C058 Certification Report

SmartData v1.4.0.0

File name: ISCB-5-RPT-C058-CR-v1
Version: v1
Date of document: 28 January 2015
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)
Corporate Office:
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

C058 Certification Report
SmartData v1.4.0.0

28 January 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

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 29 January 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).

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	16 January 2015	All	Initial draft of certification report.
v1	25 January 2015	All	Final

Executive Summary

SmartData v1.4.0.0 from Smart Consult Solutions Sdn Bhd is the Target of Evaluation (TOE) for the Evaluation Assurance Level 2 (EAL2) evaluation.

SmartData is an engine for a web application that tracks and manages security items in a production environment. The TOE provides security functionality such as access control, identification and authentication, Cryptographic Operation, security management and secure communication.

It keeps track of the quantity of the security item(s) from warehouse (processing place for all the raw materials of the security item(s)) until it becomes a final product. The system is able to keep track of the security item(s) within the boundary of the warehouse (during processing of raw materials), within the process of delivery of the security item(s), production status and security item status. These process flow and monitoring systems by the TOE is operate with the integration of the production machine.

The scope of evaluation covers major security features as follow:

a) Security Audit: The TOE generates audit records for security events. The Superuser is the only roles with access to the audit trail and has the ability to view the audit log in either pdf or csv files.

b) Identification and authentication: The TOE requires that each user is successfully identified (user IDs) and authenticated (password) before any interaction with protected resources is permitted.

c) Cryptographic Operation: The TOE supports TDES (192 bits) and Rijndael encryption (128 bits) method to protect against disclosure.

d) Security Management: The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.

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

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). 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 MySEF CyberSecurity Malaysia evaluation facility and completed on 22 December 2014.

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 SmartData meet their requirements. It is recommended that a potential user of SmartData 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

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE), is SmartData version 1.4.0.0 (hereafter referred as SmartData) is an engine for a web application that tracks and manages security items in a production environment. It keeps track of the quantity of the security item(s) from warehouse (processing place for all the raw materials of the security item(s)) until it becomes a final product. The system is able to keep track of the security item(s) within the boundary of the warehouse (during processing of raw materials), within the process of delivery of the security item(s), production status and security item status. These process flow and monitoring systems by the TOE operates with the integration of the production machine.

2 The TOE contains 6 system modules, which are MRP, OMM, VMM, PPM, QCM and Settings. The system module(s) can be configured to operate as a single function separately (MRP, OMM, VMM, PPM and QCM) in one server. Each system module controls, manage, monitor and enforce data protection on all information related to the security item(s) from being removed in the production environment unintentionally. Furthermore, the system is able to generate product information in an encrypted format and applied it in a secure packaging for delivery processes.

3 The details of TOE functions can be found in section 1.6 of the Security Target version 1.1.

4 There are five security functionalities covered under the scope of the evaluation which are:

a) Security Audit: The TOE generates audit records for security events. The superuser is the only roles with access to the audit trail and has the ability to view the audit log in either pdf or csv files.

b) Identification and authentication: The TOE requires that each user is successfully identified (user IDs) and authenticated (password) before any interaction with protected resources is permitted.

c) Cryptographic Operation: The TOE supports TDES (192 bits) and Rijndael encryption (128 bits) method to protect against disclosure.

d) Security Management: The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.

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

1.2 TOE Identification

5 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	C058
TOE Name	SmartData
TOE Version	1.4.0.0
Security Target Title	SmartData v1.4.0.0 Security Target
Security Target Version	1.1
Security Target Date	24 Nov 2014
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
Sponsor and Developer	Smart Consult Solutions Sdn Bhd B-1-03, 04 & 05, SME Technopreneur Centre 1, 2270, Jalan Usahawan 2, 63000 Cyberjaya , Selangor , Malaysia
Evaluation Facility	CyberSecurity Malaysia MySEF (CSM MySEF)

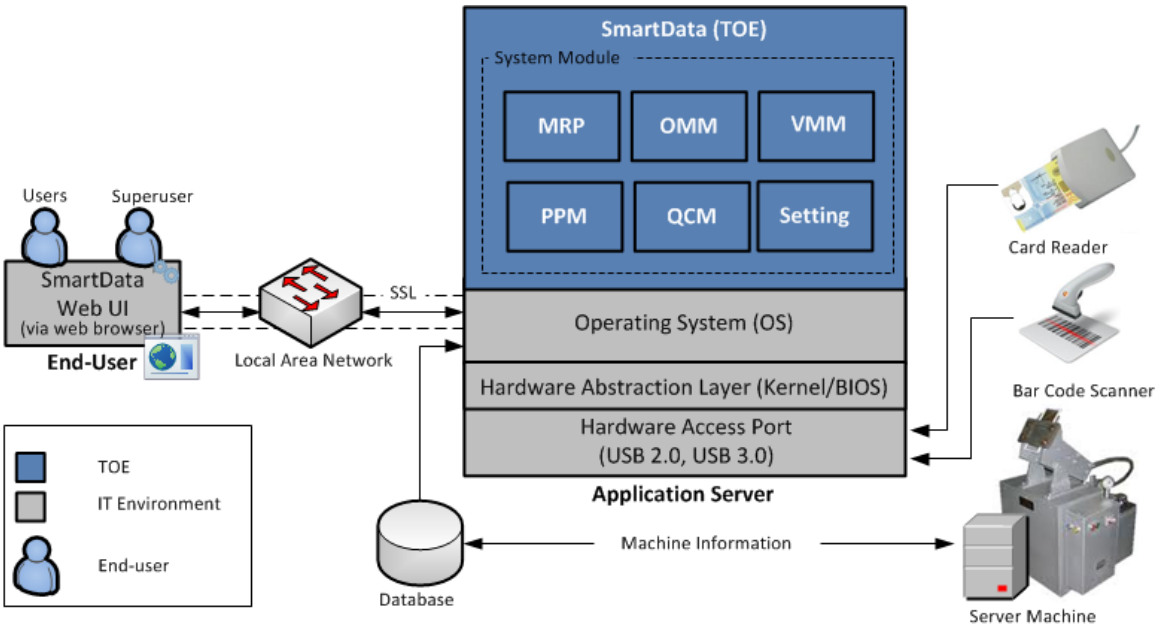
1.3 Security Policy

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

1.4 TOE Architecture

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

8 The following figure 1 shows the subsystems that constructs the TOE:



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:

a) Security Audit: The TOE generates audit records for security events. The superuser is the only roles with access to the audit trail and has the ability to view the audit logs.

b) Identification and authentication: All users are required to be identified and authenticated before any information flows are permitted. The TOE checks the credentials (username and password) presented by the user at the login page against the authentication information stored in the database. Additionally, superuser or permissible users must be authenticated before performing any administrative functions.

c) Cryptographic Operation: The TOE provides a cryptographic library that utilizes the following cryptographic algorithms/functions:

   i. TDES (192 bit keys) – The TOE uses TDES key to encrypt the delivery order (DO) data. The system module OMM has the functionality to encrypt the delivery order (DO) data.

   ii. Rijndael Encryption (128 bit keys) – The TOE uses Rijndael encryption to encrypt user password and store it in the database.

d) Security Management: The TOE contains various management functions or modules to ensure efficient and secure management of the TOE. The license key determines the module users can access on SmartData. The license key only allows addition of new modules but not removal of modules. The TOE maintains role-based access control mechanisms to ensure that functions are restricted to those

who have the privilege to access them. The superuser has the ability to create users roles, assigning access privilege to user for specific functions. The functions above are restricted based on this role.

e) Secure Communication: The TOE supports secure communications between the TOE and user's browser in order to authenticate users and access the TOE functionality. Encryption using SSL prevents modification and disclosure of this information.

1.4.2 Physical Boundaries

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

1.5 Clarification of Scope

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

12 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 an engine for a web application that tracks and manages security items in a production environment. The TOE was made to increase the level of monitoring on security items in a production environment by providing an end-to-end monitoring solution. The TOE is suited for use in a close network environment (ad-hoc/intranet) or open environment (hosted at DMZ) as the system is deployed using secure communication via TLS/SSL.

13 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

14 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

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

a) It is assumed that the superuser 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.

c) It is also assumed that the user password is between a minimum of 6 and a maximum of 30 alphanumeric characters.

1.6.2 Environment assumptions

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

a) The TOE environment will provide appropriate authentication and authorisation controls for all users in the underlying environment (including the database, network, operating system and Application Server).

b) It is assumed that the underlying operating system, application server and database are patched and hardened to protect against known vulnerabilities and security configuration issues.

c) It is assumed that the servers hosting the application and database servers are in a secure operating facility with restricted physical access and non-shared hardware.

1.7 Evaluated Configuration

17 The TOE is an engine for a web application that manages and tracks the security items in a production environment and shall be installed in a dedicated host server running on compatible Windows Operating System as described in Section 1.6 of the Security Target (Ref [6]).

1.8 Delivery Procedures

18 The delivery process for the TOE is as follows:

a) Customers must request the delivery order of a Smartdata. Orders are never sent without being requested.

b) When the order is taken, the customer will receive the encrypted release note by email for the release information (Product Name, version and customer name.

c) Customers will exchange their public keys with Datasonic's representative for encryption purposes.

d) A compressed and encrypted archive containing the Smartdata installer ISO is produced by Datasonic and will be burned into a physical media (CD).

e) The CD will then be sealed in an envelope and sent to the customer.

f) Verify the sealed envelope. If the seal on the envelope are damaged or removed, the TOE installer may have been tampered with.

g) Contact Datasonic if there is any suspicion that tampering has occurred.

h) Datasonic will perform the installation for the customer. After completion of installation the developer will create a superuser role account for the customer's administrative purposes. Then the username and password will be emailed to the customer. This section is of particular importance, as it provides a baseline for the evaluated product delivery procedures.

1.9 Documentation

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

20 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) SmartData Development Installation Guide, v0.2, 10 October 2014

b) SmartData Error Message and Warning, v0.3, 21 November 2014

c) SmartData Operation Manual, v0.5, 21 November 2014

2 Evaluation

21 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

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

2.1.1 Life-cycle support

23 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.

24 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

25 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).

26 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.

27 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

28 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

29 Testing at EAL2 consists of assessing developer tests, perform independent function test, and perform penetration tests. The TOE testing was conducted by evaluators from CyberSecurity Malaysia MySEF (CSM 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

30 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).

31 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

32 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 the developer's test plan, and creating test cases that augmented developer tests.

33 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:

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULTS
Test Group A To test on how TOE identifies and authenticates user through the enforcement of username and password management in the system, which falls under the scope of Authentication and Identification	• FIA_UID.2, • FIA_UAU.2 • FCS_COP.1b	Superuser Interface USER Interface	**PASS**. Result as expected.

Test Group B To test on how TOE manage user accounts in the system, which falls under the scope of Security Management	• FMT_SMF.1	Superuser Interface	**PASS**. Result as expected.
	• FMT_MSA.1 • FMT_SMR.1 • FMT_MTD.1a • FMT_MTD.1b • FDP_ACC.1 • FDP_ACF.1	Superuser Interface USER Interface	
Test Group C To test on how TOE protects against disclosure using encryption method and also verify the encryption standard that has been used, which falls under the scope of Cryptographic Operation.	• FCS_CKM.1a • FCS_COP.1a	Superuser Interface USER Interface	**PASS**. Result as expected.
	• FCS_CKM.1b • FCS_COP.1b	Superuser Interface	
Test Group D To test on how TOE tracks the events performed inside the TOE bound to the user accounts and tracks the system transactions through audit log management, which falls under the scope of Security Audit.	• FAU_GEN.1	Superuser Interface USER Interface	**PASS**. Result as expected.
	• FAU_SAR.1	Superuser Interface	
Test Group E To test on how TOE communicates in the system, which falls under the scope of Secure Communication.	• FTP_TRP.1 • FCS_CKM.1c	Superuser Interface USER Interface	**PASS**. Result as expected.

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

2.1.4.3 Penetration Testing

35 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.

36 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.

37 The penetration tests focused on:

a) Identification of Common Vulnerabilities

b) Network Packet Sniffing on the Communication Transaction between TOE and TOE

c) SQL Injections

d) Cross Site Scripting (XSS

e) Broken Authentication & Session Management

f) Password Attack

g) Directory Traversal

38 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 1.5.3 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

39 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

40 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 SmartData v1.4.0.0 performed by CyberSecurity Malaysia MySEF.

41 CyberSecurity Malaysia MySEF, found that SmartData v1.4.0.0 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).

42 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

43 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.

44 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.

45 EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

46 Opinions and interpretations expressed herein are outside the scope of SAMM accreditation.

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 are recommended to update 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 are advise to seek any help, assistance or guidance from developer of the TOE if in any cases of specific requirements shall be configure onto the TOE to meet certain policies, procedures and security enforcement within the consumer/client organization; thus, are recommended to seek details 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.

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] SmartData v1.4.0.0 Security Target, v1.1, 24 November 2014

[7] E037 Evaluation Technical Report for SmartData v1.4.0.0, v1, 6 January 2015

A.2 Terminology

A.2.1 Acronyms

Table 2: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
Authentication Data	It is information used to verify the claimed identity of a user.
ACL	Access control lists
Java EE	Java Platform Enterprise Edition
RDBMS	Relational database management system
TDES	Triple DES is the common name for the Triple Data Encryption Algorithm symmetric-key block cipher, which applies the Data Encryption Standard cipher algorithm three times to each data block.
TSF data	Data created by and for the TOE, which 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.

Acronym	Expanded Term
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.
Users	It means any entity (human user or external IT entity) outside the TOE that interacts with the TOE. In this case, there are users of the TOE access the TOE through a web browser.
User data	Data created by and for the user, which does not affect the operation of the TSF.
Audit records	An individual item of information contained in an audit trail
Rijndael	A key for encryption that has a size of 128, 192 or 256 bits, which provides high protection against brute force attacks
MRP	Material Requirement Planning. This module provides function for production product preparation. It allow user to customize the raw material needed, production process to produce a final product and manage the Job in production environment.
OMM	Order Management Module. This module provides function to purchase raw material until delivery order to the customer.
VMM	Vault Management Module. This module provides all the stock movement and information in warehouse and in production.
PPM	Production Process Module. This module provides information capture from the machine and production information from each process
Work center	Work center is an operation room that contain production process in a factory. The work center may or may not contain any machine.
QCM	Quality Control Module. This module provides different QC checking state, Incoming QC, In Production QC and Quality Assurance checking of the product
Security Items	Security items can be defined as number of chips, passport data page and raw cards
Barcode Fonts	Storing numbers printed in a way that a computer can easily read
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)

Acronym	Expanded Term
CCRA	Common Criteria Recognition Arrangement
EOR	Evaluation Observation Report
GUI	Graphical User Interface
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
SAMM	Skim Akreditasi Makmal Malaysia
SFR	Security Functional Requirement
RAID	Redundant Array of Independent Disk
CLI	Command Line Interface
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

Term	Definition and Source
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.
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 ---