C046 Certification Report

MQAssure™ NetSignOn v3.0

File name: ISCB-5-RPT-C046-CR-v1a
Version: v1a
Date of document: 17 December 2013
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

C046 Certification Report

MQAssure™ NetSignOn v3.0

17 December 2013

ISCB Department

CyberSecurity Malaysia

Level 5, Sapura@Mines,

No 7 Jalan Tasik, The Mines Resort City

43300 Seri Kembangan, Selangor, Malaysia

Tel: +603 8992 6888 □Fax: +603 8992 6841

http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C046 Certification Report – MQAssure™ NetSignOn v3.0
DOCUMENT REFERENCE:	ISCB-5-RPT-C046-CR-v1a
ISSUE:	v1a
DATE:	17 December 2013

DISTRIBUTION:	UNCONTROLLED COPY – FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 5, Sapura@Mines

No 7, Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 17 December 2013, 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.

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
v1	29 November 2013	All	Final Released.
v1a	17 December 2013	Page iv	Add the date of the certificate.

Executive Summary

MQAssure™ NetSignOn v3.0 (hereafter referred as NetsignOn) from Magnaquest Solutions Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level 2 (EAL2) evaluation.

NetSignOn is a client authentication agent that integrates with Windows operating system platforms of the desktops and laptops. It leverages multiple authentication methods such as MyKAD, biometric (Fingerprint/Iris), USB token, and userid/password to perform the login functionality to a system in a Domain (Network connected mode and network disconnected mode). The evaluation only covers NetSignOn that runs in system which is connected to the domain.

MQAssure™ NetSignOn v2.0 is EAL1 certified by MyCC Scheme in 2012. The additional features of MQAssure™ NetSignOn v3.0 which were evaluated in this evaluation includes:

MQAssure™ NetSignOn v2.0 EAL 1 Certified	MQAssure™ NetSignOn v3.0 changes overview	Details
Access to IAM web is implemented over SSL.	Access to IAM Web as well as NetSignOn Client Communication with IAM Web Service is also implemented over SSL.	To enhance the security in accessing the IAM Web Service, even the communication to IAM Web Service is also implemented over SSL along with IAM Web access.
Supports password, smart card and fingerprint based authentication schemas.	Included iris based biometric authentication schema.	Along with fingerprint and smart card based authentication schemas, iris based authentication is also added to enhance the authentication process.
User enrolment and provisioning is done through IAM Web.	User provisioning can also be done at the NetSignOn Client Application.	Users who are enrolled at IAM can provision with IAM at their workstation itself when login to the system for the first time with NetSignOn Client installed.
Change/Reset token pin or user password is done through IAM Web.	Change/Reset of token pin or user password can also be done through NetSignOn Client Application.	Change/Reset of USB token pin and user password can also be done through NetSignOn Client Application.

Supports Internet Explorer 8 for accessing IAM Web.	Supports Google Chrome, Mozilla Firefox and Internet Explorer browsers.	The latest version of NetSignOn supports access to IAM Web through Google Chrome, Mozilla Firefox browsers along with Internet Explorer browser.
For evaluation purpose, iKey 2032 with 32KB (iKey) is used.	Replaced iKey 2032 with eToken Pro 72K.	eToken Pro got enhanced features when compared with iKey.
No support for iris authentication.	Iris image based authentication schema is implemented.	Along with finger print and smart card based authentication schemas, iris based authentication is also Included.

The scope of evaluation covers major security functions described as below:

a) **User Data Protection**: The TOE provides five different mechanisms to login into the domain. User may select to login by using combination of Userid and password, or MyKAD and PIN/password, or MyKAD and Biometric (finger printing), or eKey and PIN, or iris Biometric image.

b) **Identification and Authentication**: The TOE allows authorised users to access the TOE once the user is successfully identified and authenticated by the TOE.

c) **Security Management**: The TOE provides various management functions to ensure efficient and secure management of the TOE such as user management and changing password through NetSignOn user application or MQAssure™ Identity Manager (IM).

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 Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]). The evaluation was performed by CyberSecurity Malaysia MySEF and completed on 12 November 2013.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc and the

Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org

It is the responsibility of the user to ensure that NetSignOn meets their requirements. It is recommended that a potential user of NetSignOn 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

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE), MQAssure™ NetSignOn v3.0 (hereafter referred as NetSignOn) is a client authentication agent that runs on Windows operating systems. NetSignOn supports various type of authentication mechanisms for instance MyKAD, biometric (Fingerprint/Iris), USB token, and userid/password to perform the login functionality to a system in a Domain (Network connected mode and network disconnected mode). The scope of the evaluation only covers NetSignOn that runs in system which is connected to the domain.

2 NetSignOn provides the login interface to the users to login into their respective workstations. NetSignOn make use of the MQAssure™ IAM2.0 services to select appropriate authentication scheme and retrieve the credentials for that particular user.

3 The Active Directory Server is not part of the TOE scope. However, the server is required for the usage of the TOE in a network environment.

4 In the context of the evaluation, the TOE is expected to provide the following major security features:

a) **User Data Protection** – the TOE provides five different login mechanisms into the domain. User may select to login by using the combination of Userid and password, or MyKAD and PIN/password, or MyKAD and Biometric (finger printing), or eKey and PIN, or iris Biometric image. Regardless of the authentication mechanism used, the initial userid must be entered at the beginning of the authentication process. Users are required to re-login once the system is locked out or logged out.

   Note: the locked out state is defined as when the users has reached the maximum number of unsuccessful authentication attempt. The logged out state is defined as when the users choose to log out.

b) **Identification and Authentication** – users must be identified and authenticated before access to relevant resources is allowed.

   The user identities, type of authentication scheme such as via eKey or MyKAD or iris biometric, user credentials and roles are maintained. If a user authentication scheme is done via a combination of userid and password, the TOE 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 locked or disable after several unsuccessful authentication attempts.

c) **Security Management** – only user role was declared for this evaluation, administrator role is not part of the evaluation scope. Users are allowed to

login into the domain, as well as change their passwords through NetSignOn user application or MQAssure™ Identity Manager (IM).

User account will be disabled or locked after a number of unsuccessful authentication attempts (default is 3 attempts). Users are required to re-authenticate once the system is locked out or logged out through the security questionnaire in order to unlock their account.

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	C046
TOE Name	MQAssure™ NetSignOn
TOE Version	v3.0
Security Target Title	MQAssure™ NetSignOn v3.0 Secure Desktop Login
Security Target Version	v1.10
Security Target Date	22 October 2013
Assurance Level	Evaluation Assurance Level 2 (EAL 2)
Criteria	Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 4 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation , version 3.1 Revision 4 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 conformant CC Part 3 conformant Package conformant to EAL 2
Sponsor and Developer	MagnaQuest Solutions SdnBhd A-2-07 & A-2-09 SME Technopreneur Centre, 2270, JalanUsahawan 2, 63000 Cyberjaya, Selangor DarulEhsan
Evaluation Facility	CyberSecurity Malaysia MySEF

1.3 Security Policy

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 Security Target (Ref [6]).

7 In order to provide user data protection, the TOE enforces access control policy for users to login with one of the secure authentication mechanism that is configured in MQAssure™ IAM v2.0 (IAM). The users must enter their userid prior to one of the following authentication schemes:

a) If the assigned authentication scheme for the user is userid and password, then the user is prompted to enter his password, or

b) If the assigned authentication scheme for the user is MyKAD and PIN/password, then the user is prompted to insert his MyKAD into the reader and provide the PIN/password, or

c) If the assigned authentication scheme for the user is MyKAD and biometric, then the user is prompted to insert his MyKAD into the reader and place the thumb on the finger print scanner, or

d) If the assigned authentication scheme for the user is eKey and PIN, then the user is prompted to insert his eKey into the USB port and provide the PIN, or

e) If the assigned authentication scheme for the user is iris biometric, then the user is prompted for iris biometric image.

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

8 The details of the security policy are described in Section 6.1 and Section 7 of the Security Target (Ref [6]).

1.4 TOE Architecture

9 The TOE includes both logical and physical boundaries which are described in Section 2.3 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

10 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 TOE enforces access control policy to ensure that user data is protected. Users may choose to login using the combination of authentication schemes as follows:

i) Userid and password, or

ii) MyKAD and PIN/password, or

iii) MyKAD and Biometric (finger printing), or

iv) eKey and PIN, or

v) iris Biometric image.

Users are required to login through one of the above combinations from a locked out or logged out state. The users must first press Ctrl-Alt-Del prior to the authentication to the domain using the defined authentication scheme above.

Subsequently, the access control policy in MQAssure™ IAM v2.0 will check on the following objects to ensure that users are properly identified and authenticated:

i) User identity (userid).

ii) Type of the authentication scheme assigned.

iii) Credential for the assigned authentication scheme.

- PIN / Password for either userid or MyKAD.
- MyKAD number.
- Fingerprint biometric reference for MyKAD.
- Iris biometric reference for iris.
- PIN for eKey.
- Serial number for eKey.

iv) Role: User and administrator (not part of the evaluation scope).

b) **Identification and Authentication**

Users can only access the TOE (MQAssure™ NetSignOn v3.0 component and password management component of IM) once they are identified and authenticated.

The identification and authentication is accomplished via one of the following methods:

i) If the assigned authentication scheme for the user is MyKAD/PIN (or password), then the user is prompted to insert his MyKAD into the reader and provide the PIN / password after entering the userid.

ii) If the assigned authentication scheme for the user is MyKAD/Biometric, then the user is prompted to insert his MyKAD into the reader and place the thumb on the finger print scanner after entering the userid.

iii) If the assigned authentication scheme for the user is eKey/PIN, then the user is prompted to insert his eKey into the USB port and provide the PIN after entering the userid.

iv) If the assigned authentication scheme for the user is iris based, then the user is prompted for iris biometric after entering the userid.

v) If the assigned authentication scheme for the user is userid/password, then the user is prompted to enter his userid and password.

User account will be locked or disable after several unsuccessful authentication attempts. Users need to be re-authenticated once they are either locked or logged out from 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 and 99.

By default, user password will be the same as userid. At first time login and authenticated to IAM, the user is enforced to change the default password. The TOE verifies the entered PIN/password during changing password to ensure that it includes 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. This run-time (real-time) check is performed during the authentication process by AM.

The password policy above is set by an administrator in IM (this process is not part of the TOE).

c) **Security Management**

The TOE provides security management functionality for authorised users in order to change their password via the TOE (NetSignOn user application or IM). User is allowed to change the password depends on the following situations:

i) Change password at first time login.

ii) Unlock user account or user forgot the password.

iii) The users want to change their password.

By default, user PIN/password will be the same as userid. At first time login and authenticated to IAM, the user is enforced to change the default password. The TOE verifies the entered PIN/password during changing password to ensure that it includes 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. This run-time (real-time) check is performed during the authentication process by AM.

The password policy above is set by an administrator in IM (this process is not part of the TOE).

The TOE also maintains two distinct roles which are administrator and user. The users' roles are maintained by the TOE to determine what the users can access. If user authenticates as role "user" in IAM, the user will get several functionalities such as access to user profile and viewing audit events logs. However, the user profile management functions (except changing password) and viewing audit events logs are not part of the scope. If user authenticates as role "administrator" in IAM, the user will get all TOE administrative functionalities. However, the role administrator and all administrative functionalities is not part of the scope.

Both administrator and user will get access into Windows and have privileges as assigned in Active Directory. However, the privilege as assigned in Active Directory is not part of the evaluation scope

1.4.2 Physical Boundaries

11 The TOE is a client agent that runs on Windows operating systems and provides multifactor user authentication method to the 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.

12 Figure 1 below identifies the TOE and various supporting components of the system.

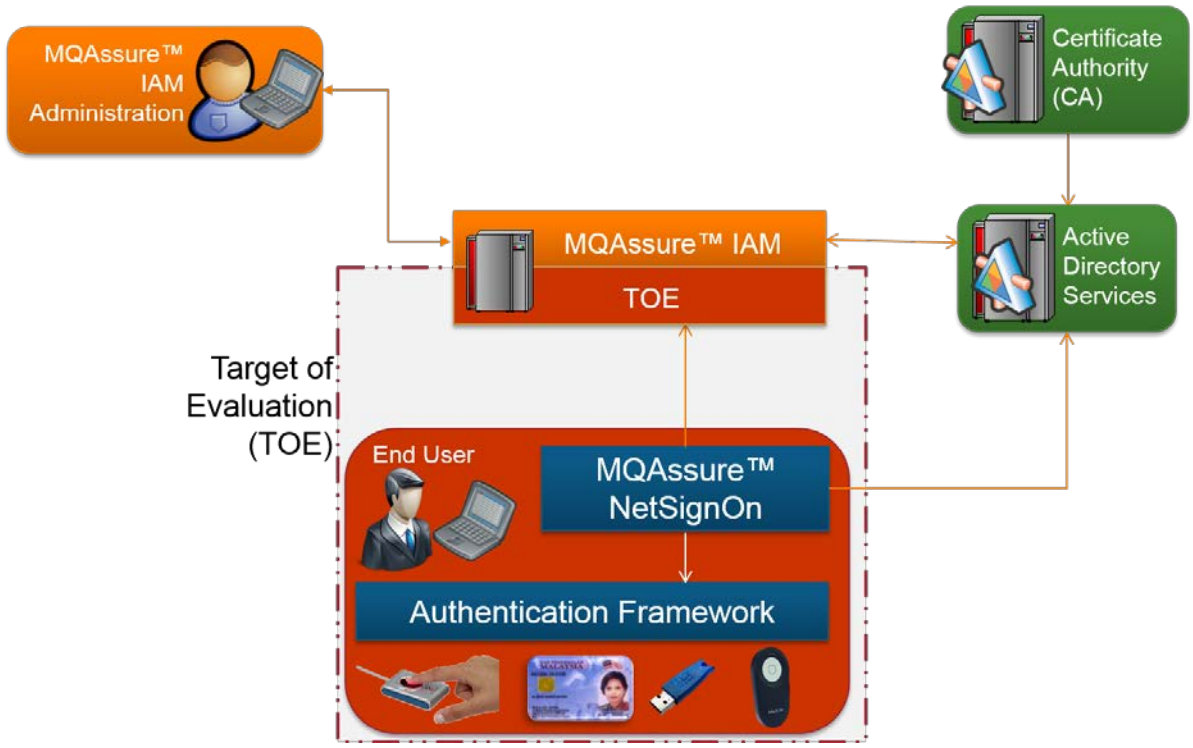

Figure 1: TOE Components

13 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 Security Target (Ref [6]). The following is the components require for the implementation of the TOE:

a) MQAssure™ IAM v2.0 (IAM)

IAM is a centralised identity and access management platform. It provides the backbone for the TOE by providing centralised policy management (part of IM), session management and audit logging (part of AM). In the overall infrastructure, the TOE acts as a policy enforcement agent for workstations. IAM provides a centralised 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:

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

ii) MQAssure™ Identity Manager (IM) is where administrators will define the authentication policy and viewing the reports. The Self-help function within IM (that is available to the TOE users) is within the scope of the TOE, the remaining part of the IM is outside the TOE scope.

iii) Admin Module, not in scope of the TOE, is the module where the administrators would use to connect to IM for policy definition and self-help.

b) Active Directory (AD) Services

AD 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 into a domain. User information is synchronised between the databases in IAM and AD. The synchronisation of the databases will be done manually during the initial setup. Subsequently, the databases will be synchronised automatically for any changes to the user information. AM will verify 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

1.5 Clarification of Scope

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

15 Section 1.4 of this document described the scope of the evaluation which was limited to those claimed made in the Security Target (Ref [6]). The TOE is a client authentication agent that is responsible to manage multiple authentication methods such as MyKAD, biometric (Fingerprint/Iris), USB Token, and user id/password combination to perform the login functionality to a system in a Domain or respective resources.

16 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 consumer of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

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

1.6.1 Usage assumptions

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

a) The TOE administrators are trustworthy.

1.6.2 Environment assumptions

19 The following 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 installed in secure physical location that can only be accessed by authorised administrators or users.

b) The trusted third party software is operating correctly and securely. Third party software is defined as in Section 2.2.2 of the Security Target (Ref [6]).

c) The usage of keys and other secret data are generated and stored outside the TOE is managed in accordance with the level of risk.

d) The TOE configuration is securely protected from other interruption and remains unchanged by other applications.

1.7 Evaluated Configuration

20 The TOE is a client agent that runs on Windows operating systems and provides multifactor user authentication method to the workstations. The TOE required non-TOE hardware, and software specified in Section 2.2.2 of the Security Target (Ref [6]).

21 The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the documented preparative user guidance (Ref 26a) and 26b)).

1.8 Delivery Procedures

22 NetSignOn is delivered to the customers by MagnaQuest Solutions Sdn Bhd personnel using delivery procedures (Ref 25a)) to ensure that the TOE is securely transferred to the respected customers. Before the TOE being delivered to the customers, there are some steps need to be performed by the Magnaquest Solutions Sdn Bhd personnel as below:

a) The TOE shall be prepared by Developer at their site before delivered to the customer. The TOE installer as well as supporting documentation and software are copied onto appropriate media (generally CD/DVD) and send to the customer through courier.

b) The CD/DVD key and generated hashes of the product installer are sent separately to customer's premises through courier.

23 Once receive the installation package and license key, the customer is instructed (as per the guidance) to verify the integrity of the TOE ;

a) Receipt of the TOE and identification of package contents checking that all components are present (TOE media, copy of license agreement, printed license key and TOE installation package hashes);

b) Performing a hash of all TOE media components (based on the software hashing mechanism specified in delivery procedure (Ref 25a)) and performing a compare against the hashes stated in the shipping notice;

c) Installation of the TOE with the supplied license key;

d) Verification of the TOE version as part of the installation process (identified in one stage of the TOE installer (Ref 26a));

e) If there any inconsistency found; the primary contact at customer has to communicate with MagnaQuest Solutions Sdn Bhd.

1.9 Documentation

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

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

a) MQAssure NetSignOn version 3.0 Delivery Procedure, v1.1, 15 June 2013.

b) MQAssure NetSignOn version 3.0 User Manual, v2.2, 20 June 2013.

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

a) MQAssure NetSignOn version 3.0 Installation Administration, v2.2, 14 June 2013.

b) MQAssure NetSignOn version 3.0 Preparative Procedure, v1.0, 15 June 2013.

2 Evaluation

27 The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 4 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 (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

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

2.1.1 Life-cycle support

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

30 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

31 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 TSF implements the security functional requirements (SFRs).

32 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.

33 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

34 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

35 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 at CyberSecurity Malaysia MySEF lab. 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

36 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).

37 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

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

39 The testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were developed and performed by the evaluators to verify the TOE functionality as follow:

Table 2: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
To test on access control for each user.	User Data Protection	• User Interface TSFI • Resource TSFI • Hardware TSFI	**PASS**. Result as expected.
To test on identification and authentication of user to	Identification and	• User Interface	**PASS**. Result as

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
Windows through NSO and authentication of user in IAM. The authentication scheme includes: • MyKAD/PIN • MyKAD/Biometric • eKey/PIN • Iris Biometric • Password	Authentication	TSFI • Resource TSFI • Hardware TSFI	expected.
To test on TOE management function that is allowed for respective user.	Security Management	• User Interface TSFI • Resource TSFI	**PASS**. Result as expected.

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

2.1.4.3 Penetration Testing

41 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.

42 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 design and operation (knowledge of the TOE);

d) Window of opportunity; and

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

43 The penetration tests focused on:

a) Vulnerabilities Scanning to identify any major loop hole;

b) Physical Password Attacks on TOE Server;

c) Physical Password Attacks on TOE Client;

d) Sniffing;

e) Cookies Manipulations;

f) Cross Site Scripting;

g) SSL Strip;

h) SQL Injections;

i) Brute Force Attack;

j) User impersonation using fake biometric items;

k) Cloning USB token; and

l) Compromising NSO component.

44 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 together with the non-TOE hardware and software requirements as specified in Section 2.2.2 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

45 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

46 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 MQAssure™ NetSignOn v3.0 performed by the CyberSecurity Malaysia Security Evaluation Facility which known as CyberSecurity Malaysia MySEF.

47 CyberSecurity Malaysia MySEF found that MQAssure™ NetSignOn v3.0 upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance level 2 (EAL2).

48 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. This risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

49 EAL2 provides assurance by a full security target and an 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.

50 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.

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

3.2 Recommendation

52 In addition to ensure secure usage of the product, below are additional recommendations for NetSignOn 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, hardware and software are patched and hardened to protect against known vulnerabilities and security configuration issues.

c) Digital certificates are valid (not revoked or expired), are sourced and verified from a trusted entity.

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

e) The TOE owners should test the NetSignOn to ensure that the underlying environment meets their security requirements.

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] MQAssure™ NetSignOn v3.0 Secure Desktop Login, version 1.10, 22 October 2013

[7] E031 Evaluation Technical Report for MQAssure™ NetsignOn v3.0, Version, 1.0 12 November 2013

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)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
EAL	Evaluation Assurance Level
GINA	Graphical identification and authentication
IAM	MQAssure™ IAM v2.0
IEC	International Electrotechnical Commission
IM	MQAssure™ Identity Manager
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
IT	Information Technology

Acronym	Expanded Term
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
NetSignOn	MQAssure™ NetSignOn v3.0
PIN	Personal Identification Number
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

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
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
eKey	USB smart card token that is used for two-factor authentication.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS ISO/IEC Guide 65

Term	Definition and Source
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
GINA	The graphical identification and authentication (GINA) library is a component of some Microsoft Windows operating systems that provides secure authentication and interactive logon service.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.
Iris	Biometric iris image.
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.
MyKAD	Official compulsory smart identity card of Malaysia. It contains a smart card chip.
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.
User	Any entity (human or external IT entity) outside the TOE that interacts with the TOE.

--- END OF DOCUMENT ---