An agency under MOSTI

Ministry of Science, Technology and Innovation

C027 Certification Report
NetSignOn version 2.0

File name: ISCB-5-RPT-C027-CR-v1a
Version: v1a
Date of document: 16 April 2012
Document classification: PUBLIC

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

C027 Certification Report
NetSignOn version 2.0

16 April 2012

ISCB Department

CyberSecurity Malaysia
Level 8, Block A, Mines Waterfront Business Park,
No 3 Jalan Tasik, The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8946 0999 Fax: +603 8946 0888
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C027 Certification Report - NetSignOn version 2.0
DOCUMENT REFERENCE:	ISCB-5-RPT-C027-CR-v1a
ISSUE:	v1a
DATE:	16 April 2012

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:
Level 8, Block A,
Mines Waterfront Business Park,
No 3 JalanTasik, The Mines Resort City,
43300 Seri Kembangan
Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee
Company No. 726630-U

Printed in Malaysia

Forward

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), CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the ISCB 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 16 April 2012, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement at www.commoncriteriaportal.org).

Reproduction of this report is 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 3 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 3 (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
v1	26 March 2012	All	Final Released
v1	16 April 2012	Page vi	Add the date of the certificate.

Executive Summary

MQAssure™ NetSignOn Version 2.0 (hereafter referred as NSO) from MagnaQuest Solutions Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 1 evaluation.

The TOE is a client agent that integrates with Windows operating system platforms of the desktop and laptops. It leverages multiple authentication methods such as MyKAD, biometric, USB token, and userid/password to perform the login functionality to a system in a Domain (network connected mode and network disconnected mode).

NSO is utilising MQAssure™/AppShield v1.2_CR6 Integrated with MQAssure™ IAM v1.0_CR6 (IAM), a centralized identity and access management platform. It provides the backbone for the NSO by providing centralized policy management (part of IM), session management and audit logging (part of AM). In the overall infrastructure, NSO acts as a policy enforcement agent for workstations. IAM provides a centralized administration console through which the administrators can create and enforce various policies to control the authentication schemes to workstations in a domain. IAM consists of the following modules:

- MQAssure™ Access Manager (AM) that is partially in scope of the TOE, which is where the run-time (real-time) checks are performed during the authentication phase.
- MQAssure™ Identity Manager (IM) is enforcing the authentication policy and reports viewing function which is within the scope of the TOE. Additionally, only Self-help function for TOE users is within the scope of the TOE.

The security functions that the TOE provides include the following:

- **User data protection** – Users are required to login using the combination of multiple authentication methods.
- **Identification and Authentication** – Users must be identified and authenticated before access to relevant resources is allowed.
- **Security Management –** The TOE contains various management functions to ensure efficient and secure management of the TOE such as user management and changing passwords.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for NSO, 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 describes the findings of the security evaluation of NSO, to the Common Criteria (CC) evaluation assurance level EAL1 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 10 February 2012.

Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the NSO evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificate. The product will be listed on 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 the NSO meets their requirement and security needs. It is recommended that prospective users of the NSO refer to the ST (Ref [6]), and read this Certification Report prior to deciding whether to purchase and deploy the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE), MQAssure™ NetSignOn Version 2.0 (hereafter referred as NSO), is a client agent that integrates with Windows operating system platforms of the desktop and laptop. It leverages multiple authentication methods such as MyKAD, biometric, USB token, and userid/password to perform the login functionality to a system in a Domain (network connected mode and network disconnected mode).

2 The security functions that the TOE provides include the following:

a) User Data Protection – User access the domain via several methods such as userid and password combination, or MyKAD and PIN combination, or MyKAD and Biometric (finger printing) combination, or iKey and PIN combination. Userid and password combination must be combined with either MyKAD or iKey authentication scheme. Regardless of the authentication mechanism used, the initial userid must be entered at the very beginning of the authentication process.

b) Identification and Authentication – Users must be identified and authenticated before access to relevant resources is allowed. The user identities, type of authentication scheme (example via iKey or MyKAD), the user credentials and roles are maintained. If a user authentication scheme is done via a combination of userid and password, the TSF verifies the password to ensure that it includes both alpha and numeric characters, contains at least one complex character, and does not contain repeating predictable sequence. The password must also adhere to the minimum number of characters. User account will be disabled after several unsuccessful authentication attempts.

c) Security Management – Only 1 role (user role) declared for the evaluation. Administrator role is not part of the scope. User can change their password through MQAssure™ Identity Manager (IM). User account will be disabled after a number of unsuccessful authentication attempts (default is 3 attempts) in IM.

3 The scope of evaluation only covers NSO that runs in system connected to domain.

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	C027
TOE Name	NetSignOn
TOE Version	Version 2.0

Security Target Title	MQAssure™ NetSignOn Secure Desktop Login
Security Target Version	1.7
Security Target Date	8 February 2012
Assurance Level	Evaluation Assurance Level 1 (EAL 1)
Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, version 3.1 revision 3 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant. CC Part 3 Conformant. Package conformant to EAL1.
Sponsor and Developer	MagnaQuest Solutions Sdn Bhd, A-2-07 & A-2-09 SME Technopreneur Centre, 2270, Jalan Usahawan 2, 63000 Cyberjaya, Selangor MALAYSIA
Evaluation Facility	CyberSecurity Malaysia MySEF

1.3 Security Policy

5 In order to provide user data protection, the TOE enforces an access control policy where the users can login to the domain using one of the following authentication schemes:

a) Userid and password combination

b) Userid, MyKAD and PIN/password combination. This authentication scheme is only supported at the NSO component (not applicable when user login to IAM). The management of the scheme is however performed at the IAM component.

c) Userid, MyKAD and Biometric (finger printing) combination

d) Userid, iKey and PIN combination

Users are required to login through one of the above combinations from a locked out or logged out state.

6 The detail of the security policy of the TOE is expressed by the set of security functional requirements which includes user data protection, identification and authentication, and security management. Further details on these security policies may be found in Section 5 of the ST (Ref [6]).

1.4 TOE Architecture

7 The Security Target (Ref [6]) defines clearly both logical and physical boundaries of the TOE.

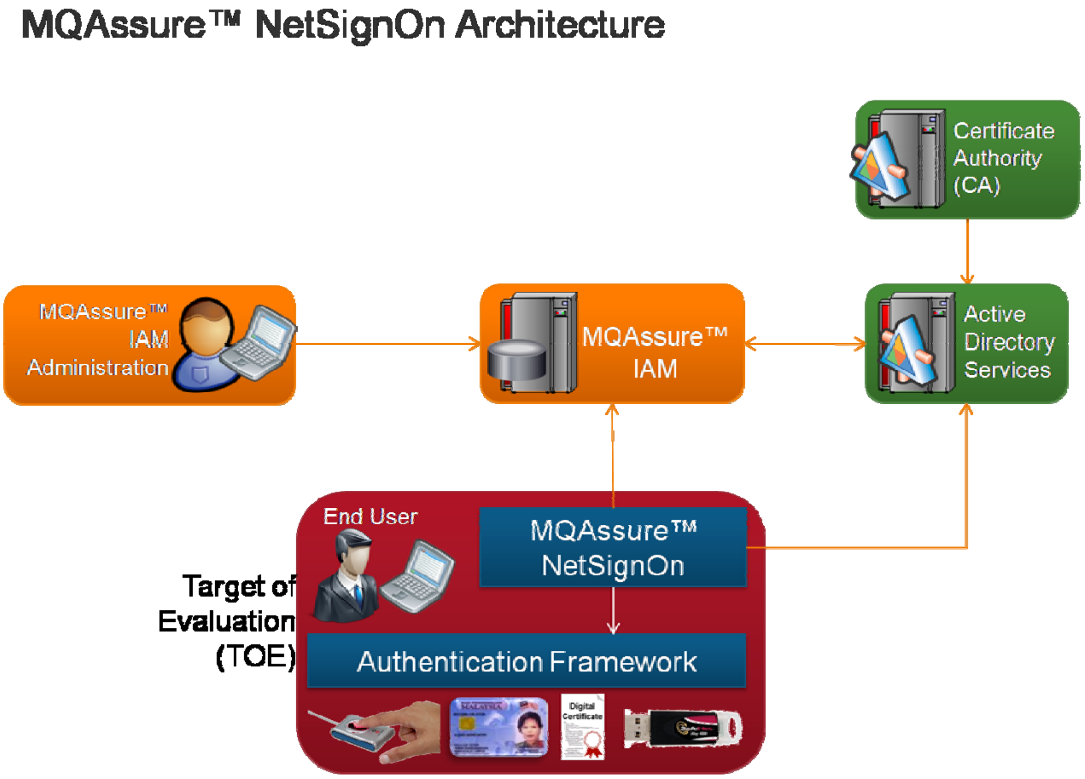
MQAssure™ NetSignOn Architecture
Certificate Authority (CA)
MQAssure™ IAM Administration
MQAssure™ IAM
Active Directory Services
End User
MQAssure™ NetSignOn
Target of Evaluation (TOE)
Authentication Framework

Figure 1: NSO Architecture

8 The architecture of the TOE can be found in Figure 1 above and identifies the various supporting components that combine to deliver the system. The TOE is an application that requires a server machine, operating system, and other supporting software as described in Section 2.2.2 of the ST (Ref [6]). The following is the components require for the implementation of the TOE:

a) MQAssure™/AppShield v1.2_CR6 Integrated with MQAssure™ IAM v1.0_CR6 (MQAssure™ IAM 1.0 or IAM), a centralized identity and access management platform. It provides the backbone for the NSO by providing centralized policy management (part of IM), session management and audit logging (part of AM). In the overall infrastructure NSO acts as a policy enforcement agent for workstations. IAM provides a centralized administration console through which the administrators can create and enforce various policies to control the authentication schemes to workstations in a domain. IAM consists of the following modules:

   o MQAssure™ Access Manager (AM), which is partially in scope of the TOE, is where the run-time (real-time) checks are performed during the authentication phase.

- o MQAssure^{TM} Identity Manager (IM) is enforcing the authentication policy and reports viewing function which is within the scope of the TOE. Additionally, only Self-help function for TOE users is within the scope of the TOE.
- o Admin Module, not in scope of the TOE, is the module where the administrators would use to connect to IM for policy definition.

b) Active Directory (AD) Services, is a directory structure used on Microsoft Windows based computers and servers to store information and data about networks and domains. It also stores user account details and workstations details joined in to a domain. User information is synchronized between the databases in IAM and AD. The synchronization of the databases will be done manually during the initial setup. Subsequently, the databases will be synchronized automatically for any changes to the user information. AM will verify the userid and password during the authentication phase with the AD server. This part is not in the scope of the TOE.

c) Windows Certificate Authority on AD Server (Windows CA). A certificate authority or certification authority (CA) is an entity that issues digital certificates. The Windows CA digital certificate is used to authenticate the AD server to the IAM server. This part is not in the scope of the TOE.

9 NSO provides the login interface to the users to login to their respective workstations. It is implemented as a custom GINA dll in Windows. The TOE makes use of the IAM services to select appropriate authentication scheme and retrieve the credentials for that particular user.

1.5 Clarification of Scope

10 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 communication security in accordance with administrator guidance that is supplied with the product. 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) **User Data Protection** - The users can login to the domain via one of the following methods: Userid and password combination, or MyKAD and PIN combination, or MyKAD and Biometric (finger printing) combination, or iKey and PIN combination. Userid and password combination must be combined with either MyKAD or iKey authentication scheme. Regardless of the authentication mechanism used, the initial userid must be entered at the very beginning of the authentication process.

Users are required to login through one of the above combinations from a locked out or logged out state. Note that the locked out state is defined as when the users of IM has reached the maximum number of allowable login trials whether the authentication has failed. The logged out state is defined as when the users of IM or NSO component choose to log out.

b) **Identification & Authentication** - Users must be identified and authenticated before access to relevant resources is allowed.

The user identities, type of authentication scheme (like via iKey or MyKAD), the user credentials and roles are maintained. If a user authentication scheme is done via a combination of userid and password, the TOE security function (TSF) verifies the password to ensure that it includes both alpha and numeric characters, contains at least one complex character, and does not contain repeating predictable sequence. The password must also adhere to the minimum number of characters.

User account will be disabled after several unsuccessful authentication attempts when users log in to IM (not in the NSO component). And, users must be re-authenticated once they are either locked or logged out of the domain. The number of unsuccessful attempts is set by the administrator in IM (this process is not part of the TOE). The default value is 3 however it can be set as an integer value between 1 to 99.

c) **Security Management –** The role of TOE's users are maintain by IAM to determine what the users can access based on the privileges assigned in the Active Directory. Only change passwords function of the user profile management of User role is part of the evaluation scope.

The following management functions are not part of the TOE:

- Registration or enrolment of users into IAM
- Enrolment of user credentials into iKey or with MyKAD
- Synchronization of the IAM and AD databases
- Verification of userid and password at the AD server
- Policy configuration in IAM and AD servers
- Self-help function in IM for the administrator of IAM and NSO

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

12 Functions and services which are not included in the scope of the evaluation, but these IT environment are required to ensure that the TOE perform in its intended operations, are as follows:

a) Servers such as directory and web server;

b) Certificate Authority;

c) Client token such as USB token, e-ID smartcard, biometric reader;

d) Operating Systems (Microsoft Windows XP, Windows Vista and Windows 7);

e) Database;

f) Other software such as Active Directory

13 Secure installation of the operational environment is an important element in ensuring that the TOE is initialised correctly and protection from tampering.

1.6 Assumptions

14 This evaluation was performed at EAL1. Therefore, no assumptions for the TOE were defined in the ST (Ref [6]).

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:

a) EAL1 Preparative Guidance (Ref 20a)).

b) Installation Document for AppShield/IAM (Ref 20b)).

c) NSO Installation and Administration Manual (Ref 20c)).

1.8 Delivery Procedures

16 The TOE is delivered to user not in an operational state. The TOE installation and configuration can be executed by the client themselves or developer, based upon the client preference.

17 However, for this EAL1 evaluation, TOE Delivery (ALC_DEL) is not included. Thus, developer did not provide any documentation on TOE delivery and the evaluators did not verify any TOE delivery process.

18 In Section 4.1 of the ST (Ref [6]), OE_INSTALL stated that those responsible for the TOE must ensure that the TOE and third party software are delivered, installed, managed, and operated in a manner which maintains the organizational IT security objectives. Therefore, the evaluators relied on the environment to provide a secure TOE delivery process.

1.9 Documentation

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

20 The following documentation is provided by the developer to the end user as guidance to ensure secure installation of the TOE:

a) EAL1 Preparative Guidance, v1.4, 2 Dec 2010 *(NetSignOn PRE v1.4)*.

b) Installation Document for AppShield/IAM, v1.14, 11 Nov 2010 *(MQAssure_AppShield_1.2_Installation_Document_v1.14).*

c) NSO Installation and Administration Manual, v1.6, 30 Nov 2010 *(MQAssure_NetSignOn_Installation_Administration_Document_v1.6).*

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

a) User Manual for AppShield/IAM, v1.10, 23 Nov 2010 *(MQAssure_AppShield_1.2_User_Manual_v1.10)*.

b) NSO User Manual, v1.4, 21 Nov 2010 *(MQAssure_NetSignOn_User_Manual_v1.4)*.

2 Evaluation

22 The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 1 (EAL1). 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 NetSignOn Version 2.0, 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 confirmed that the configuration list which includes the TOE and the evaluation evidence were clearly and uniquely labelled.

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 (TSF) interfaces (TSFIs), and how the TSF implements the security functional requirements (SFRs).

2.1.3 Guidance documents

26 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

27 Testing at EAL1 consists of performing independent function test, and performing penetration tests. The formal testing was conducted by evaluators from CyberSecurity Malaysia MySEF where it was subject to an independent functional and penetration tests. 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 Independent Functional Testing

28 At EAL1, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining functional and guidance documentation, and creating test cases to verify the behaviour of the TOE.

29 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 tests developed and performed by the evaluators to verify the TOE functionality are as follows:

Table 2: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
To test on the TOE security functions of how the TOE control access and privilege for each users.	User Data Protection	User Data Protection	**PASS**. Result as expected.
To test on the TOE security functions of identification and authentication of users to Windows through NSO and the authentication of user in IAM. The authentication scheme includes: • MyKad/Biometric • iKey/PIN • Password	Identification and Authentication	Identification and Authentication	**PASS**. Result as expected.
To test on the TOE security functions of management function that is allowed for the user.	Security Management	Security Management	**PASS**. Result as expected.

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

2.1.4.2 Penetration Testing

31 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, and functional specification.

32 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 (specialist expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

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

33 The penetration tests focused on :

a) Web scanning;

b) Physical password attack;

c) Sniffing;

d) Cookies manipulation;

e) Cross Site Scripting (XSS);

f) Man-in-the-Middle (MIIM) attack;

g) SQL injection; and

h) Privilege escalation.

34 The results of the penetration testing note that there is no exploitable vulnerability and/or residual vulnerability found. However, it is important to ensure that the TOE environment have been correctly configured, patched and hardened.

2.1.4.3 Testing Results

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

36 Based on the results of penetration testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

3 Result of the Evaluation

37 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 NSO performed by the CyberSecurity Malaysia MySEF.

38 The CyberSecurity Malaysia MySEF found that NSO 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 EAL1.

39 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

40 EAL1 provides a basic level of assurance by a limited Security Target and an analysis of the security functions in that Security Target, using a functional and interface specification and guidance documentation, to understand the security behaviour.

41 The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TOE security functions.

42 EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

3.2 Recommendation

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

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

b) Those responsible for administrating the TOE and also the environment must ensure that the following is maintained:

   - The underlying operating system for the database and web-servers are patched and hardened to protect against known vulnerabilities and security configuration issues.
   - Digital certificates are valid (not revoked or expired), are sourced and verified from a trusted entity.
   - The servers that host the web and database servers are hosted in a secure operating facility with restricted physical access and are not installed in shared hardware.

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 3, July 2009.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

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

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

[6] MQAssure™ NetSignOn Secure Desktop Login, Version 1.7, 8 February 2012.

[7] Evaluation Technical Report NetSignOn version 2.0, Version 1.1, 10 February 2012.

A.2 Terminology

A.2.1 Acronyms

Table 3: List of Acronyms

Acronym	Expanded Term
AM	MQAssure™ Access Manager
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology (ISO/IEC 18045)
IAM	MQAssure™/AppShield v1.2_CR6 Integrated with MQAssure™ IAM v1.0_CR6 (may also be referred to as MQAssure™ IAM 1.0 or IAM)
IEC	International Electrotechnical Commission
IM	MQAssure™ Identity Manager
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
PIN	Personal Identification Number
PP	Protection Profile
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
USB	Universal Serial Bus

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Certifier	The certifier responsible for managing a specific certification task.
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.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
GINA	The graphical identification and authentication (GINA) library is a component of some Microsoft Windows operating

Term	Definition and Source
	systems that provides secure authentication and interactive logon service.
iKey	USB token that is used for a two-factor authentication.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.
Local Cache	A local instance of the database at the client's machine.
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.
MyCB Personnel	Includes all members of the Certification Subcommittee, the Scheme Manager, the Senior Certifier, Certifiers and the Quality Manager.
MyKAD	Official compulsory smart identity card of Malaysia. It contains a smart card chip.
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 ---