C082 Certification Report

Automated Privilege Password Management v4.0.01

File name: ISCB-5-RPT-C082-CR-v1
Version: v1
Date of document: 24 November 2017
Document classification: PUBLIC

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

CyberSecurity Malaysia
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999
www.cybersecurity.my

C082 Certification Report

Automated Privilege Password Management v4.0.01

24 November 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:	C082 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C082-CR-v1
ISSUE:	v1
DATE:	24 November 2017

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

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 24 November 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).

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	8 November 2017	All	Initial draft of certification report
v1	9 November 2017	All	Final version of certification report

Executive Summary

Automated Privilege Password Management (APPM) is the Target of Evaluation (TOE) for the Common Criteria Evaluation Assurance Level 2 evaluation. The Target of Evaluation (TOE), APPM is a solution to manage the issuance of One Time Password access credentials and permissions on Unix servers, Linux servers, Windows servers, network devices and other relevant applications for the assigned/registered privileged accounts in these stated components.

APPM is an appliance based password management software that manage access credentials (e.g. username and password) for connected system as such servers, network appliance and relevant IT components through trusted connecting networks.

With the multiple options or permutations available in the above implementation, the APPM enables the organization to manage the overall security through a single framework that enables the defining and assignment or implementation based on these following security functions in one system:

a) Security Audit;
b) User Data Protection;
c) Authentication and Identification; and
d) Security Management;

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2) 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 Across Verticals MySEF (Malaysia Security Evaluation Facility) and completed on 20 October 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 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 APPM v4.0.01 meets their requirements. It is recommended that a potential user of Automated Privilege Password Management v4.0.01 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

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE), Automated Privilege Password Management (APPM) is a solution to manage the issuance of One Time Password access credentials and permissions on Unix servers, Linux servers, Windows servers, network devices and other relevant applications for the assigned/registered privileged accounts in these stated components.

2 APPM enables enterprise to authorise users through the integrated workflow and manage the passwords automatically. By implementing the APPM solution, enterprise able to enforce password associated security compliance. In addition, it shall improve the security of password protection by removing the hard-coded password stored in the script. Furthermore, by having a 3rd backup mechanism through secured USB, provides fast recovery, and prevent a password loss from any system failure.

3 In traditional implementations, clients or customers will need to have different access credentials (e.g. usernames and password) to different products or systems and the management of these separate application accesses can be an administrative burden. This also can lead to unnecessary exposure to security leakages if accesses to different systems that are linked or integrated are not implemented according to a consistent policy.

4 With the multiple options or permutations available in the above implementation, the APPM enables the organization to manage the overall security through a single framework that enables the defining and assignment or implementation based on these following security functions below.

5 The details of TOE security functions can be found in section 1.6.2 of the Security Target (Ref[6])

6 There are four (4) security functionalities covered under the scope of evaluation which are:

a) Security Audit: The TOE will generate audit records for selected security events in several log files and categories. Each audited event will be recorded along with date and time of event, user accounts that performed the event, event name and other event details.

b) Authentication and Identification: All TOE Administrator (Super User) must have a valid username/user ID inclusive of password to access and OTP. TOE Administrator (Super User) must login to APPM to manage all the connected devices (IT entities) as well as credentials of accessing these IT entities. Thus, configurations of these IT entities required to be registered in the APPM system, plus configuration policy of managing the access credentials of the IT entities shall be defined.

c) User Data Protection: User data and credentials including TOE Administrator (Super User) information is protected by ensuring that specific TOE Administrator (Super User) that is assigned with roles and privilege scan only access specific

web pages/portals and hence the data associated with the web pages/portal. The accessibility of the pages/portals is protected based upon the access control policy.

d) Security Management: TOE Administrator (Super User) has access to all TOE features, that applicable to be managed through web application portal hosted by TOE. TOE is able to provide accessibility of account that has access privilege, similar or limited, to "Super User" account. In which, Super User account has the full access rights, role and privileges to the TOE.

1.2 TOE Identification

7 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	C082
TOE Name	Automated Privilege Password Management
TOE Version	V4.0.01
Security Target Title	SECUREKi APPM Security Target
Security Target Version	0.5
Security Target Date	2 October 2017
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
Sponsor and Developer	SecureKi Sdn Bhd DF2-09-03A (Unit No.2), Level 9, Persoft Tower, Persiaran Tropicana,
Evaluation Facility	Across Verticals MySEF

1.3 Security Policy

8 There are two (2) organisational security policies that have been defined regarding the use of the TOE.

Table 2: Organizational Security Policies

OSP	Description
P.ROLE	Only authorized persons assigned by the organization have access to the TOE.
P.PASSWORD	Authorized administrator shall use password with combination of special character, number and alphabet with minimum lengths of 12 to make it hard to guess.

1.4 TOE Architecture

9 The TOE includes both logical and physical boundaries, which are described in Section 1.6.1 and 1.6.2 of the Security Target (Ref [6]).

10 The following figure 1 shows the evaluated configuration that comprise the TOE:

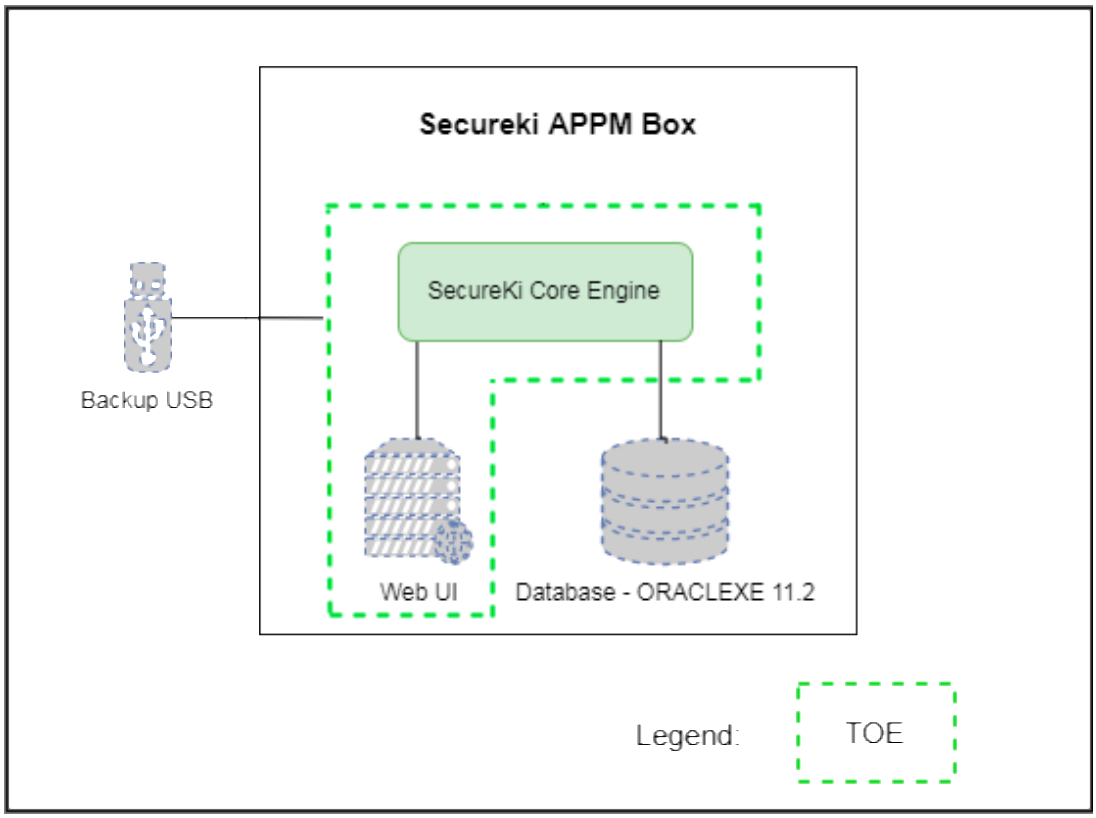

Figure 1: TOE boundary and subsystems

1.4.1 Logical Boundaries

11 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:

a) Security Audit: The TOE will generate audit records for selected security events in several log files and categories. Each audited events will be recorded along with date and time of event, user accounts that performed the event, event name and other event details. Audit records can be viewed by TOE Administrator (Super User) and cannot be edited. TOE Administrator (Super User) could select and filter the logs for easy viewing. TOE will create a new log file and may overwrite the old audit log records to store the audit records if the size limit is reached for a log file. Limitation of the log storage is based on the internal hard disk equipped within the TOE hardware server. Note that, TOE Administrator (Super User) shall be advice to backup all logs that is crucial to the TOE operational environment in accordance to organizational security policies in protecting the logs from any damages or tampering or loss.

   The security audit function ensures that all TOE Administrator (Super User) activities pertaining to creation/update/delete of TOE Administrator (Super User), as well as the assigning TOE Administrator (Super User) roles and privilege accessibilities shall be log by audit functions. Details of audit logs and management of audit components are being explained in the Guidance documentations. Types of logs and descriptions of logs are described in details at TOE Summary Specification (TSS).

b) Identification and Authentication: All TOE Administrator (Super User) must have a valid username/user ID inclusive of password to access and OTP. The OTP is not part of the scope of the TOE. Accessibility mechanism to the TOE is included inside the scope of the TOE. TOE Administrator (Super User) must login to APPM to manage all the connected devices (IT entities) as well as credentials of accessing these IT entities. Thus, configurations of these IT entities required to be registered in the APPM system, plus configuration policy of managing the access credentials of the IT entities shall be defined. Whilst, each access credentials that managed by the APPM system is been monitor through policy defined enforcement through the applied configuration made by the TOE Administrator (Super User).

   In aspects of access control and session established upon authentication and identification, each TOE Administrator (Super User) are given a known configure value of idle mode, in which the value is configurable. This feature is configurable based on the policies defined by the organization security policies. If a login session has remained idle for a certain value that are been configure, such e.g. in 20 minutes, the TOE Administrator (Super User) will have to re-login to access the application again.

c) Security Management: TOE Administrator (Super User) has access to all TOE features, that applicable to be managed through web application portal hosted by TOE. TOE is able to provide accessibility of account that has access privilege, similar or limited, to “Super User” account. In which, Super User account has the full access rights, role and privileges to the TOE. TOE Administrator (Super User) could enable, disable and modify the behaviour of services controlled by TOE, user attribute values, network settings, time-of-day web access, NTP Time Server, backup and restore configurations setting and related functions of TOE.

   Nonetheless, there are another 3 roles that are allows to access the TOE features, which is: Auditor, General User and Helpdesk. These roles are defined with limited access to the TOE features compared to the TOE Administrator (Super User).

d) User Data Protection: User data and credentials including TOE Administrator (Super User) information is protected by ensuring that specific TOE Administrator (Super User) that is assigned with roles and privilege scan only access specific web pages/portals and hence the data associated with the web pages/portal. The accessibility of the pages/portals is protected based upon the access control policy.

The access control policy allows the TOE Administrator (Super User) to create username/user of the users that is assigned to access the TOE.

TOE has the capabilities of enforcing protection upon resources that the TOE protected, by implementing access control protection on authentication and identification webpage (login page) through access control policy. The TOE will check for legitimate access control credentials such as username/user ID and password/PIN before allowing such credentials to access the web applications portal protected by the TOE. TOE Administrator (Super User) could manage and configure access control policy and privilege access control, are defined to specific user account accessibility. By default, users without any access control credentials are not allowed to access the protected resources. There is also an information flow policy to control the control the information flow between the subjects and controlled information via controlled operations.

1.4.2 Physical Boundaries

12 The TOE includes both logical and physical boundaries, which are described in Section 1.6.1 and 1.6.2 of the Security Target (Ref [6]).

1.5 Clarification of Scope

13 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 the user guidance supplied with the product.

14 Section 1.5.3 of the Security Target describes the scope of the evaluation which was limited to those claims made in the Security Target (Ref [6]).

15 Potential consumers of the TOE are advised that some functions and services of the overall product have not been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

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

1.6.1 Usage assumptions

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

a) Authorized administrators are non-hostile and following the guidance.

1.6.2 Environment assumptions

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

a) The TOE and its environment are physically secure.
b) The TOE environment will provide reliable time stamps and backup space.

c) The TOE environment will provide a secure connection between TOE and users.

1.7 Evaluated Configuration

19 The evaluated configuration is according to the Preparative Guidance.

20 The TOE is delivered as an appliance by the developer to the customer, the TOE will be in inactive state where it will have a factory default IP settings. TOE Administrator (Super User) will use the default IP address using SSH connection to access the APPM Admin Console or Admin Utility menu. Once successfully authenticated, TOE Administrator can invoke the admin menu using command "admin" and configure the relevant configurations of TOE such as eth1 and gateway IP address.

21 After each boot or if stopping the services, file system shall be mount by TOE Admin through APPM Admin Console. Then, TOE Admin shall run the database, web application and APPM Process.

SSH Key is also generated for establishing secure communication with target connected systems. Encryption key for users' password backup encryption and decryption is also setup. Only then, TOE will be in its initial secure state.

TOE Administrator shall access the web console using the configured IP address with initial login user account and password.

22 Protection from Tampering:

a) Physical Protection: APPM appliance sealed with a security tape at the APPM casing to avoid product being tampered during distribution to the customer. If the security tape is broken, unauthorized person may have tampered the TOE. APPM appliance shall be located in a physically secure facility to ensure unauthorized access prevented.

b) Logical: Apart from physical protection, TOE Administrator able to run "Integrity Check" to check the integrity policy of the APPM file system and database for the service processes using the APPM Admin console. If the integrity checking failed, TOE Administrator shall update the APPM patching to update the changes of the new integrity information.

23 Protection from Bypassing: TSF ensures that the security functionality is always invoked and hence, with the self-protection (as described earlier in this document) and correct functional behaviour (as described in the FSP/TDS/ATE evaluation evidence), the SFRs are always enforced.

TOE is not by passable dependent on trusted path HTTS for web console access and SSH for remote access. The communication is encrypted throughout the session establishment.

1.8 Delivery Procedures

24 The delivery process will be performed by SECUREKi personnel in maintaining security when distributing APPM to the customer as stated below:

a) Procurement by customer: The customer will purchase the product and complete the payment. Once payment is confirmed and legal documentations have been completed, SECUREKi personnel can proceed with preparing and delivering the

product.;

b) Preparing the delivery package: SECUREKi personnel will make the necessary preparation:

i. Prepare the User Guide document for APPM.
ii. Label the APPM appliance with APPM identification and serial number.
iii. Apply security tape at the APPM casing to avoid the product being tampered during distribution to customer.
iv. The product will be hand-delivered to customer

c) Receipt and Verification: Once the package is delivered, the customer is expected to perform the following measures:

i. Receive the package.
ii. Acknowledge received items receipt.

25 SECUREKi personnel will keep the Acknowledge received items as proof of product receipt. Acceptance of product will be based on customer's selection of product functionalities.

1.9 Documentation

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

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

[1]. SecureKi APPM Administrator's Guide, v3.0.8

[2]. SecureKi APPM Tech Training, v4.0

[3]. SecureKi APPM Configuration Management, v0.1

[4]. SecureKi Delivery Procedure, v0.1

2 Evaluation

28 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). 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

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

2.1.1 Life-cycle support

30 The evaluators checked that the TOE provided for evaluation is labelled with its reference.

31 The evaluators checked that the TOE references used are consistent.

32 The evaluators examined the method of identifying configuration items to determine that it describes how configuration items are uniquely identified.

33 The evaluators examined the configuration items to determine that they are identified in a way that is consistent with the CM documentation.

34 The evaluators checked that the configuration list includes the

a) the TOE itself;

b) the parts that comprise the TOE;

c) the evaluation evidence required by the SARs

35 The evaluators examined the configuration list to determine that it uniquely identifies each configuration item.

36 The evaluators checked that the configuration list indicates the developer of each TSF relevant configuration item.

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

38 The evaluators examined aspects of the delivery process to determine that the delivery procedures are used.

2.1.2 Development

39 The evaluators examined the functional specification to determine that the TSF is fully represented, it states the purpose of each TSFI and the method of use for each TSFI is given.

40 The evaluators examined the presentation of the TSFI to determine that it completely identifies all parameters associated with every TSFI.

41 The evaluators examined the presentation of the TSFI to determine that it completely and accurately describes all parameters associated with every TSFI.

42 The evaluators examined the presentation of the TSFI to determine that it completely and accurately describes the SFR-enforcing actions associated with the SFR-enforcing TSFIs.

43 The evaluators examined the presentation of the TSFI to determine that it completely and accurately describes error messages that may result from SFR-enforcing actions associated with each SFR-enforcing TSFI.

44 The evaluators checked that the tracing links the SFRs to the corresponding TSFIs.

45 The evaluators examined the functional specification to determine that it is a complete and accurate instantiation of the SFRs.

46 The evaluators examined the security architecture description to determine 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 document.

47 The evaluators examined the security architecture description to determine that it describes the security domains maintained by the TSF.

48 The evaluators examined the security architecture description to determine that the initialisation process preserves security.

49 The evaluators examined the security architecture description to determine that it contains information sufficient to support a determination that the TSF is able to protect itself from tampering by untrusted active entities.

50 The evaluators examined the security architecture description to determine that it presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

51 The evaluators examined the TOE design to determine that the structure of the entire TOE is described in terms of subsystems and all subsystems of the TSF are identified.

52 The evaluators examined the TOE design to determine that each SFR-supporting or SFR-non-interfering subsystem of the TSF is described such that the evaluator can determine that the subsystem is SFR-supporting or SFR-non-interfering.

53 The evaluators examined the TOE design to determine that it provides a complete, accurate, and high-level description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

54 The evaluators examined the TOE design to determine that interactions between the subsystems of the TSF are described.

55 The evaluators examined the TOE design to determine that it contains a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

56 The evaluators examined the TOE security functional requirements and the TOE design, to determine that all ST security functional requirements are covered by the TOE design.

57 The evaluators examined the TOE design to determine that it is an accurate instantiation of all security functional requirements.

2.1.3 Guidance documents

58 The evaluators examined the operational user guidance to determine 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.

59 The evaluators examined the operational user guidance to determine that it describes, for each user role, the secure use of the available interfaces provided by the TOE.

60 The evaluators examined the operational user guidance to determine that it describes, for each user role, the available security functionality and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

61 The evaluators examined the operational user guidance to determine that it 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.

62 The evaluators examined the operational user guidance and other evaluation evidence to determine that the guidance identifies all possible modes of operation of the TOE (including, if applicable, operation following failure or operational error), their consequences and implications for maintaining secure operation.

63 The evaluators examined the operational user guidance to determine that it 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.

64 The evaluators examined the operational user guidance to determine that it is clear and it is reasonable.

2.1.4 IT Product Testing

65 Testing at EAL2 consists of assessing developer tests, performing independent functional tests, and performing penetration tests. The TOE testing was conducted by evaluators from Across Verticals MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Report.

2.1.4.1 Assessment of Developer Tests

66 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).

67 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

68 At EAL2, independent functional testing is the evaluation conducted by evaluators 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 augment developer tests.

69 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The evaluators confirmed that the developer supplied test documentation includes test plans, expected test results and actual test results. The results of the independent functional tests that were developed and performed by the evaluators are consistent with the expected test results in the test documentation.

Table 3: Test results

Test Title	Status	Descriptions
AVCC001-F001	PASS	This test aims to verify that the TOE able to generate an audit record of the auditable events. In additional, the TOE able to associate each auditable event with the identity of the user that caused the event.
AVCC001-F002	PASS	This test aims to verify that the TOE allows only administrator and whoever has been granted explicit read-access to read all the audit records.
AVCC001-F003	PASS	This test aims to verify that the stored audit records in the audit trail are protected from unauthorised deletion.
AVCC001-F004	PASS	The test aims to verify the security attributes stored belonging to valid users.
AVCC001-F005	PASS	This test aims to verify that TOE requires each user to be successfully authenticated before allowing the user to perform any other TSF-mediated actions such as below: Super User – View the APPM dashboard, Manage APPM users, Manage APPM user password policy, Manage the password for all the connected servers, view audit log. Auditor – View Report and view audit log. General User – Request password of connected servers Helpdesk – Manage APPM users
AVCC001-F006	PASS	This test aims to verify that TOE requires each user to be successfully identified before allowing the user to perform any other TSF-mediated actions such as below: Super User – View the APPM dashboard, Manage APPM users, Manage APPM user password policy, Manage the password for all the connected servers, view audit log. Auditor – View Report and view audit log. General User – Request password of connected servers Helpdesk – Manage APPM users All these actions will be logged under the particular user name whoever performed the action.
AVCC001-F007	PASS	This test aims to verify that TOE enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

Test Title	Status	Descriptions
		a) Authentication and Identification shall be enforced upon TOE Administrator when accessing TOE; and b) TOE Administrator shall use APPM Web GUI accordingly upon authentication and identification processes as per requested by TOE. c) The configuration of TOE can only be modified by TOE administrator.
AVCC001-F008	PASS	The test aims to ensure that TOE shall enforce the access control policy, information flow control policy and able to perform the following management functions such as create, delete and update account, create, delete and disable management of other types of data, view logs of all activities, and centralize management.
AVCC001-F009	PASS	The test aims to ensure that TSF able to maintain and associate the user roles
AVCC001-F010	PASS	The test aims to ensure that TOE able to enforce the access control policy to restrict the ability to manage user credential to TOE Administrator only
AVCC001-F011	PASS	This test aims to verify that TOE will enforce the access control policy to provide permissive default values for security attributes that are used to enforce the SFP and TOE administrator is allowed to specify alternative initial values to override the default values when an object or information is created.

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

2.1.4.3 Penetration Testing

71 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.

72 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks 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.

73 The penetration tests focused on:

a) Injection

b) Broken Authentication and Session Management

c) Cross-Site Scripting (XSS)

d) Insecure Direct Object References

e) Security Misconfiguration

f) Sensitive Data Exposure

g) Missing Function Level Access Control

h) Cross-Site Request Forgery (CSRF)

i) Using Components with Known Vulnerabilities

74 The results of the penetration testing noted that there was 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 the Security Target and its functional specification. In addition, the documentation supplied as evidence for the EAL2 Common Criteria evaluation of the TOE was analysed 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 Automated Privilege Password Management v4.0.01 performed by Across Verticals MySEF.

77 Across Verticals MySEF, found that Automated Privilege Password Management v4.0.02 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).

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 EAL2 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.

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 EAL2 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) The TOE users are recommended to keep on updating, maintaining, backing up configuration, logs and related data/files of the TOE, auditing the security enforcing rules of the TOE and performing checks on the TOE regularly to maintain its secure operational environment.
b) A strict adherence to guidance documentations and procedures provided by the developer are highly recommended.
c) The TOE users should be aware and implement available security or critical updates related to the TOE security features and its supporting hardware, software, firmware or relevant guidance documents.
d) Users are advice to seek assistance or guidance directly from the developer of the TOE if specific requirements shall be configured or implemented by the TOE to meet certain policies, procedures and security enforcement within the users' organization. This is important in order to reduce operational error, misconfiguration, malfunctions or insecure operations of the TOE that may compromise the confidentiality, integrity and availability of the assets that is

protected by the TOE.

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, 26 February 2016.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1c, 26 February 2016.

[6] SECUREKi APPM Security Target, Version 0.5, 2 Oct 2017

[7] Evaluation Technical Report v.12, AVCC001-ETR-1.0, 20 Oct 2017

A.2 Terminology

A.2.1 Acronyms

Table 2: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
TSF data	Data created by and for the TOE, which might affect the operation of the TOE.
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
TSFI	TOE Security Functions Interface
SFR	Security Functional Requirement
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

Acronym	Expanded Term
MySEF	Malaysian Security Evaluation Facility
CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
APPM	Automated Privilege Password Management
NTP	Network Time Protocol
OSP	Organizational Security Policy
SSH	Secure Shell

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

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

--- END OF DOCUMENT ---