C067 Certification Report

DNSVault Version 4.8

File name: ISCB-5-RPT-C067-CR-v1
Version: v1
Date of document: 25 April 2017
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)

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

Securing Our Cyberspace

C067 Certification Report

DNSVault Version 4.8

25 April 2017

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

DOCUMENT TITLE:	C067 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C067-CR-v1
ISSUE:	v1
DATE:	25 April 2017

DISTRIBUTION: UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright and Confidentiality Statement

Registered office:

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

Registered in Malaysia – 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 10 April 2017 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).

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

Disclaimer

The Information Technology (IT) product identified in this certification report and its associated certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (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	10 April 2017	All	Initial draft of certification report
v1	25 April 2017	All	Final version of certification report

Executive Summary

The TOE is DNSVault management system designed to view, manage and secure DNS services. The TOE provides security functionality such as Security Audit, Identification and Authentication, Security Management, TSF Protection and Secure Communication. The TOE can be categorized as a Network and Network-Related Devices and Systems.

The scope of the evaluation is defined by the Security Target (Ref [6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security 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). 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 CyberSecurity Malaysia MySEF (Malaysia Security Evaluation Facility) and completed on 28th March 2017.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at http://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 the user to ensure that DNSVault version 4.8 meet their requirements. It is recommended that a potential user of the TOE refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Document Authorisation ii

Copyright Statement iii

Foreword iv

Disclaimer v

Document Change Log vi

Executive Summary vii

Table of Contents viii

Index of Tables ix

Index of Figures ix

1 Target of Evaluation 1

1.1 TOE Description 1

1.2 TOE Identification 1

1.3 Security Policy 2

1.4 TOE Architecture 2

1.4.1 Logical Boundaries 3

1.5 Clarification of Scope 4

1.6 Assumptions 4

1.6.1 Usage assumptions 4

1.6.2 Environment assumptions 5

1.7 Evaluated Configuration 5

1.8 Delivery Procedures 5

1.9 Documentation 6

2 Evaluation 7

2.1 Evaluation Analysis Activities 7

2.1.1 Life-cycle support 7

2.1.2 Development 8

2.1.3 Guidance documents 10

2.1.4 IT Product Testing 10

3 Result of the Evaluation 13

3.1 Assurance Level Information 13

3.2 Recommendation 13

Annex A References 15

A.1 References 15

A.2 Terminology 15

A.2.1 Acronyms 15

A.2.2 Glossary of Terms 16

Index of Tables

Table 1: TOE identification 1

Table 2: List of Acronyms 15

Table 3: Glossary of Terms 16

Index of Figures

Figure 1: Physical of TOE the TOE 3

1 Target of Evaluation

1.1 TOE Description

1 The TOE shall be known as DNSVault. This product is a DNS management system; installed in DNSVault Series of appliances (e.g. 2000, 5000 and 10000 series) and has the capability to view, manage and secure DNS services. With the built-in network protection and built-in Load Balancing. The TOE provides advanced DNS management features with an intuitive web console on a high availability platform with real-time disaster recovery capabilities. This allows IT departments to truly provide DNS services in almost zero downtime. Alternatively, the TOE can be used as a tool for managing DNSSEC services on existing DNS network while protecting core DNS services from security threats and service failures.

2 The functionality defined in the Security Target that was subsequently evaluated is as follows:

- Security Audit
  - The Toe generates audit records for security events. The Administrator is the only role with access to the audit trial and has the ability to view all user activities such as the date and time of the event, type of event, subject identity and outcome of the event.
- Identification and Authentication
  - The TOE requires that each user is successfully identified (user ID(and authenticated(password) before any interaction with protected resources is permitted
- Security Management
  - The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to management functions based on the role of the user
- TSF Protection
  - The TOE includes its own time source for providing reliable time stamps that are used in audit records, DNSSEC operation and TSIG operation. The TOE also protects all current sessions from compromise by enforcing a timeout. When a session becomes idle for more than 5 minutes, it will automatically route users to the login page.
- Secure Communication
  - The TOE is able to protect user data from disclosure and modification using SSL as a secure communication between a user’s browser and the TOE.

1.2 TOE Identification

3 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C067
TOE Name	DNSVault
TOE Version	4.8
Security Target Title	DNSVault Security Target v1.0
Security Target Version	Version 1.0
Security Target Date	31 January 2017
Assurance Level	Evaluation Assurance Level 2
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [2])
Methodology	Common Criteria 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 EAL 2
Sponsor	DNSVAULT Sdn Bhd No 29-2, Tingkat 2, Jalan Tukul N15/N, Seksyen 15, 40200 Shah Alam, Selangor, Malaysia
Developer	DNSVAULT Sdn Bhd No 29-2, Tingkat 2, Jalan Tukul N15/N, Seksyen 15, 40200 Shah Alam, Selangor, Malaysia
Evaluation Facility	CyberSecurity Malaysia MySEF (CSM MySEF)

1.3 Security Policy

4 There are no organisational security policies that have been defined regarding the use of the TOE.

1.4 TOE Architecture

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

6 The TOE architecture consists of the following components:

- Database
- Operating System
- Hardware Abstraction Layer (Kernel/BIOS)
- Hardware Access Port

7 The following figure illustrates how the TOE components can be deployed in a network.

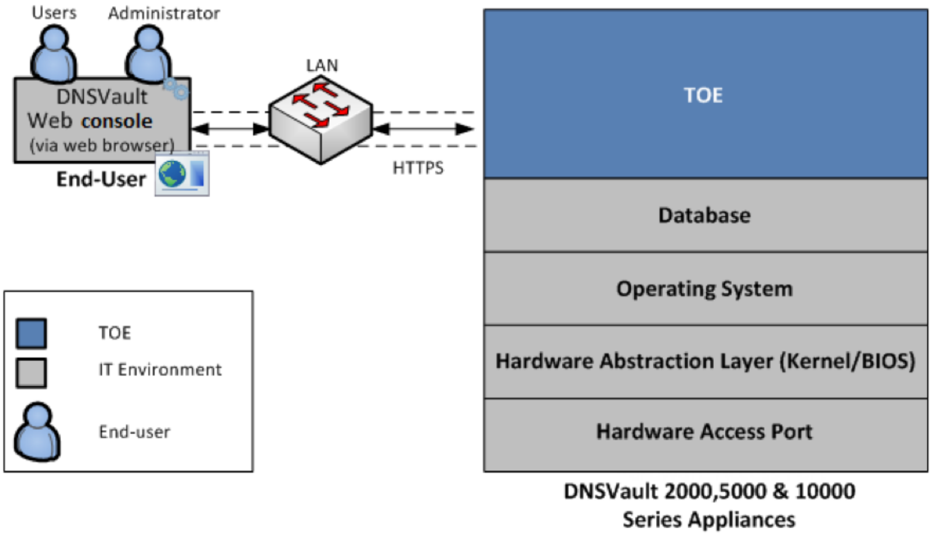
Users
Administrator
DNSVault Web console (via web browser)
End-User
LAN
HTTPS
TOE
Database
Operating System
Hardware Abstraction Layer (Kernel/BIOS)
Hardware Access Port
DNSVault 2000,5000 & 10000 Series Appliances
TOE
IT Environment
End-user

Figure 1: Physical Scope of the TOE

1.4.1 Logical Boundaries

8 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:

- Security audit
- Identification and authentication
- Security Management
- TSF Protection
- Secure Communication

9 **Security audit:** TOE generates audit records for security events. The Administrator is the only role with access to the audit trail and has the ability to view all user activities such as the date and time of the event, type of event, subject identity and outcome of the event.

10 **Identification & Authentication:** All users are required to be identified and authenticated before any information flows are permitted. The TOE checks the credentials presented by the user at the login page against the authentication information stored in the database.

11 **Security Management:** The TOE contains various management functions to ensure efficient and secure management of the TOE. The TOE maintains role-based access control mechanisms to ensure that functions are restricted to those who have the privilege to access them. The Administrator has the privileged to control access to the network. The functions above are restricted based on this role.

12 **TSF Protection:** The TOE includes its own time source for providing reliable time stamps that are used in audit records, DNSSEC operation and TSIG operation. The TOE also protects all current sessions from compromise by enforcing a timeout. When a session becomes idle for more than 5 minutes, it will automatically route user to the login page.

13 **Secure Communication**: The TOE is able to protect user data from disclosure and modification using SSL as a secure communication between a user's browser and the TOE.

1.5 Clarification of Scope

14 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, trained personnel and secure communication in accordance with user guidance that is supplied with the product.

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

16 The following features and capabilities of the TOE described in the guidance documentation are not included within the scope of the evaluation:

- Cryptographic Operation

17 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 requirement for using functions and services outside of the evaluated configuration.

1.6 Assumptions

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

1.6.1 Usage assumptions

19 Assumptions for the TOE usage as listed in the Security Target:

a) It is assumed that the person who manages the TOE is not hostile and is competent.

b) It is assumed that users will keep their passwords secret and not write them down or disclose them to any other system or user. It is also assumed that the user password length is between a minimum of 8 and a maximum of 18 alphanumeric characters.

c) It is assumed that the TOE is patched and hardened to protect against known vulnerabilities and security configuration issues.

d) It is assumed that the web console has valid SSL certificates installed (not revoked or expired) and are sourced from a trusted entity.

1.6.2 Environment assumptions

20 In order to provide a baseline for the IT product during the evaluation effort, certain assumptions about the environment the product is to be used in have to be made. This section documents any environmental assumptions made about the IT product during the evaluation. Assumptions for the TOE environment listed in Security Target are:

a) The TOE will provide appropriate authentication and authorisation controls for all.

b) It is assumed that the TOE are in a secure operating facility with restricted physical access.

1.7 Evaluated Configuration

21 The evaluated configurations is described in details (see Figure 1).

1.8 Delivery Procedures

22 The TOE is delivered as an appliance by an Authorized Representative to the customer. Before the appliance is delivered, the following steps are performed by an Authorized Representative:

- ensuring that the underlying software/hardware platforms meet the required specifications; a schedule is given to customers via email or phone call regarding the delivery of the TOE to allow customer to know when the TOE is expected to be delivered by the Authorized Representative.
- The TOE configuration will be performed by the Authorized Representative. The configuration processes include the TOE configuration, credentials configuration IP address, zone upload and license generation.
- Upon completion of installation and configuration of the TOE, the customer needs to complete the Application Installation Acceptance form & Sign-off

23 The acceptance process for the TOE is as follows:

- Upon acknowledging the receipt for the appliance and the TOE, the customer will cross check the delivery order (DO) with the labelling, appliance part number and the version of the TOE.
- If any problem occurs, the customer can directly approach the Authorized Representative during the setup phase or contact DNSVault Sdn Bhd support via email or phone for guidance.

24 The user may determine the version of the TOE via the methods listed below.

- Upon successful login. At the main page, on the Menu Bar, click Appliance Management. Click on Updates and click the Check button. This will review software update information which is our Product Name and Software version

1.9 Documentation

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

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

- DNSVault Web UI UserGuide v4.8_201701091713
- DNSVault Guidance Documentation v1.0

2 Evaluation

27 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. The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [4]).

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

2.1.1.1 Configuration Management Capability

29 The evaluators confirmed that the TOE provided for evaluation is labelled with its reference.

30 The evaluators confirmed that the TOE references used are consistent.

31 The evaluators examined the method of identifying configuration items and determined that it describes how configuration items are uniquely identified.

32 The evaluators examined the configuration items in the configuration item list and determined that they are identified in a way that is consistent with the CM documentation.

33 The evaluators examined the access control measures described in the CM plan and determined that they are effective in preventing unauthorised access to the configuration items.

34 The evaluators confirmed that the CM documentation provided includes a CM plan.

35 The evaluators examined the CM plan and determined that it describes how the CM system is used for the development of the TOE.

36 The evaluators confirmed that the configuration items identified in the configuration list are being maintained by the CM system.

37 The evaluators checked the CM documentation and confirmed that it includes the CM system records identified by the CM plan.

38 The evaluators confirmed that the CM system is being operated in accordance with the CM plan.

2.1.1.2 Configuration Management Scope

39 The evaluators confirmed that the configuration list includes the following set of items:

- the TOE itself;

- the parts that comprise the TOE;
- the TOE implementation representation; and
- the evaluation evidence required by the SARs in the ST.

40 The evaluators confirmed that the configuration list uniquely identifies each configuration item.

41 The evaluators confirmed that the configuration list indicates the developer of each TSF relevant configuration item.

2.1.1.3 TOE Delivery

42 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

2.1.1.4 TOE Lifecycle Definition

43 The evaluators examined the documented description of the life-cycle model used and determined that it covers the development and maintenance process.

44 The evaluators examined the life-cycle model and determined that use of the procedures, tools and techniques described by the life-cycle model will make the necessary positive contribution to the development and maintenance of the TOE.

2.1.2 Development

2.1.2.1 Architecture

45 The evaluators examined the security architecture description and 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.

46 The security architecture description describes the security domains maintained by the TSF.

47 The initialisation process described in the security architecture description preserves security.

48 The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

2.1.2.2 Functional Specification

49 The evaluators examined the functional specification and determined that:

- the TSF is fully represented,
- it states the purpose of each TSF Interface (TSFI),

- the method of use for each TSFI is given,
- the completeness of the TSFI representation,
- it is a complete and accurate instantiation of the SFRs.

50 The evaluators also examined the presentation of the TSFI and determined that:

- it completely identifies all parameters associated with every TSFI,
- it completely and accurately describes all SFR-enforcing actions associated with every SFR-enforcing TSFI,
- it completely and accurately describes all error messages resulting from an invocation of each SFR-enforcing TSFI,
- it summarises the SFR-supporting and SFR-non-interfering actions associated with each TSFI.

51 The evaluators also confirmed that the developer supplied tracing links the SFRs to the corresponding TSFIs.

2.1.2.3 TOE Design Specification

52 The evaluators examined the TOE design and determined that the structure of the entire TOE is described in terms of subsystems. The evaluators also determined that all subsystems of the TSF are identified. The evaluators determined that interactions between the subsystems of the TSF were described.

53 The evaluators examined the TOE and determined that each SFR-non-interfering subsystem of the TSF was described such that the evaluators could determine that the subsystem is SFR-non interfering.

54 The evaluators found the TOE design to be a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

55 The evaluators examined the TOE design and determined that it provided a complete and accurate high-level description of the SFR-supporting and SFR-non-interfering behaviour of the SFR-enforcing subsystems. The evaluators determined that the TOE design provided a complete and accurate high-level description of the behaviour of the SFR-supporting subsystems.

56 The evaluators determined that the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

57 The evaluators determined that all Security Target SFRs were covered by the TOE design, and concluded that the TOE design was an accurate instantiation of all SFRs.

2.1.3 Guidance documents

2.1.3.1 Operating Guidance

58 The evaluators examined the operational user guidance and determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

59 The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

60 The evaluators examined the operational user guidance (in conjunction with other evaluation evidence and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

61 The evaluators determined that the operational user guidance describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

62 The evaluators found that the operational user guidance is clear and reasonable.

2.1.3.2 Preparation Guidance

63 The evaluators examined the provided delivery acceptance documentation and determined that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

64 The evaluators determined that the provided installation procedures describe the steps necessary for secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST.

65 The evaluators performed all user procedures necessary to prepare the TOE during testing and determined that the TOE and its operational environment can be prepared securely using only the supplied preparative user guidance.

2.1.4 IT Product Testing

66 Testing at EAL2 consists of assessing developer tests, performing independent functional tests, and performs penetration tests. The TOE testing was conducted by evaluators for CyberSecurity Malaysia 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

67 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).

68 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

69 At EAL2, 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 developer's test plan and creating test cases that developer tests.

70 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 developed and performed by the evaluators and are consistent with the expected test documentation.

Test ID	Description	Security Function	TSFI
TEST GROUP A.3 TEST GROUP A.4	Comprises a series of test cases on TOE security functions related to identified and authenticated for administrator	Identification and authentication	Administrator interface
TEST GROUP B.3 TEST GROUP B.4	Comprises a series of test cases on TOE security functions related to identified and authenticated for Pre-defined user	Identification and authentication	User Interface
TEST GROUP C.2 TEST GROUP C.3	Comprises a series of test cases on TOE security functions related to SSL certificate in securing the communication for each User TOE access.	Secure Communication	Network Interface
TEST GROUP D.2 TEST GROUP D.3	Comprises a series of test cases on TOE security functions related Audit data generation and review audit for Administrator.	Security Audit	Administrator Interface
TEST GROUP E.6 TEST GROUP E.7 TEST GROUP E.8 TEST GROUP E.9	Comprises a series of test cases on TOE security functions related to the management configuration, security, and password of TOE for each users.	Security Management	Administrator Interface User Interface
TEST GROUP F.2 TEST GROUP F.3	Comprises a series of test cases on TOE security functions related to the Reliable Time Stamps and Session termination for each users.	TSF Protection	Administrator Interface User Interface

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

2.1.4.3 Penetration Testing

72 The evaluators performed 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, and TOE design and security architecture description.

73 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 (elapsed time);

b) Specialist technical expertise required (specialist 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.

The penetration tests focused on:

a) Scanning

b) Cross Site Scripting (XSS)

c) Sniffing

d) Injection

e) Broken Authentication and session management

f) Brute Force Attack

g) Failure to Restrict URL Access

h) Unvalidated Redirects and forwards

74 The results of the penetration testing note that there is no residual vulnerability found. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in the Security Target (Ref [6]).

2.1.4.4 Testing Results

75 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target (Ref [6]) and its functional specification. In addition, the documentation supplied as evidence for the EAL2 Common Criteria evaluation of the TOE was analyzed to identify possible vulnerabilities.

3 Result of the Evaluation

76 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 DNSVault version 4.8 performed by CyberSecurity Malaysia MySEF.

77 CyberSecurity Malaysia MySEF found that DNSVault 4.8 upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance Level 2 (EAL2).

78 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

79 EAL 2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using a functional and interface specifications, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

80 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 an attacker possessing a Basic attack potential.

81 EAL 2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

82 The following recommendations are made:

a) Developer is recommended to keep on updating the TOE user guide and relevant documentations based on latest information and features updates of the TOE. Additionally, through the new updates released, Developer is recommended to notify their customer on the latest updates, as well as, any changes made on the TOE that related to its security features through any official communication platform. Thus, Consumer/Client is aware about the latest updates and information about the TOE.

b) Consumer/Client is advised to seek any help, assistance or guidance from developer of the TOE if in any cases of specific requirements shall be configured onto the TOE to meet certain policies, procedures and security enforcement within the consumer/client organization; thus, are recommended to seek detailed information directly from the developer. Therefore, there should not be any misconfiguration or malfunctions or insecure operations of the TOE that may affect consumer/client assets that is protected by the TOE.

c) Consumer/Client is advised to ensure that the TOE are applies all the security objective for the environment thus vulnerability will not be exploitable in its operational environment.

d) Developer is recommended to make improvement by adding error message and should have a method to validate URL when a suer is trying to login to web page using manipulate URL/redirect or forward URL to avoid phishing scam and steal user credentials.

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 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), v1d, CyberSecurity Malaysia, February 2016.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1c, February 2016.

[6] DNSVault Security Target, Version 1.0, 31 January 2017

[7] MySEF-3-EXE-E043-ETR-v1, Evaluation Technical Report, Version 1.0, 28 March 2017

A.2 Terminology

A.2.1 Acronyms

Table 2: 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
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 3: 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
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.

Term	Definition and Source
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 ---