEKRA Testing and Certification S.A.U.