CyberSecurity MALAYSIA
An agency under MOSTI

People First, Performance Now

MOSTI
Ministry of Science, Technology and Innovation

C050 Certification Report

SCAN S3 Security Manager Console Release 14556 (v2.0) integrated with SCAN S3 Agent (v2.0.1.6.2)

File name: ISCB-5-RPT-C050-CR-v1
Version: v1
Date of document: 9 July 2014
Document classification: PUBLIC

Malaysian Common Criteria Evaluation & Certification Scheme
MyCC

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

Securing Our Cyberspace

CyberSecurity Malaysia
(726630-U)

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

C050 Certification Report

SCAN S3 Security Manager Console Release 14556 (v2.0) integrated with SCAN S3 Agent (v2.0.1.6.2)

23 June 2014

ISCB Department

CyberSecurity Malaysia

Level 5 Sapura@Mines,
No 7 Jalan Tasik, The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8946 0999 Fax: +603 8946 0888
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 9 July 2014, 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 associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	23/6/2014	All	Draft
v1	9/7/2014	All	Final

Executive Summary

SCAN S3 Security Manager Console Release 14556 (v2.0) integrated with SCAN S3 Agent (v2.0.1.6.2) (hereafter referred as SCAN S3) from SCAN Associates Berhad is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation. The TOE is comprises of two main component as known as Management console and the agent which provides user interface with the system.

SCAN S3 Security Manager Console which known as SCAN S3 SMC is integrated with SCAN S3 Agent is a Web-Based Application Access Control Management, which enable users to access their internal network resources securely through PKI implementation via soft-certificates, roaming certificates and smart cards. It provides administration console for the operation for of SCAN S3 SMC-AGENT.

SCAN S3 SMC-AGENT is a platform that consolidates various security services into a single enterprise-wide architecture. SCAN S3 SMC-AGENT helps to mitigate the security risks when implementing an Enterprise Application and e-Services.

In general, the SCAN S3 SMC is comprises of Administration module, Logging module, Policy Management module, Token Management, User Authentication Management and Login Module. Meanwhile for SCAN S3 AGENT, it interacts directly with the SCAN S3 SMC module. However, the Certificate Repository Service is excluded from the scope of evaluation.

The TOE provides Security Audit, Identification and Authentication, Cryptography, Security Management, User Data Protection and Protection of the TSF security functions. These security functions of the SCAN S3 will address the threats and Organizational Security Policy (OSP) that are described in section 3 of the Security Target (Ref [6]).

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies the following:

i) Assumptions made during the evaluation,

ii) The intended environment for SCAN S3,

iii) The security requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements.

Consumers are advised to verify that their operating environment is consistent with that specified in the security target, 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 SCAN S3 to the Common Criteria (CC) evaluation assurance level EAL2. The report confirms that the product has met the target assurance level of EAL2 and the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]). The evaluation was performed by the CyberSecurity Malaysia MySEF and was completed on 30 May 2014

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that SCAN S3 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 EAL2. The product Certificate, Certification Report and Security Target will be listed on the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc.

It is the responsibility of the user to ensure that SCAN S3 meets their requirements. It is recommended that a potential user of SCAN S3 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), SCAN S3 Security Manager Console Release 14556 (v2.0) integrated with SCAN S3 Agent (v2.0.1.6.2) (hereafter referred as SCAN S3) is an authentication system which being able to be integrated with the enterprise system. The TOE provides the several user authentication mechanisms such as combination of username and password, password and PIN and PKI token (e.g soft certificates, roaming certificates and/or smart card).

2 The details of TOE functions can be found in section 1.6 of the Security Target version 2.7.

3 There are six security functionalities covered under the scope of the evaluation which are Security Audit, Identification and Authentication, Cryptography, Security Management, User Data Protection and Protection of the TSF.

1.2 TOE Identification

4 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	C050
TOE Name	SCAN S3 Security Manager Console Release 14556 (v2.0) integrated with Scan S3 Agent (v2.0.1.6.2)
TOE Version	SCAN S3 Security Manager Console Release 14556 (v2.0) integrated with Scan S3 Agent (v2.0.1.6.2)
Security Target Title	SCAN S3 Security Target
Security Target Version	2.7
Security Target Date	14 April 2014
Assurance Level	EAL 2
Criteria	Common Criteria Part 1, Common Criteria Part 2, Common Criteria Part 3 Version 3.1 Revision 4
Methodology	Common Methodology for IT Security Evaluation , version 3.1 revision 4
Protection Profile Conformance	None
Common Criteria	CC Part 2 Extended

Conformance	CC Part 3 conformant Package conformant to EAL 2
Sponsor and Developer	SCAN Associates Berhad Level 7, Menara Naluri, 161-B, Jalan Ampang, 50450 Kuala Lumpur
Evaluation Facility	CyberSecurity Malaysia MySEF

1.3 Security Policy

5 SCAN S3 does implement several policies for Organizational Security Policy. This policy requires criteria that should be adhered where the TOE may be initialised such as:

a) TOE is accessible by authorized person only.

b) The user and administrator of the TOE shall practice secure form of password combination by using special character, number and alphabet with minimum number lengths of 12 characters.

1.4 TOE Architecture

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

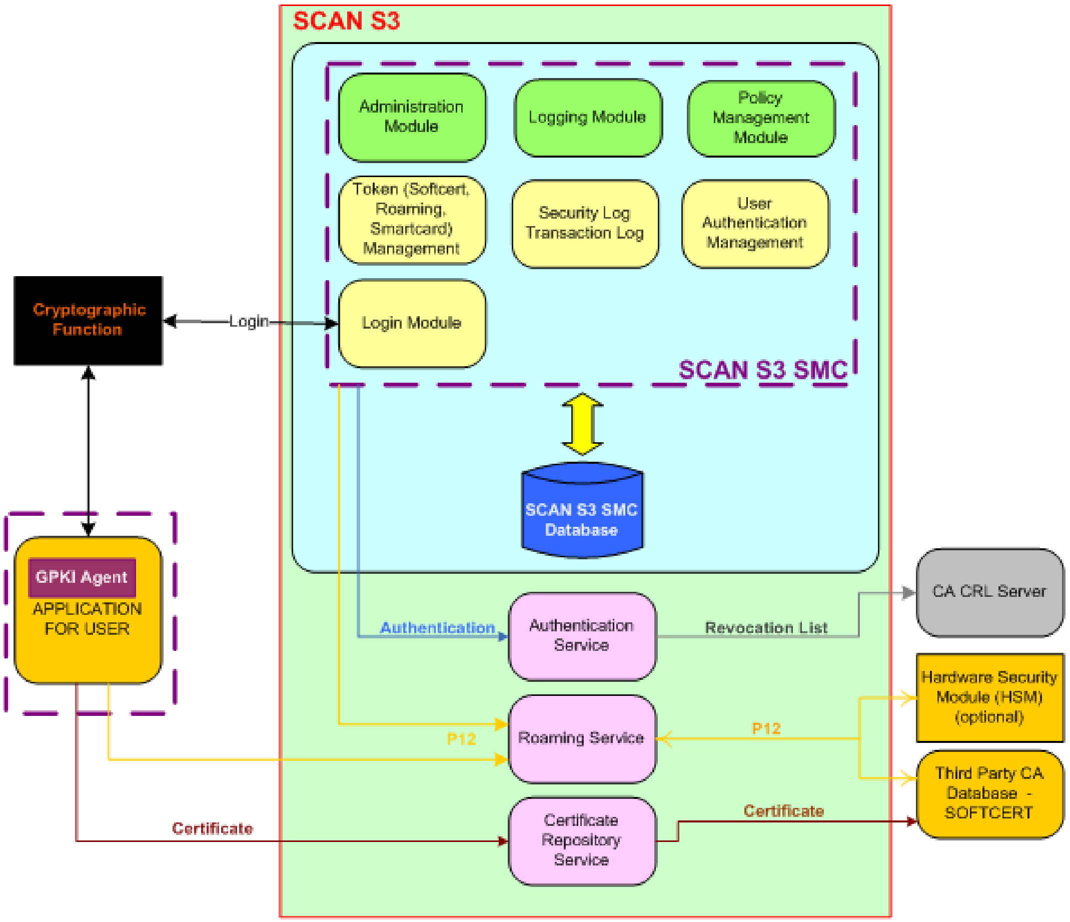

Figure 1 TOE Architecture

7 Typically the SCAN S3 is deployed in enterprise environment. The description of the TOE console and agent as below:

a) SCAN S3 Security Manager Console (SCAN S3 SMC)

The SCAN S3 SMC, which is the first element of the TOE, is the security administration console to set up the user authorization parameters, defining the user’s authentication mode as well as the workstation and risk policy. The following describes the features of SCAN S3 SMC:

- Centralized administration of logon ID’s.
- Centralized policy configuration.
- Centralized collection of logging of events.

b) SCAN S3 Agent

It is a Software desktop component that provides PKI related functions (importing certificate, removing certificate, listing all loaded certificates, signing user data, verification of signing data and user credential, authentication components, and checking for roaming certificate usage (for user that assigned with the roaming certificate usage)) at client side.

8 Following are the major security functions provided by the TOE:

a) **Security Audit**- The TOE ensures that all crucial events being captured and audited.

b) **Cryptography** – SCAN S3 AGENT has the capabilities of performing cryptographic functions such as Import certificate, removing certificate, capturing certificate from PKI token, listing all certificates, signing, verification, authentication and checking for roaming certificate at client side in their workstation or desktop.

c) **User Data Protection –** The TOE provides Access Control Policy to all users who tries to access the TOE and the user is granted based on certain user attributes defined.

d) **Identification and Authentication** – The TOE ensures that only authorized user is permitted to access the TOE.

e) **Security Management** – The TOE provides functionality to Administrator to manage TOE secure setting and user management via TOE console.

f) **Protection of the TSF** – The TOE ensures that the time stamps to be taken from a reliable source from the environment that integrated with the underlying operating system.

1.5 Clarification of Scope

9 The logical scope of the TOE as below:

a) **Security Audit** – The TOE captures all crucial events recorded along with date and time of event, user accounts that performed the event, event name and other event details. The audit log can only be viewed by TOE administrator. The protected audit log also cannot be edited or modified.

b) **Cryptography**– TOE has a built-in feature of cryptography that bound to the operations of SCAN S3 AGENT at Users and Administrators workstation. Each of them is required to install the SCAN S3 AGENT before initiating communication with the SCAN S3 SMC components via web browsers.

c) **User Data Protection** – TOE implements Access Control Policy to all users who try to access the TOE and the user is granted based on certain user attributes defined.

d) **Identification and Authentication** – Each user must be successfully identified and authenticated with a username and password via authentication mechanism invoked by the TOE before access is allowed to the TSF.

e) **Security Management** –This module provides various TOE system functionalities to TOE administrator in managing the user account, access right, role and privileges to the TOE. The Administrator is able to modify, delete and add user or modify TOE configurations. TOE Administrator/s 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.

f) **Protection of the TSF** - TOE shall ensure that the reliable time stamp is provided by the environment for instance integrating with the underlying operating system.

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

11 Functions and services which are not included as part of the evaluated configuration are as follows:

a) All hardware appliance, operating systems, and third party supporting software such as database are not part of the scope evaluation.

b) Third party Certificate Authority.

c) Other supporting softwares:

   i) Tokens (Smart Card, Soft certificate, Roaming certificate)

   ii) JRE 1.7

   iii) Adobe Acrobat Reader

   iv) Archive Utility (Winzip)

   v) Monitor resolution – SVGA

1.6 Assumptions

12 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 required for secure operation of the SCAN S3.

1.6.1 Usage assumptions

13 The following specific conditions are required to ensure the security of the TOE in term of TOE Usage:

a) The authorized administrator is non-hostile, assigned by the organization and follows guidance documentation accordingly.

b) All data and information is passing through the TOE.

c) Administrator can access the TOE via secure connection.

d) Remote access is only given to authorized administrator.

1.6.2 Environment assumptions

14 The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed:

a) The TOE is operated and protected in physically secured environment.

b) The TOE is managed from the separated network including internal and external. Remote management is only permitted using secure channel only such as VPN and others secure connection.

c) Time stamp of the TOE is reliable on TOE environment.

d) The communication link between client side and server side is constructed securely.

1.7 Evaluated Configuration

15 This section describes the configurations of the TOE that are included within the scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the documented preparative and operational user guidance, and only by trustworthy staff.

16 The TOE, and its supporting hardware and software listed in the Security Target (Ref [6]) are configured based on secure installation guidance as follows:

a) SCAN S3 Security Manager Console and SCAN S3 Agent setup including network setup between both sides.

1.8 Delivery Procedures

17 SCAN S3 is delivered to the client by SCAN Associates Berhad personnel. Secure delivery process and procedure is practised to preserve the integrity value between vendor and client. Below is listed guidance for end-user to identify SCAN S3 SMC-AGENT integrity:

a) Labelling the SCAN S3 SMC-AGENT.

b) Verification of SCAN S3 SMC-AGENT Software and Version.

c) Delivery of the Product on the Client Side.

18 Details of the delivery process can be found in SCAN S3 Delivery Procedure (Ref (8)).

1.9 Documentation

19 To ensure continuous secure usage of the product, it is important that the SCAN S3 is used in accordance with the guidance documentation.

20 The following documentation is provided by the developer to the end user as guidance to ensure secure usage and operation of the product:

a) SCAN S3 Admin Manual, version 1.1 , 4 April 2014

b) SCAN S3 User Manual, version 1.0, 5 April 2014

c) SCAN S3 Security Operational Procedure, version 1, 27 May 2014

d) SCAN S3 Configuration Management and Configuration List, version 1, 27 May 2014

21 The following guidance documentation is used by the developer's authorised personnel and administrator as guidance to ensure secure installation of the product:

a) SCAN S3 Installation Guide, version 1.1, 4 April 2014

2 Evaluation

22 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

23 The evaluation activities involved a structured evaluation of SCAN S3, including the following components:

2.1.1 Life-cycle support

24 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 unauthorized access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

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

2.1.2 Development

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

27 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.

28 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

29 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

30 Testing at EAL2 consists of assessing developer tests, independent function test, and performing penetration tests. SCAN S3 testing was conducted by CyberSecurity Malaysia MySEF lab in Seri Kembangan, Selangor. 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

31 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).

32 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

33 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 a sample of the developer’s test plan, and creating test cases that augmented the developer tests.

34 The results of the independent test developed and performed by the evaluators to verify the TOE functionality as follow:

Table 2: independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
To test on TOE security functions of TOE control access, privilege and management function that is allowed for the user and how TOE reacts to inactivity session	FMT_MOF.1 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1 FMT_MSA.1 FMT_MSA.3 FDP_ACC.1 FDP_ACF.1 FDP_IFC.1 FDP_IFF.1 FTA_SSL.1	• TOE Administrator/s with Administration Module • TOE Administrator/s with Policy Management Module • TOE Administrator/s with Token Management Module • TOE Administrator/s with Logging Module • TOE Administrator/s with User Authentication Module	**PASS.** Result as expected.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
		• [TOE Administrator/s & TOE User/s] with SCAN S3 AGENT • [SCAN S3 SMC& SCAN S3 AGENT] with Underlying Operating System	
To test on TOE security functions of security audit and time stamp from the operational environment	FAU_GEN.3 FAU_GEN.2 FAU_SAR.1 FAU_SAR.2 FAU_STG.1 FAU_STG.4 FPT_STM.2	• [TOE Administrator/s & TOE User/s] with SCAN S3 AGENT • [SCAN S3 SMC& SCAN S3 AGENT] with Underlying Operating System	**PASS.** Result as expected.
To test on TOE security functions of performing cryptographic functions	FCS_COP.1	• [TOE Administrator/s & TOE User/s] with SCAN S3 AGENT • [SCAN S3 SMC& SCAN	**PASS.** Result as expected.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
		S3 AGENT] with Underlying Operating System	
To test on TOE security functions of identification and authentication of user to protected websites through SCAN S3 Agent and SCAN S3 SMC. The PKI tokens available includes: a) Soft certificate b) Roaming certificate c) Smart card	FIA_ATD.1 FIA_UAU.2 FIA_UID.2 FIA_USB.1	• TOE Administrator/s with Policy Management Module • TSFI's between TOE Administrator/s with Token Management Module • TOE Administrator/s with Login Module • TOE Administrator/s with User Authentication Module • Login Module & [Authentication Service& Roaming	**PASS.** Result as expected.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
		Service]	

35 All tests performed by the evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration Testing

36 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.

37 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential. The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE;

d) Window of opportunity; and

e) IT hardware/software or other requirement required for exploitation.

38 The penetration tests focused on:

a) Scanning on TOE Server;

b) Cross Site Scripting

c) Session Hijacking

d) SQL Injection

e) Sniffing

f) Brute force attack

g) Restrict URL Access

h) Redirect and Forward URL

i) Cross Site Request Forgery (CSRF)

j) Unrestricted File Upload

39 The results of the penetration testing note that a number of additional vulnerabilities exist that are dependent on an attacker having access to the end-user host

computer. Therefore, it is important for the user to ensure that the TOE is use only in its evaluated configuration and in secure environment.

2.1.4.4 Testing Results

40 Tests conducted for the SCAN S3 produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

3 Result of the Evaluation

41 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 SCAN S3 performed by the CyberSecurity Malaysia Security Evaluation Facility which known as CSM MySEF.

42 CSM MySEF found that SCAN S3 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 EAL2.

43 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 undiscovered in its claimed security functionality. This risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

44 EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

45 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.

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

3.2 Recommendation

47 In addition to ensure secure usage of the product, below are additional recommendations for SCAN S3 users:

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

b) The underlying operating system and database server are patched and hardened to protect against known vulnerabilities and security configuration issues.

c) The servers that host the server side application and database servers are hosted in a secure operating facility with restricted physical access and on dedicated hardware.

d) The communication medium between server side and agent side is secured by organizational policy that enforces prohibition of malicious tool usage in the corporate network such as network sniffer.

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] SCAN S3 Security Target, version 2.7, 14 April 2014

[7] Evaluation Technical Report, Version 1.0, 30 May 2014

[8] SCAN S3 Delivery Procedure, version 1, 27 May 2014

A.2 Terminology

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

Acronym	Expanded Term
ST	Security Target
TOE	Target of Evaluation

A.2.1 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.

Term	Definition and Source
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 ---