CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science,
Technology and Innovation

C005 Certification Report

MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6

File name: ISCB-5-RPT-C005-CR-v1a
Version: v1a
Date of document: 11 April 2011
Document classification: PUBLIC

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

C005 Certification Report

MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6

11 April 2011

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:	C005 Certification Report – MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6
DOCUMENT REFERENCE:	ISCB-5-RPT-C005-CR-v1a
ISSUE:	v1a
DATE:	11 April 2011

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 was 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 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 11 April 2011, 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.

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	30 March 2011	All	Final Released
v1a	11 April 2011	Page iv Page 1 (paragraph 1)	Add the date of the certificate. Refine the sentence '...an access control software ~~and input parameters validation~~ for web applications.'

Executive Summary

MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 from MagnaQuest Solutions Sdn Bhd is the Target of Evaluation (TOE) for Evaluation Assurance Level (EAL) 4 evaluation*.* MQAssure™/AppShield (hereafter referred as Appshield); integrated with MQAssure™/IAM (hereafter referred as IAM) provides security to web applications by enforcing authentication and authorisation. It provides multifactor authentication capability to the web applications without modifying application code.

AppShield is use to prevent a number of common input tampering attacks by scanning all the input parameters and validating the requests against the rules defined for the web application.

IAM (Identity and Access Management) is a centralised identity and access management platform. It provides the back bone for the AppShield by providing centralised policy management, session management and audit logging.

In the overall infrastructure, AppShield acts as a policy enforcement agent for the web applications. Whereas, the IAM provides a centralised administration console through which the administrators can create and enforce various policies to control the access to various web application resources protected by AppShield.

IAM supports various authentication schemes such as User name/password, smartcard, biometric and USB token which is leveraged by AppShield to enforce multifactor authentication for web applications. The TOE can also support credentials from the smartcard reader of Smartek CID from Integrity and SafeNet iKey USB tokens.

The MQAssure™ Client Component (Client) provides a browser plug-in that communicates to the tokens and devices to retrieve the user credentials. The role of the client is simply as a mechanism to assist the entry of authentication credentials. The client is not part of the TOE.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions, the intended environment and the security requirements for the TOE, in addition to 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 MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6, to the Common Criteria (CC) evaluation assurance level EAL4. The report confirms that the product has met the target assurance level of EAL4 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 March 2011.

Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 evaluation meets all the conditions of the Arrangement on the Recognition of

Common Criteria Certificates and that the product 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 the MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 meets their requirement and security need. It is recommended that prospective users of MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 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) is a software product, which comprises of MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6. The MQAssure™/AppShield v1.2_CR6 (hereafter referred as Appshield) combined with MQAssure™/IAM v1.0_CR6 (hereafter referred as IAM) is an access control software for web applications. The TOE controls access to web filtering applications by enforcing authentication and authorisation using multifactor authentication schemes. It is also capable of session control, and request validation based on its core engine policy and rules.

2 IAM or Identity and Access Management is the core engine of the TOE. It is a centralised identity and access management platform that provides the back bone for the AppShield security functionality. In the overall infrastructure, AppShield acts as a policy enforcement agent for the web applications.

3 The security features within the scope of the evaluation for IAM includes:

a) Multifactor User Authentication which includes MyKad-Biometric, iKey-PIN or password.

b) TOE Administration which provides a web based GUI console for the administrator to configure and manage the TOE.

c) Security Audit which generates audit records for relevant authentication events and access events to various objects.

4 The security features within the scope of the evaluation for AppShield includes:

a) Access Control which enforces access control policy decision made by the IAM.

b) HTTP request validation which protects the web applications from common input tampering attacks.

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	C005
TOE Name and Version	MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6
Security Target Title	Security Target for the MQAssure™/AppShield v1.2 Integrated with MQAssure™/IAM v1.0
Security Target Version	v1.21

Security Target Date	3 January 2011
Assurance Level	EAL4
Criteria	Common Criteria Part 1, Common Criteria Part 2, Common Criteria Part 3 Version 3.1 Revision 3
Methodology	Common Methodology for IT 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 EAL4.
Sponsor and Developer	MagnaQuest Solutions Sdn Bhd A-2-07 & A-2-09 SME Technopreneur Centre, 2270, Jalan Usahawan 2, 63000 Cyberjaya Selangor Darul Ehsan MALAYSIA
Evaluation Facility	CyberSecurity Malaysia MySEF

1.3 Security Policy

6 AppShield enforces access control policy decisions made by the IAM server. The access control decisions are made based on user roles, requested resources and requested operations. The policy management component of IAM allows the administrator to define various access control policies.

7 IAM is a centralised identity and access management platform by providing centralised policy management, session management and audit logging. IAM provides a centralised administration console through which the administrators can create and enforce various policies to control the access to various web application resources protected by AppShield.

8 IAM supports various kinds of security policies for authorisation like location-based (IP Address), Time-based, strong password and password expiry which are enforced by AppShield. The IAM session manager performs various session management activities like session timeout and forced logoff. AppShield validates the session through the IAM session manager each time an access request comes to the web application. This policy rules should be implemented in accordance with users own organisation IT policy.

9 The security policy of MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 is expressed by the set of security functional requirements which includes audit, user data protection, identification and

authentication, security management, and TOE access. Further details on these security policies may be found in Section 5 of the ST (Ref [6]).

1.4 TOE Architecture

10 In order to secure a web application, AppShield need to be deployed in the same application server as the application being protected and configured to intercept the HTTP requests from the users to that application. This enables AppShield to intercept the user requests to the protected web application and redirect the user to an appropriate authentication scheme of IAM based on the authentication policies governing that user.

11 Referring to following Figure 1, IAM is represented as IAM Core or Core Security Services subsystem. Meanwhile, AppShield is represented as Appshield SSO or Access Control subsystem.

12 Through these interfaces the AppShield then enforces the access control, input filtering and session redirection of users. Identity management of a user is identified in terms of user and roles. Figure 1 illustrates the architecture of the TOE in terms of subsystems, modules and interactions.

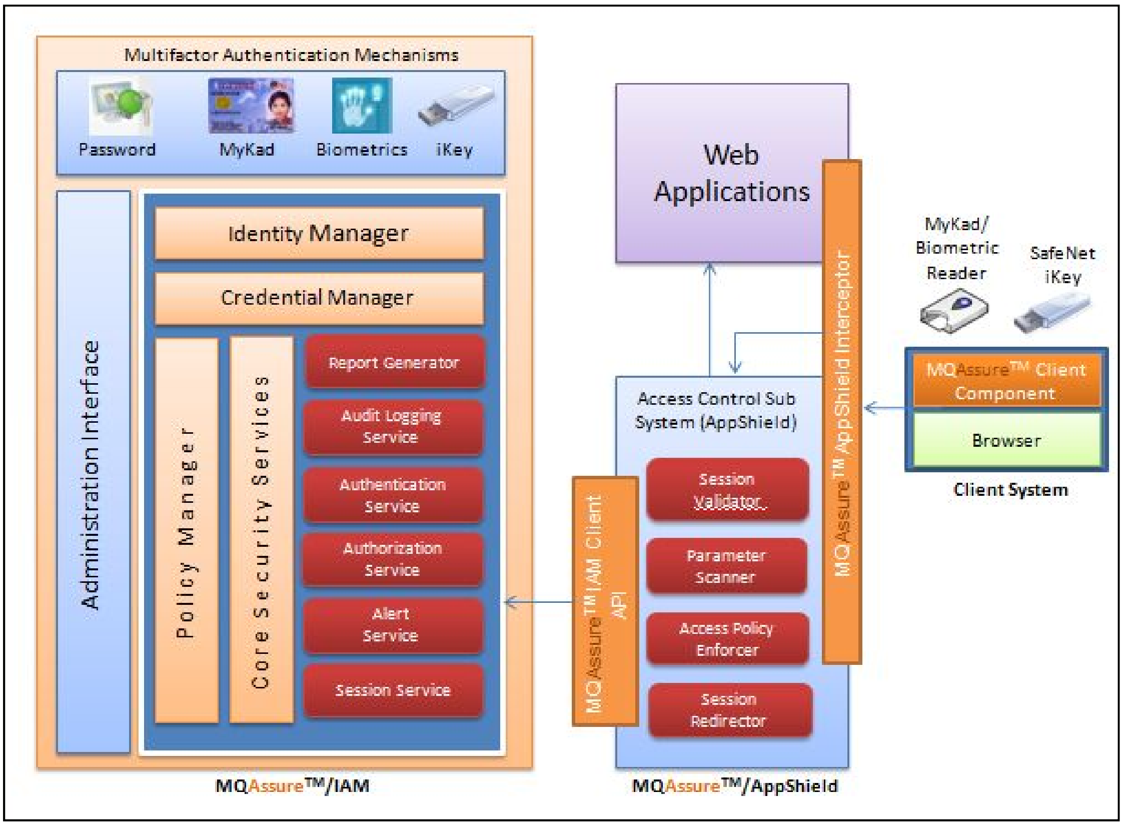

Figure 1: Subsystem of the TOE

13 The TOE is made up of several subsystems and module as following:

a) IAM subsystem – provides multifactor authentication functionalities which managing the authentication schemes.

i. Identity Manager module – provides centralized management of identities such as Users, Roles and Resources.

ii. Credential Manager module – provides centralized management of user credentials with respect to the different authentication schemes.

iii. Core Security Service module – provides cryptographic library to encrypt and decrypt user credentials. These services are used for encrypting the user credentials before it is stored into the database and also for decrypting the same after retrieving from the database.

iv. Policy Manager module – provides management for the authentication and authorization policies for the AppShield instances. Through the administration console, the authorized administrator can define access policies for various resources.

v. Authentication Service module – provides the authentication functions to AppShield. The authentication service makes use of a set of authentication plug-ins to implement the authentication logic. Authentications plug-in are implemented for MyKad-Biometric, iKey-PIN and password authentication schemes.

vi. Authorization Service module – verifies the access request forwarded by the Session Validator service of AppShield against the list of policies on the server.

vii. Alert Service module – provides the functionality to notify a configured user upon the detection of a specific event in the system such as security policy violation. The alert service uses email as the medium of notification.

viii. Session Service module – provides the centralized management of user sessions and continuously monitors the user activities on the session and the session expiry

b) Administration Interface subsystem – provides a web based administration console (GUI) for managing identities, policies, resources and audit logs on the IAM server.

i. Identity Manager – provides centralized management of identities such as Users, Roles and Resources, through the Administration console (web GUI).

ii. Policy Manager – provides policies management through the Administration console (web GUI).

iii. Session Service – provides the centralized management of user sessions through the Administration console (web GUI).

iv. Report Generator – provides various searching filters to search audit log through the Administration console (web GUI).

c) Audit Log subsystem – provides logging of an audit record, searching based on various filters, archiving the audit records. Audit log subsystem provides two types, which are Audit Logon service and Data Transaction Log events.

i. Logon Service – provides API to audit User Login, User Logout, Login Time out, Login Max Time out and Login Failure.

ii. Transaction Log – provides API to audit all data access and transactions.

iii. Report Generator – provides a Report Generator service, which calls the Logon Service and Transaction Log service to generate audit reports for Logon Events and Transaction Log events in various formats such as CSV, Excel, XML and PDF.

d) Access Control subsystem – provides access to protected application resources is as per the organisational policies and ensure proper trail of the user access to the protected resources.

i. AppShield Interceptor – provides interception of HTTP requests originating from the web clients to a protected application resource. After intercepting an HTTP request, the interceptor validates the user session, validates the request parameters, verifies the access policy and enforces the policy decisions.

ii. Parameter Scanner – provides scanning of all the input parameters from HTTP Request Object and validates against the rules defined for the web application. This service is configurable to add or modify various parameter validation rules. The parameter scanner ensure that all input data from request URL, query string, headers and cookies is validated against Cross site Scripting, file inclusion, SQL injection and cookie poisoning.

iii. Session Validator – provides validation of the session parameters of the user requests to verify that user has a valid session or not.

iv. Access Policy Enforcer – enforces the policy decisions made by the Authorization Service and make audit logs for the auditable access events. Authorization Service returns the policy decision (Allowed/Denied) to Access Policy Enforcer.

v. Session Redirector – redirect user request to respective web application resource once the user is authenticated and authorized to access the requested protected resource.

vi. IAM Client API – provides Service Locators and Business Delegates to communicate with Core Security Services.

14 The underlying hardware and software that are used to support the TOE are described in Section 1.2.1 of the Security Target (Ref [6]).

1.5 Clarification of Scope

15 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) **Strong Multifactor User Authentication** – IAM accepts multiple authentication schemes including MyKad-Biometric, iKey-PIN and/or password.

b) **TOE Administration** – IAM provides a web based GUI console for the administrator to configure and manage the TOE. This includes the management capability of identity management, session services, policy management, and audit reporting.

c) **Security Audit** – IAM provide the ability to generate audit records for relevant authentication events such as Login, Logout, Login failure, Logout failure, Account locks. This function also includes audit generation of access events such as creation, modification, deletion, approval, and denial of various objects.

d) **Access Control** – AppShield enforces access control policy decisions made by the IAM. The access control decisions are made based on User role, requested resource and requested operations. The policy management component of IAM allows the administrator to define various access control policies.

e) **HTTP request validation** – AppShield protects the web applications from common input tampering attacks by scanning the input parameters and validate the requests against the rules defined for the web application.

16 The TOE is designed to be suitable for use in well-protected environments that have affective countermeasures. The environment for the TOE should be physical and logically secured against unauthorized personnel and network access in accordance with administrator guidance that is supplied with the product.

17 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.

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

a) All underlying supporting hardware and software of both IAM and AppShield are not considered part of the TOE, including the MQAssure™/IAM Database and MQAssure™/IAM Client Component.

b) Web applications protected by AppShield are also part of the environment.

c) The client authentication component is a mechanism to assist the entry of authentication credentials and not part of the TOE.

1.6 Assumptions

19 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 MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 defined in subsequent sections and in the Security Target (Ref [6]).

1.6.1 Usage assumptions

20 Assumption for the TOE usage listed in the ST includes:

a) Authorized administrators and users are assumed to be non-hostile and trusted to perform all their duties in a competent manner.

1.6.2 Environmental assumptions

21 Assumption for the TOE environmental listed in the ST includes:

a) The TOE shall be hosted inside of a physically secure area.

b) The TOE environment will provide the following services to support the TOE: mail server to facilitate alerts from TOE in the form of email, and reliable time stamps to the TOE for audit log generation.

c) The environment is configured to block all traffic to the IAM server except for traffic required to perform security functionality.

d) The IT environment will provide a secure channel so that all potentially valuable information (including credentials and enterprise data) is protected between the user and AppShield server.

e) The IT environment will implement gateway filtering; only allowing HTTP and HTTPS traffic to pass through to AppShield.

f) The IAM database is located within the enterprises network boundary and is configured so that only TOE administrators can directly access the interface of the database.

1.7 Evaluated Configuration

22 This section describes the configurations of the TOE that were included within the scope of the evaluation.

23 MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 is software that will be hosted on a server. The TOE is delivered in the CD/DVD media that contain the TOE, related documentation and supporting software.

24 Upon acceptance, the client administrator will need to perform verification and identification of the installation CD/DVD media with reference to the preparative guidance (Ref [10]).

25 After verification is found to be consistent, administrator will configure the environment of the TOE based on requirement and procedure listed in the installation document (Ref [11]).

26 Table below list the environment requirements which include software and hardware component needs for installation of the TOE and supporting the security functionality.

Table 2: TOE hardware and software component

Item	Description	Scope
Hardware	Server Hardware - A standard workstation or server class machine with 2.4 GHz or higher Intel processor, 2 GB or more RAM, running Windows 2003 Server	Environment

	Client Hardware - A standard workstation or laptop with 1.6 GHz or higher Intel/AMD processor, 1 GB or more RAM, running Windows XP or Vista or 2003 Server - E-ID Smart Card (For evaluation purpose, Malaysian Identity Card (MyKAD) is used) - E-ID Smart Card reader (For evaluation purpose, Smartec CID version xx is used. The reader must be PC/SC compliant) - USB token (For evaluation purpose, SafeNet iKey 2032 is used)	
Software	Application Server - GlassFish 2.1 - Tomcat Server 5.5.9	Environment
	Database Server - MySQL 5.0	
	Mail Server - SMTP Server - POP3 Server	
	Browser - IE v6.0 to IE v8.0	
	Client Component - Smartec CID Drivers (Not applicable if user not using MyKad/Biometric Scheme) - SafeNet iKey 2032 Drivers (Not applicable if user not using iKey/PIN Scheme) - MQAssure™ Client Components version CR3 (Not applicable if user only use Password Scheme) - IE v6.0 to IE v8.0	
Firmware	Specific to the Hardware.	Environment

1.8 Delivery Procedures

27 MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 is sent to the customers using the procedure described in the delivery documentation (Ref [15]) which ensures that the MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 is securely transferred from the development environment into the responsibility of the customer. The delivery procedures are outlined below.

28 Procurement of the TOE begins once the customer agrees on the purchase of the product and an exchange of funds between the customer and MagnaQuest Sdn Bhd occurs. Only after licensed agreement is duly signed by both parties, delivery of the TOE is then processed. The TOE will never be shipped to customers without the license agreement first being signed.

29 The TOE is manufactured at the development site by the responsible development team member. The content of the CD/DVD media is then be hashed against MD5 using a tool available in the public domain that are conformant to RFC 1321.

30 CD media containing the TOE package, related documentation and supporting software is sent via standard couriers or hand-delivered by developer's representative to the customer's premises based on customer choice. The integrity of the TOE can be verified upon delivery using software hashes. If the product is sent using courier, a shipping notice is generated and forwarded to the email address of the customer's primary point of contact.

31 The developer also provides support for installation of TOE, client training and issue of supporting hardware components based on client's request. The supporting hardware is delivered by the developer representative to the customer's premises along with TOE if TOE is also hand-delivered.

32 Upon receipt of the TOE CD/DVD media installation package and license key, the client administrator is required to refer to preparative guidance document (Ref [10]) for identification and verification of the package content by performing hashes checks against the list of hash codes delivered by the developer.

33 Listed below are the four steps for customers to verify the TOE CD/DVD media package:

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

b) Performing a hash of all files/packages located on the media and performing a compare against the hashes stated in the license key document,

c) Installation of the TOE with the supplied license key, and

d) Verification of the TOE version as part of the installation process (identified in one stage of the TOE installer).

34 After the verification of the installation package and licence key, the administrator needs to complete secure preparation of the operational environment of the TOE according to the installation document (Ref [11]).

1.9 Documentation

35 To ensure continued secure usage of the product, it is important that the MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 is used in accordance with guidance documentation.

36 The following guidance documentation is provided by the developer as guidance to ensure secure usage and secure installation of the product:

a) [LET] MQAssure™ TOE Delivery Letter of Acceptance (Ref [8]),

b) [HASH] MQAssure™ Hash values of TOE CD Installer (Ref [9]),

c) [PPD] MQAssure™/Appshield v1.2 integrated with MQAssure™/IAM v1.0 Preparative Procedure Document (Ref [10]),

d) [IM] MQAssure™/Appshield v1.2 integrated with MQAssure™/IAM v1.0 Installation Manual (Ref [11]),

e) [AM] MQAssure™/Appshield v1.2 integrated with MQAssure™/IAM v1.0 Administration Manual (Ref [12]),

f) [UM] MQAssure™/Appshield v1.2 integrated with MQAssure™/IAM v1.0 User Manual (Ref [13]),

g) [SUG] MQAssure AppShield/IAM Supplementary Document for User Guidance (Ref [14]),

h) [DEL] MQAssure™/Appshield v1.2 integrated with MQAssure™/IAM v1.0 Delivery Procedure Document (Ref [15]), and

i) [CID] Installation Manual CID 308 Card Reader (Ref [16]).

2 Evaluation

37 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 4 (EAL4). 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

38 The evaluation activities involved a structured evaluation of MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6, including the following components:

2.1.1 Life-cycle support

39 An analysis of the MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 configuration management system and associated documentation was performed. The evaluators found that the MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 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.

40 It is evaluated that the implemented configuration management system can control changes to those items that have been placed under configuration management system. The developer's configuration management system was also observed during the site visit, and it was found security flaws under configuration management ensures that security flaw reports are not lost or forgotten, and allows a developer to track security flaws to their resolution. This is evaluated to be consistent with the provided evidence.

41 During the site visit the evaluators examined the development security documentation and determined that it detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 design and implementation. The evaluators confirmed that the developer used a documented life-cycle model which provides necessary control over the development and maintenance of the TOE by using the procedures, tools and techniques described by the life-cycle model.

42 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 during distribution to the consumer.

2.1.2 Development

43 The evaluators analysed the MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and modules. The design described the TOE subsystems to sufficiently determine the TSF boundary, and provides a description of the TSF internals in terms of modules. It provides a detailed description of the SFR-enforcing modules and enough information about the SFR-supporting and SFR-non-interfering modules for the evaluator to determine that the SFRs are completely and accurately implemented.

44 The evaluators analysed the MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 security architectural description and determined that the delivery and installation process was secure and the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

2.1.3 Guidance documents

45 The evaluators examined the MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 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

46 Testing at EAL4 consists of assessing developer tests, performing independent function test, and performing penetration tests. The MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 testing was conducted at CyberSecurity Malaysia MySEF and at the developer's site where it was subjected to a comprehensive suite of formally documented, 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 Assessment of Developer Tests

47 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).

48 The evaluators analysed the developer's test coverage and depth analysis 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 implementation

representation, functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

49 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.

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

Table 3: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
To verify that the TOE provides quality checks on TOE user authentication based on the access control policy, password policy etc setup by the Administrator and to test the combination of multiple authentication schemes such as: • MyKad-Biometric • iKey-PIN • Password	Strong Multifactor User Authentication	Admin Console User Interface Client Components	PASS. The output shows that the TOE identification and authentication function as per policies setup by the Administrator.
To verify and observe the security configuration made using Administrator web based console. The test covers: • Identity management • Session Services • Policy management • Audit reporting	TOE Administration	Admin Console User Interface Client Components Resources	PASS. The output shows that the TOE functions as per security configuration setup by the Administrator.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
This includes the observation on password expiration settings and implementation.			
To test audit records generation for relevant authentication and management events such as: • Login and logout • Login and logout failure • Account locks • Access events such as creation, modification, deletion, approval and denial of various objects. • Email alerts on potential security violation This includes the observation of transaction logs behaviour on how the TOE tie user ID to event and vice versa.	Security Audit	Admin Console User Interface Client Components	PASS. The output shows that the TOE generates audit record for the relevant security events and those users that have been granted explicit read access can read the audit record.
To verify the TOE security functions of handling user access to the web resources and admin web console. The test covers: • Intercepting HTTP/HTTPS request • HTTP/HTTPS input	Access Control & HTTP/HTTPS Request Validation	Admin Console User Interface Client Components	PASS. The output shows that the access to the web resources and admin web console is based on user role and

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
parameter scanner • Validation of user session • Session expiration • Validation and policy enforcement on user request to access a web resource			parameters like IP address and time of access, setup by the Administrator.

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

2.1.4.3 Penetration Testing

52 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE and to determine whether these were exploitable in the intended operating environment of the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, security architecture description, and implementation representation.

53 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing Basic and Enhanced-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.

54 The penetration tests focused on:

a) Scanning;

b) Physical Password Attacks;

c) Sniffing;

d) Cookies Manipulation;

e) Hidden Field Manipulation;

f) Logs Flooding;

g) Strip SSL; and

h) Session ID Analysis.

55 The penetration testing did not uncover any exploitable vulnerability in the anticipated operating environment. However, the results of the penetration testing note that a number of additional vulnerabilities exist that are dependent on an attacker effort, time, skill/knowledge, and focused tools/exploits use to gather the TOE and environment configuration information. Therefore, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment.

2.1.4.4 Testing Results

56 Tests conducted for the MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

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

3 Result of the Evaluation

58 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™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 performed by CyberSecurity Malaysia MySEF.

59 CyberSecurity Malaysia MySEF found that MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 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 EAL4.

60 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

61 EAL4 provides assurance by a full Security Target (ST) and an analysis of the security functions in the ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation to understand the security behaviour.

62 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis demonstrating resistance to penetration attackers with an Enhance Basic attack potential.

63 EAL4 also provides assurance though the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

3.2 Recommendation

64 In addition to ensure secure usage of the product, below are additional recommendations for MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6:

a) Use the product only in its evaluated configuration;

b) The MQAssure™ Client Component, and supporting software and hardware for the MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6 were not evaluated. As such, it is recommended that these features are installed and configured in a secure manner;

c) The system owner should implement a separate management network to provide secure management of the MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6;

d) The system owner should manage the network by implementing a firewall and only allow HTTP and HTTPS traffic to pass through to AppShield;

e) The system owner should ensure that the IAM database is located within the enterprises network boundary and is configured so that only TOE administrators can directly access the interface of the database;

f) Digital certificate used in TOE environment is recommended to be verified by certificate authority; and

g) Ensure strict adherence to the delivery procedures.

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] Security Target for the MQAssure™/AppShield v1.2 Integrated with MQAssure™/IAM v1.0, Version 1.21, 3 January 2011

[7] Evaluation Technical Report MQAssure™/AppShield v1.2_CR6 integrated with MQAssure™/IAM v1.0_CR6, Version 1.5, 30 March 2011

[8] MQAssure™ TOE Delivery Letter of Acceptance, 12 November 2010

[9] MQAssure™ Hash values of TOE CD Installer, 15 November 2010

[10] MQAssure™/Appshield v1.2 integrated with MQAssure™/IAM v1.0 Preparative Procedure Document, version 1.7, 30 March 2011

[11] MQAssure™/Appshield v1.2 integrated with MQAssure™/IAM v1.0 Installation Manual, version 1.14, 11 Nov 2010

[12] MQAssure™/Appshield v1.2 integrated with MQAssure™/IAM v1.0 Administration Manual, version 1.10, 24 November 2010

[13] MQAssure™/Appshield v1.2 integrated with MQAssure™/IAM v1.0 User Manual, version 1.10, 24 November 2010

[14] MQAssure AppShield/IAM Supplementary Document for User Guidance, version 1.1, 15 Nov 2010

[15] MQAssure™/Appshield v1.2 integrated with MQAssure™/IAM v1.0 Delivery Procedure Document, version 1.9, 30 March 2011

[16] Installation Manual CID 308 Card Reader, version 1.0, 25 April 2007.

A.2 Terminology

A.2.1 Acronyms

Table 4: List of Acronyms

Acronym	Expanded Term

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
ICC	Integrated Circuit Card
IEC	International Electrotechnical Commission
ISO	International Standards Organisation
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 5: 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.

Term	Definition and Source
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
ISCB Personnel	Includes all members of the Certification Subcommittee, the Scheme Manager, the Senior Certifier, Certifiers and the Quality Manager.
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 ---