CyberSecurity MALAYSIA
An agency under MOSTI

People First, Performance Now

MOSTI
Ministry of Science, Technology and Innovation

C059 Certification Report

qCrypt-xStream R1.1

File name: ISCB-5-RPT-C059-CR-d1
Version: v1
Date of document: 27 March 2015
Document classification: PUBLIC

Malaysian Common Criteria Evaluation & Certification Scheme® MyCC

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

Securing Our Cyberspace

CyberSecurity Malaysia
(726630-U)

Best Brand Internet Security 2008 & 2009
STANDARDS MALAYSIA ACCREDITED LABORATORY MS ISO/IEC 17025 TESTING SAMM NO. 456 (MySEF LABORATORY)
MSC MALAYSIA Status Company
Best Child Online Protection Website

T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

C059 Certification Report

qCrypt-xStream R1.1

27 March 2015

ISCB Department

CyberSecurity Malaysia

Level 5, Sapura@Mines,

No 7 Jalan Tasik,The Mines Resort City

43300 Seri Kembangan, Selangor, Malaysia

Tel: +603 8992 6888 Fax: +603 8992 6841

http://www.cybersecurity.my

Document Authorisation

Copyright Statement

Registered office:
Level 5, Sapura@Mines
No 7, Jalan Tasik,
The Mines Resort City,
43300 Seri Kembangan
Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee
Company No. 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 03 April 2015, 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 www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement at www.commoncriteriaportal.org).

Reproduction of this report is authorised provided the report is reproduced in its entirety.

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (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	23 March 2015	All	Initial draft.
v1	27 March 2015	vii	Update Executive Summary

Executive Summary

qCrypt-xStream R1.1 from QuintessenceLabs is the Target of Evaluation (TOE) for the Evaluation Assurance Level 2 (EAL2) evaluation.

qCrypt-xStream consisting of the two main components which is Appliance qCrypt-xStream R1.1-Part number 1362 and Quantum Random Number Generator (QRNG) card - Part number 1108. The TOE is a cryptographic key management appliance, designed to centrally manage enterprise digital keys and certificates for enterprise applications, users and devices throughout their full life cycle, including key generation, distribution, usage, automated rotation and renewal in accordance with TOE-defined policy. The TOE can be deployed as part of any cryptographic system that uses digital keys. The TOE is intended to provide a high-level of assurance in protection of the digital keys, especially keys that are of high-value, to avoid negative impact on the system if the keys were to be compromised.

The powerful synthesis of the TOE with its key management functionality delivers significant cost-effective benefits and efficiencies in the operational, incident and change management processes.

The scope of evaluation covers major security features as follows:

a) Access control- the TOE implements a role based access control to ensure that only users authenticated with their credentials are permitted to perform allocated functions.

b) Audit- the TOE logs significant events to an internal audit log with at minimum a timestamp.

c) Cryptographic operations - the TOE implements several cryptographic algorithms in hardware and software. These algorithms are used internally by the TOE and are also provided to users by the QuintessenceLabs Key Manager (QKM). The TOE implements asymmetric and symmetric encryption algorithms, key generation algorithms, signing, cryptographic checksum and random number generation algorithms.

d) Data protection - the TOE implements mechanisms to secure TOE data when it is both at rest and when it is exported from the TOE.

e) Secure key management - the TOE provides the means to generate and manage cryptographic keys as part of the KMIP service offered to clients, as well as for use with its various cryptographic functions.

f) Security management - the TOE implements a set of self-test that verifies the TOE's cryptographic algorithms and random number generator (QRNG).

g) Self-test - the TOE implements a set of self-test that verifies the TOE's cryptographic algorithms and random number generator (QRNG).

h) User authentication - the TOE provides a mechanism for secure authentication.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for TOE, the security function 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 2 (EAL2) Extended with Extended Declaration of FCS_RNG_EXT. 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 BAE Systems Lab – MySEF evaluation facility and completed on 17 March 2015.

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 www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of user to ensure that qCrypt–xStream R1.1 meets their requirements. It is recommended that a potential user of qCrypt–xStream R1.1 to 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), qCrypt-xStream R1.1 (hereafter referred as qCrypt-xStream) consist of two main components which is Appliance qCrypt-xStream R1.1-Part number 1362 and Quantum Random Number Generator (QRNG) card – Part number 1108.

2 The TOE is a cryptographic key management appliance, designed to centrally manage enterprise digital keys and certificates for enterprise applications, users and devices throughout their full life cycle, including key generation, distribution, usage, automated rotation and renewal in line with TOE-defined policy.

3 The TOE is intended to provide a high-level of assurance in protection of the digital keys, especially keys that are high-value, to avoid negative impact on the system if the keys were to be compromised. The powerful synthesis of the TOE with its key management functionality delivers significant cost-effective benefits and efficiencies in the operational, incident and change management processes.

4 The TOE primary features include:

a) Secure generation, distribution and destruction of cryptographic keys;

b) On-board cryptographic functions to secure traffic sent between the TOE and external users,

c) Secure storage and management of keys throughout their lifecycle,

d) Role-based authentication and access control mechanisms to facilitate controlled access to cryptographic key management and TOE management functions by trusted personnel only;

e) Functionality to detect errors in received traffic or replay attacks;

f) Auditing of security relevant events to provide suitable accountability;

g) Protection of stored audit data to prevent modification or accidental deletion; and

h) Self-test of the core cryptographic functions and algorithms of the TOE.

5 The major security functions that implemented by the TOE are as below:

a) **Access control**- the TOE implements a role based access control to ensure that only users authenticated with their credentials are permitted to perform allocated functions.

b) **Audit**- the TOE logs significant events to an internal audit log with at minimum a timestamp.

c) **Cryptographic operations** – the TOE implements several cryptographic algorithms in hardware and software. These algorithms are used internally by the TOE and are also provided to users by the QuintessenceLabs Key Manager (QKM). The TOE implements asymmetric and symmetric encryption algorithms, key generation algorithms, signing, cryptographic checksum and random number generation algorithms.

d) **Data protection** – the TOE implements mechanisms to secure TOE data when it is both at rest and when it is exported from the TOE.

e) **Secure key management** – the TOE provides the means to generate and manage cryptographic keys as part of the KMIP service offered to clients, as well as for use with its various cryptographic functions.

f) **Security management** – the TOE implements a set of self-test that verifies the TOE's cryptographic algorithms and random number generator (QRNG).

g) **Self-test** – the TOE implements a set of self-test that verifies the TOE's cryptographic algorithms and random number generator (QRNG).

h) **User authentication** – the TOE provides a mechanism for secure authentication.

1.2 TOE Identification

6 The details of the TOE are identified in **Error! Reference source not found.** below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C059
TOE Name	qCrypt–xStream
TOE Version	R1.1
Security Target Title	qCrypt–xStream R1.1 Security Target
Security Target Version	Version 1.0
Security Target Date	16 March 2015
Assurance Level	Evaluation Assurance Level 2 (EAL2)
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref [2])
Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL2 Extended with Extended Declaration of FCS_RNG_EXT
Sponsor and Developer	QuintessenceLabs Unit 1 Lower Ground 15 Denison St Deakin, ACT 2600
Evaluation Facility	BAE Systems Lab – MySEF

1.3 Security Policy

7 There are no organisational security policies defined regarding the use of the TOE.

1.4 TOE Architecture

8 The TOE includes both logical and physical boundaries which are described in Section 1.6 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

9 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality in Table 2:

Table 2: Logical Boundaries

Security function	Description
Access control	The TOE implements administrative roles that are used for segmenting access control. Each role has pre-defined access to certain functions.
Audit	The TOE logs significant events to an internal audit log with at minimum a timestamp.
Cryptographic operations	The TOE implements several cryptographic algorithms in hardware and software. These algorithms are used internally by the TOE and are also provided to users by the QuintessenceLabs Key Manager (QKM). The TOE implements asymmetric and symmetric encryption algorithms, key generation algorithms, signing, cryptographic checksum and random number generation algorithms.
Data protection	The TOE implements mechanisms to secure TOE data when it is both at rest and when it is exported from the TOE.
Secure key management	The TOE provides the means to generate and manage cryptographic keys as part of the KMIP service offered to clients, as well as for use with its various cryptographic functions.
Security management	The TOE implements a set of functions and mechanisms to securely manage the TSF and TSF data.
Self-test	The TOE implements a set of self-test that verifies the TOE’s cryptographic algorithms and random number generator (QRNG).
User authentication	The TOE provides a mechanism for secure authentication.

1.4.2 Physical Boundaries

10 The TOE is a self-contained appliance consisting of two main components, namely the QuintessenseLabs Key Manager (QKM) and the Quantum Random Number Generator (QRNG), as a single product in the form of an appliance. It has been explained in below figure:

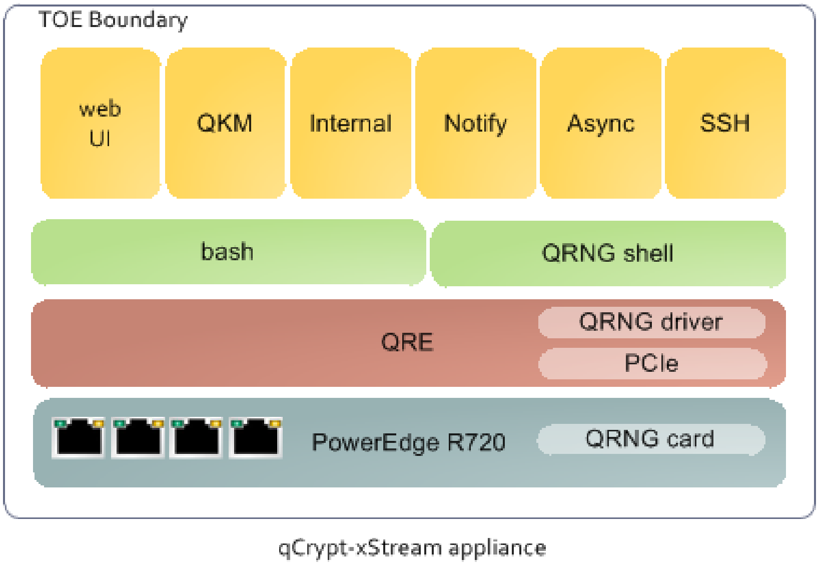
Table 3: TOE Main Components

Main Components	Figure	Description
QuintessenseLabs Key Manager (QKM)		The QKM is a software based component that is managed via a web management interface.
Quantum Random Number Generator (QRNG)		The QRNG is a hardware based component with an optics core for laser processing, which serves as a quantum based entropy source and is able to produce true random data at a rate of 1Gb/s.

11 The TOE has four (4) Ethernet ports which can be individually associated to one or more of the following networks: management, replication or client.

12 Internally, the TOE is comprised of a number of different components that combine to deliver the core security functionality and capabilities of the device. Figure 2 below illustrates the high level functionality on the scope of the TOE.

Figure 1: TOE Component



13 The key components of the TOE are described in the following table.

Table 4: TOE components

Component	Description
Web user interface (Web UI)	Provides the main mechanism for administering the TOE.
QuintessenceLabs Key Manager (QKM)	Externally-accessible KMIP server
Internal	Supports the Web UI (only accessible via local sockets).
Notify	Provides server-generated notifications to clients
Async	Supports the QKM by handling asynchronous KMIP operations.
SSH	Allows remote login to the TOE for administrative purposes.
Bash shell	Allows remote access to the TOE for general administration of the device.
QRNG shell	Allows remote access to the TOE for configuration and maintenance of the QRNG.
QuintessenceLabs run-time environment (QRE)	QRE is a purpose-built distribution of the Linux operating system

1.5 Clarification of Scope

14 The TOE is designed to centrally manage enterprise digital keys and certificates for enterprise applications, users and devices throughout their full life cycle, including key generation, distribution, usage, automated rotation and renewal in accordance with TOE-defined policy.

15 The TOE can be deployed as part of any cryptographic system that uses digital keys and intended to provide a high-level of assurance in protection of the digital keys, especially keys that are high-value in order to avoid negative impact on the system if the keys were to be compromised.

16 Section 1.4 of this document described the scope of the evaluation which was limited to those claimed made in the Security Target (Ref [6]). The TOE is a self-contained appliance consisting of two main components, namely the QuintessenceLabs Key Manager (QKM) and the Quantum Random Number Generator (QRNG) as a single product in the form of an appliance. It can be categorised as a key management system in accordance with the categories identified on the Common Criteria Portal that lists all certified products.

17 The TOE operates in their own hardware appliance, operating system and medium storage specified in Section 1.6.3 of the Security Target (Ref [6]) which are not part of TOE scope.

18 Potential consumers of the TOE are advised that some functions and services of the overall product have not have 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

19 This section summarises the security aspects of the environment/configuration in which IT product is intended to operate. Consumers should understand their own IT environments and that required for secure operation of the TOE which has defined in the Security Target (Ref [6]).

1.6.1 Usage assumptions

20 Assumption for the TOE usage as listed in Security Target :

a) The Administrator is not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by administrator documentation.

b) It is assumed that KMIP clients protect the keys and other security sensitive data that are used to communicate with the TOE.

1.6.2 Environment assumptions

21 Assumptions for the TOE environment listed in Security Target are:

a) The underlying platform on which the TOE operates will be updated when needed with the latest security patches and fixes to ensure data stores on the platform remains protected and secure.

1.7 Evaluated Configuration

22 The TOE is a cryptographic key management appliance, designed to centrally manage enterprise digital keys and certificates for enterprise applications, users and devices throughout their full life cycle, including key generation, distribution, usage, automated rotation and renewal in line with TOE-defined policy which running in their own hardware appliance and compatible with Web UI as described in Section 1.6 of the Security Target (Ref [6]).

1.8 Delivery Procedures

23 The TOE is sent to the customers using delivery procedure (Ref (25b), which ensures that the TOE is securely transferred from development environment to the responsibility of the customer. The brief delivery procedures are outlined below:

a) <u>Order placement</u>

Customer must request the shipment of a QuintessenceLabs appliance. Upon receiving a Purchase Order from the customers, QuintessenceLabs will begin the assembly process in the final manufacturing facility.

b) <u>Product Assembly</u>

Upon confirming with the customers buyer on the shipment address of the TOE, the final assembly process begins with allocating Serial Numbers to systems. This Serial Number is used to track the system through manufacturing.

The final assembly of the qCrypt-xStream components and the software is carried out in a secure environment within QuintessenceLabs, which is only accessible through a key card access. Hence, access to the appliance within the manufacturing environment is limited to QuintessenceLabs staff only.

c) <u>Product Identification Label Application</u>

The packaging of the qCrypt-xStream appliance includes labels of Warnings, Rules of Origin, quantity/weights/measurements and a Dangerous Goods Declaration.

d) <u>Packaging</u>

QuintessenceLabs packages the qCrypt-xStream appliance in a double skinned cardboard box with internal foam cut-outs. The appliance is wrapped in a plastic bag that is specifically designed to protect the DELL- PowerEdge 720 server that is used for the qCrypt-xStream. The box is then sealed with a packaging tape and labelled with heavy lift stickers, dispatch labels, a shipping document envelope that contains export permissions, an invoice and a packing list. If the packaging includes lithium batteries, a Dangerous Good Declaration is included in the invoice.

e) <u>Shipping</u>

Upon accepting a Purchase Order and a confirmed shipping address, QuintessenceLabs determines if the shipment of the TOE is expected to be returned, for example if the purpose of shipping the TOE is for a conference or demonstration, or is not expected to return. QuintessenceLabs employs the use of a commercial carrier for its shipment of goods. The current preferred carrier is DHL. Details are as the following:

DHL Freight Forwarding (TOE expected to return):

DHL Global Forwarding
23 O'riordan Street
Alexandria NSW 2015
Ph: +61 2 93330172
Fax: +61 2 93330572
Email: krishneil.kumar@dhl.com (or delegate)

DHL Express (TOE not expected to return):

Telesales Executive
Level 9, 151-171 Roma St
Brisbane QLD Australia 4003
Tel: 1800 133 583
Email: anthony.ambrosio@dhl.com (or delegate)

Once an appliance is shipped, a receipt of appliance is sent to the email address of the customer, which the customer must acknowledge. Upon acknowledging the receipt of the appliance, a secure exchange (certified mail original copy Certificate of Compliance) of factory settings parameters will take place so the customer can access the following information:

- Administrator/installation details;
- The appliance serial number and model number; and
- Random password for administrator login (delivered via a secure file transfer site)

1.9 Documentation

24 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage of the product.

25 The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product:

a) qCrypt-xStream R1.1 Guidance Documentation v1.0, 16 March 2015

b) qCrypt-xStream R1.1 Lifecycle Documentation v1.3, 16 March 2015

c) QuintessenceLabs qCrypt-xStream R1.1 User Guide v1.0, 14 August 2014

d) QuintessenceLabs qCrypt-xStream R1.1 Troubleshooting Guide v1.0, 14 August 2014

2 Evaluation

26 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 4 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 (EAL2) Extended with Extended Declaration of FCS_RNG_EXT. The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

28 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

29 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Development

30 The evaluators analysed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), and how the TOE security function (TSF) implements the security functional requirements (SFRs).

31 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

32 The evaluators examined the TOE security architecture description; they determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

2.1.3 Guidance documents

33 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to

securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

2.1.4 IT Product Testing

34 Testing at EAL2 Extended with Extended Declaration of FCS_RNG_EXT consists of assessing developer tests, perform independent function test, and perform penetration tests. The TOE testing was conducted by evaluators from BAE Systems Lab–MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Assessment of Developer Tests

35 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, 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).

36 The evaluators analysed the developer's test coverage and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

37 At EAL2 Extended with Extended Declaration of FCS_RNG_EXT, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing sample of the developer's test plan, and creating test cases that augmented developer tests.

38 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The result of the independent functional tests were developed and performed by the evaluators to verify the TOE functionality as follows:

Table 5: Independent Functional Testing

Identifier	SFR Tested	Notes	Results
D001	• Identification and Authentication	This test aims to prove that the TSF shall maintain the following list of security attributes belonging to individual user which are Web UI root, user's username and password, SSH username and password and asymmetric keypairs.	**PASS.** Result as expected.

F001	- Identification and Authentication - Security Management - User Data Protection - Security Audit	This test aims to verify that the TOE performs specification of management functions, protected authentication feedback, user authentication and identification before any action and maintains security roles	**PASS.** Result as expected.
D002	- Security Management	These tests aim to prove that the TOE: 1. Restricts the ability to revoke security attributes associated with the User under the control of the TSF to Root; and 2. Enforces authorised users to revoke security-relevant authorizations by completely deleting user security attributes, or by modifying the user name, group, or by setting a new Password. Such revocation is to take effect when the user next authenticates to the Web UI	**PASS.** Result as expected.
D003	- Cryptographic Support	These tests aim to prove that the TOE: 1. Generates cryptographic keys in accordance with a specified cryptographic key generation algorithm in Table 11 of ST **Error! Reference source not found.** and specified cryptographic key sizes in Table 11 of ST **Error! Reference source not found.**; and 2. Performs cryptographic operations specified in Table 13 of ST **Error! Reference source not found.** in accordance with a specified cryptographic algorithm specified in Table 13 of ST **Error!**	**PASS.** Result as expected.

		Reference source not found.	
F002	• User Data Protection • Cryptographic Support	This test aims to confirm the user data stored doesn't suffer from system privilege abuse by unauthorised users. It also examines the properties and attributes of the type of information that is created during the importation and exportation of user data.	
D004	• Protection of the TSF	This test aims to verify that the TSF is able to provide reliable time stamps.	**PASS**. Result as expected.
D005	• Security Audit	This test aims to verify that the TOE performs audit data generation and security audit review.	**PASS**. Result as expected.
F003	• Trusted Path/Channels • Protection of the TSF	This test aims to verify that the TOE provides Inter-TSF confidentiality during transmission, Inter-TSF detection of modification and Inter-TSF trusted channel Trusted path.	**PASS**. Result as expected.
F004	• TOE Access	This test aims to verify that the TOE performs TSF-initiated termination and User-initiated termination.	**PASS**. Result as expected.
F005	• Cryptographic Support	This test aims to verify that the TOE performs random number generation.	**PASS**. Result as expected.

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

2.1.4.3 Penetration Testing

40 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.

41 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 attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapse 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 requirement for exploitation.

42 The penetration tests focused on:

a) SQL Injection

b) Cross Site Scripting

c) Cross-site Request Forgery (CSRF)

d) Security misconfiguration

e) Failure to restrict URL Access

f) Information Disclosure

g) Directory Traversal

h) Buffer Overflow

43 The results of the penetration testing note 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 Section 4.5 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

44 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.

3 Result of the Evaluation

45 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 qCrypt-xStream R1.1 performed by CyberSecurity Malaysia MySEF.

46 CyberSecurity Malaysia MySEF, found that qCrypt-xStream R1.1 upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) assurance level 2 (EAL2) Extended with Extended Declaration of FCS_RNG_EXT.

47 Certification is not 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

48 EAL2 Extended with Extended Declaration of FCS_RNG_EXT provides assurance by a full security target and analysis of the SFRs in that Security Target, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

49 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

50 EAL2 Extended with Extended Declaration of FCS_RNG_EXT also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

51 In addition to ensure secure usage of the product, below are additional recommendations for TOE users:

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

b) The user should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

c) The users must maintain the confidentiality, integrity and availability of security relevant data for TOE initialisation, start-up and operation if stored or handled outside the TOE.

d) System Auditor should review the audit trail generated and exported by the TOE periodically.

e) The users must ensure appropriate network protection is maintained, the network on which the TOE is installed must be both physically and logically protected, commensurate with the sensitivity of the TOE keys.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[4] MyCC Scheme Policy (MyCC_P1), v1a, CyberSecurity Malaysia, December 2009.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1, December 2009.

[6] qCrypt–xStream R1.1 Security Target, v1.0, 16 March 2015.

[7] qCrypt–xStream Evaluation Technical Report, v1.0, 17 March 2015.

A.2 Terminology

A.2.1 Acronyms

Table 6: List of Acronyms

Acronym	Expanded Term
Authentication Data	It is information used to verify the claimed identity of a user.
Administrator	A role that performs TOE initialisation and general TOE administrative functions.
Authentication	The process used to verify the claimed identity of a user.
CCRA	Common Criteria Recognition Arrangement
EAL	Evaluation Assurance Level
FIPS 140-2	FIPS-140-2 is the National Institute of Standards and Technology (NIST) technical publication defining cryptography modules standards.
FIPS 180-2	FIPS-180-2 is the National Institute of Standards and Technology (NIST) technical publication defining Secure Hash standards.
FIPS 186-4	FIPS 186-4 defines the Digital Signature Standard (DSS)
FIPS 197	FIPS 197 defines the Advanced Encryption Standard (AES)
FIPS 198-1	FIPS 198-1 defines the Keyed Hash Message Authentication Code (HMAC)
NIST SP 800-67	NIST Special Publication 800-67 defines the Triple Data Encryption

Acronym	Expanded Term
	Algorithm (TDES)
NIST SP 800-90	NIST Special Publication 800-90 describes the NIST Recommendation for Random Number Generation Using Deterministic Random Bit Generators.
NIST SP 800-133	NIST Special Publication 800-133 defines the NIST Recommendation for Cryptographic Key Generation
Root	The administrator (super user) of the underlying Operating Systems, who has unrestricted access to all the TOE resources and functions.
RSA	An algorithm for public-key cryptography published by RSA Laboratories
RSA PKCS #1	PKCS #1 defines the first Public Key Cryptography Standard published by RSA.
RFC 4346	RFC 4346 defines version 1.1 of the Transport Layer Security (TLS) protocol.
RFC 5246	RFC 5246 defines version 1.2 of the Transport Layer Security (TLS) protocol.
Service	A specified function or set of functions implemented by the TOE and accessible to authorised users.
SSH	Secure Shell – network protocol used for cryptographically securing data transmitted between the TOE and external clients.
TLS	Transport Layer Security, used for securing data in transmission between the TOE and external clients.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE
TSC	TOE Scope of Control, the set of interactions that can occur with or within a TOE and are subject to the rules of the TSP
TSP	TOE Security Policy, a set of rules that regulate how assets are managed, protected and distributed.
Unauthorized users	Unauthorized users can mean a legitimate user with access rights to certain web resource, an external entity that has no rights to any protected resource or data.
Web UI	The administrative user interface provided by the TOE for the management of TOE resources and functions.

A.2.2 Glossary of Terms

Table 7: Glossary of Terms

Term	Definition and Source
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
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.
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.
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.

Term	Definition and Source
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

--- END OF DOCUMENT ---