CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science, Technology and Innovation

C019 Certification Report
Employee Express (EmplX) Security Module v1.0 (Build SVR 2.0)

File name: ISCB-5-RPT-C019-CR-v1a
Version: v1a
Date of document: 4 November 2011
Document classification: PUBLIC

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

C019 Certification Report

Employee Express (EmplX) Security Module v1.0 (Build SVR 2.0)

4 November 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:	C019 Certification Report - Employee Express (EmplX) Security Module v1.0 (Build SVR 2.0)
DOCUMENT REFERENCE:	ISCB-5-RPT-C019-CR-v1a
ISSUE:	v1a
DATE:	4 November 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

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 4 November 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 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 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	28 October 2011	All	Final Released.
v1a	4 November 2011	Page iv	Add the date of the certificate.

Executive Summary

Employee Express (EmplX) Security Module v1.0 (Build SVR 2.0) (hereafter referred as EmplX Security Module) from MYwave Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation.

EmplX Security Module is part of EmplX online Human Resource Management Systems (HRMS). It is a software module designed to be used as a core security controlling module for a web-based application environment. The TOE provides core security functionality such as authentication, access control, secure communications and application security management

The security features within the scope of the evaluation includes:

- Access control – EmplX Security Module manages access control based on user IDs, user roles and access control lists. It maintains access control lists (ACLs) for each object within an organisation. Each ACL maps users and roles to the operations that they are permitted to perform on the object.
- Organisation Management – EmplX Security Module provides strict controls on organisation management. Only Super Administrators can manage the creation, modification and destruction of an organisation. Users and Supervisors can only operate within their organisation.
- Identification and Authentication – each user is required to successfully identified using user ID and authenticated using password before any interaction with protected resources within EmplX HRMS is permitted.
- Security Management - EmplX Security Module provides functions that allow management of the TOE and its security functions. It restricts access to the management functions based on the role of the user.
- Secure Communications - EmplX Security Module is able to protect the user data from disclosure and modification when it is sent from users' browser to the EmplX HRMS using the secure SSL channel.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for EmplX Security Module, 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 IT security evaluation of EmplX Security Module, to the Common Criteria (CC) evaluation assurance level of EAL 2 and that the evaluation was conducted in accordance with relevant criteria and the requirements of the Malaysia's Common Criteria Certification (MyCC) Scheme. The evaluation was performed by the STRATSEC.NET SDN BHD (stratsec) Security Evaluation Facility (STRATSEF) and was completed on 7 September 2011.

Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the EmplX Security Module 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 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 EmplX Security Module meets their requirement and security needs. It is recommended that prospective users of the EmplX Security Module 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), Employee Express (EmplX) Security Module v1.0 (Build SVR 2.0) (hereafter referred as EmplX Security Module) is a PHP module of EmplX Human Resource Management Systems (HRMS) web application hosted on a web server. It is designed to be used as a core security controlling module for a web-based application environment.

2 The TOE provides core security functionality such as authentication, access control, secure communications and application security management. All http requests to the web server will be meditated by the TOE before allowing access to the rest of the EmplX HRMS.

3 The security functionality that is within the scope of the evaluation includes:

a) **Identification & Authentication.** The TOE requires that the user (being an Employee, Supervisor, Administrator and Super Administrator) identify (user ID) and authenticate (password) themselves before performing any TOE security functionality mediated action on behalf of the user. The TOE checks the credentials presented by the user upon the login page against the authentication information in the database. Each users account only exists in the database that relates to the user organisation.

b) **Access Control.** The access control function permits a user to access a protected resource only if a user ID or role of the user has permission to perform the requested action on the resource.

c) **Security Management.** The TOE contains various management functions to ensure efficient and secure management of the TOE: user management, permission management for functions and data and organisation management. The TOE maintains four roles: Employee, Supervisor, and Administrator and Super Administrator, within the TOE to ensure that the functions are restricted to only those users that need to have access to privileged functions.

d) **Secure Communications.** The TOE provides a secure SSL channel between the user and the EmplX HRMS application.

e) **Organisation Management.** The TOE supports hosting multiple organisations within one TOE instance. The TOE provides strict separation of information, ensuring that an Employee or Supervisor from one organisation cannot modify the data in another organisation. Only Super Administrators have the privilege required to create, modify or delete users in different organisations. Each organisation is maintained and managed in its own database.

1.2 TOE Identification

4 The details of the TOE are identified in Table 1 below.

Table 1: TOE Identification

Scheme	Malaysian Common Criteria Evaluation and Certification

	(MyCC) Scheme
Project Identifier	C019
TOE Name	Employee Express (EmplX) Security Module
TOE Version	1.0 (Build SVR 2.0)
Security Target Title	Employee Express Security Module (EmplX Security Module) Security Target
Security Target Version	1.0
Security Target Date	9 August 2011
Assurance Level	Evaluation Assurance Level 2 (EAL2)
Criteria	Common Criteria July 2009, Version 3.1, Revision 3
Methodology	Common Methodology for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL2
Sponsor and Developer	MYwave Sdn Bhd 1-3-21, Krystal Point Corporate Park, Jalan Tun Dr Awang, 11900 Bayan Lepas, Pulau Pinang MALAYSIA
Evaluation Facility	STRATSEC.NET SDN BHD known as STRATSEF

1.3 Security Policy

5 In order to provide user data protection, the TOE enforces an access control policy on protected resource. The TOE maintains access control lists (ACL) for each object within an organisation. Each ACL maps users and roles to the operations that they are permitted to perform on the object.

6 After a user identifies and authenticates to the TOE, the TOE will check all HTTP request to the protected resource from the user. The TOE will permit a user to access a protected resource only if a user ID or role of the user has permission to perform the requested action on the resource.

7 The detail of the access control policy is described in Section 5 and Section 6 of the Security Target (Ref [6]).

1.4 TOE Architecture

8 The Security Target defines clearly both logical and physical boundaries.

9 Figure 1 below provides the major architectural components that comprise the entire EmplX HRMS web-based application and identifies all the major supporting elements that combine to deliver the system. The TOE, which is one component of the EmplX HRMS, is a PHP module running on the web server.

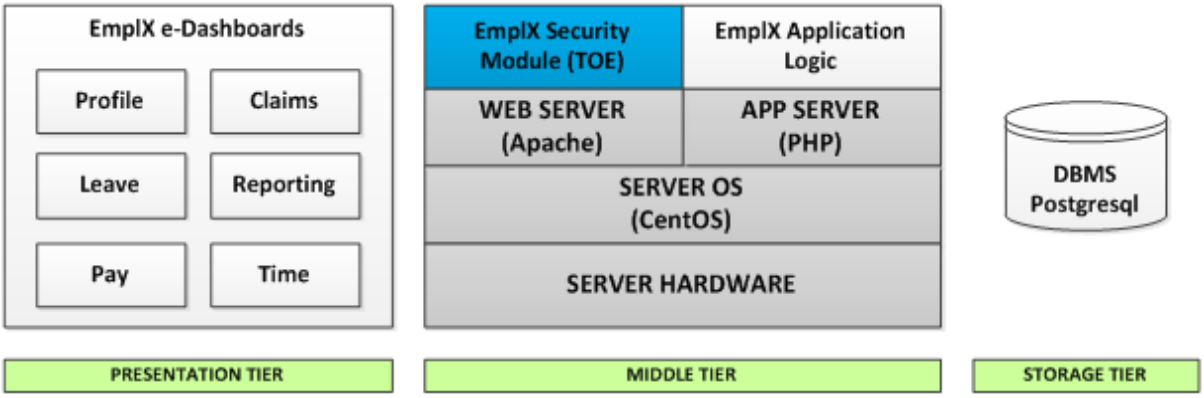

Figure 1: EmplX HRMS System Architecture

10 EmplX e-Dashboard provides the core interface elements to the end-user. The GUI will only contain the applications the user can execute when they have successfully identified and authenticated.

11 The EmplX HRMS is supported by the EmplX Security Module (TOE) and EmplX Application Logic components that provide the core functionality of the system. The web server, application server, the DBMS, and underlying operating systems are all essential to the delivery of the solution. However, they are not in the scope of the evaluation.

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

1.5 Clarification of Scope

13 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) **Identification & Authentication.** When a user issues a request to the TOE to access a protected resource (methods or PHP pages), the TOE requires that the user (Employee, Supervisor, Administrator, and Super Administrator) identify and authenticate themselves before performing any TOE security functions mediated action on behalf of the user. The TOE checks the user's credential against the authentication information in the database during login. Each users account only exists in the database that relates to the user organisation.

Users' passwords are hashed before being used to authenticate the user or when users change their passwords, and is being written to the database.

b) **Access Control.** The TOE enforces an access control policy on protected resource. After a user identifies and authenticates to the TOE, the TOE will check all HTTP request to the protected resource from the user. The TOE will permit a user to access a protected resource only if a user ID or role of the user has permission to perform the requested action on the resource. The TOE maintains access control lists (ACLs) for each object within an organisation. Each ACL maps users and roles to the operations that they are permitted to perform on the object.

There are 4 users maintained by the TOE. They are Employee, Supervisor, Administrator and Super Administrator. Each type of user will have different access rights to a protected resource. All users will have a unique user ID.

c) **Security Management.** The TOE contains various management functions to ensure efficient and secure management of the TOE as follows:

i) user management – only Administrator is responsible to query, create, delete, and modify users into the respective organisation.

ii) permission management for functions and data - Administrator and Supervisor role can modify the access control list, mapping of users to roles as well as modifying the user accounts. Supervisor can only do it if he/she is the member of the organisation that he/she is modifying.

iii) organisation management – the TOE maintains four roles within the TOE to ensure that the functions are restricted to only those users that need to have access to privileged functions.

d) **Secure communications.** The TOE initiates a Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols between the user's browser and the EmplX HRMS application when the user is trying to access EmplX HRMS.

It provides a rich API which provides functionality for:

i) dealing with protocol methods,

ii) implementing ciphers,

iii) managing keys,

iv) implementing sessions and context, and

v) establishing and managing connections.

e) **Organisation Management.** The TOE supports hosting multiple organisations within the one TOE instance. When users submit their user IDs and passwords for authentication, they also have to submit their organisation to the TOE. The TOE will reference the authentication data to the correct section in the database by selecting the information from the selected organisation.

Thus the TOE provides strict separation of information, ensuring that an Employee or Supervisor from one organisation cannot modify the data in another organisation. Only Super Administrators have the privilege required to create users in different organisations. Each organisation is maintained and managed in its own database.

14 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.

15 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) EmplX HRMS application; other than the EmplX Security Module.

b) Web server (Apache) and application server (PHP 4.4.9)

c) Database (RDBMS) – Postgresql 8

d) Operating System – CentOS 5

e) Client browsers.

1.6 Assumptions

16 This section summarises the security aspects of the environment or configuration in which the IT product is intended to operate. Consumers should understand their own IT environments and what is required for secure operation of the TOE as defined in the Security Target (Ref [6]). Consumers can make informed decisions about the risks associated with using the TOE by considering assumptions about usage and environment settings as requirements for the product's installation and its operating environment, to ensure its proper and secure operation.

1.6.1 Usage assumptions

17 Assumptions for the TOE usage listed in the Security Target are:

a) All management of the TOE will be performed through the management interfaces of the TOE and not through the underlying environment.

b) It is assumed that the administrator who manages the TOE is not hostile and is competent.

1.6.2 Environment assumptions

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

a) The TOE environment will provide appropriate authentication and authorisation controls for all users and administrators in the underlying environment (including the Operating System, RDBMS, and Web Server)

b) It is assumed that the servers that host the web and database servers are hosted in a secure operating facility with restricted physical access with non-shared hardware.

c) It is assumed that the databases in the TOE environment have been correctly configured according to the principle of least privilege.

d) It is assumed there is appropriate network layer protection, that there is a firewall in place that only permits access through required ports for external users to access the web server.

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

f) It is assumed that the web server has SSL certificates installed and are valid (not revoked or expired), are sourced from a trusted entity.

1.7 Evaluated Configuration

19 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 installation guide (Ref [9]).

20 The TOE is a PHP module which is part of the EmplX Human Resource Management System (HRMS) web application hosted on an Apache web server with all the PHP modules. A typical installation of the TOE can be found in Figure 1.

1.8 Delivery Procedures

21 This section aims to provide direction on the methods used to deliver the TOE to consumers or users of the product. In this case, the end recipient of the TOE is intended to be developers of HRMS solutions and capabilities that are to be integrated with the EmplX HRMS solution.

22 This section describes all procedures that are necessary to maintain security when distributing the TOE from the build environment to the development environment for use by the development team.

23 The delivery of the TOE from the build environment to the EmplX HRMS development environment goes through the following phases:

a) **Development and build.** The development and build process are controlled within the MYwave development environment. Section 1.2.1 of the MYwave Developer's Guidance (Ref [10]) provides specific direction on the development process and the elements around making a specific build of the TOE.

b) **Released**. A specific set of procedures are followed before a new version of the TOE or any key component can be released, the procedures include the following:

i) A pre-release meeting will be held to determine all relevant documents are in place.

ii) The pre-release meeting will also determine the release version of the Applications.

iii) The release date will be established.

iv) The release version will be then reflected correctly into the corresponding documents, ie, Modules/Bug Fix tracking, Process Flow Diagram and Data Flow Diagram.

v) All documents to be submitted for approval by respective Managers.

vi) Notification will be sent out to respective Clients to notify the blackout period prior to Release.

c) **Delivery and acceptance.** Once the new version of the TOE or key application component is released it is verified by the developers by checking the version of the TOE and checking the version with the Release logs. Only after a successful verification will the TOE be accepted and be put onto production server for use.

24 Once the Super Administrator got access to the EmplX Security Module, he/she should determine the version by opening up the code and checking the comment section found at the top of the code of EmplX Security Module.

1.9 Documentation

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

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

a) MYwave Application Security Users Guide (Ref [8])

27 The following guidance document are provided to the administrator as guidance for secure installation of the product:

a) EmplX Security Module EAL2 Guidance Documentation (Ref [12])

b) MYwave Application Installation Guide (Ref [9])

c) MYwave Application Developer's Guidance (Ref [10])

d) MYwave Application Create New HRMS Company (Ref [11])

2 Evaluation

28 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 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

29 The evaluation activities involved a structured evaluation of EmplX Security Module, including the following components:

2.1.1 Life-cycle support

30 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

31 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

32 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).

33 The evaluators examined the TOE 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.

34 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

35 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it's 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

36 Testing at EAL2 consists of assessing developer tests, independent function test, and performing penetration tests. The testing was conducted by STRATSEF at stratsec lab in Plaza Sentral, Kuala Lumpur. 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

37 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).

38 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

39 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.

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

Table 2: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	STATUS
To test that the TOE apply SHA-2 policy in cryptographic hashing function align with FIPS 180-2.	FCS_COP.1	SSL_API	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE enforce the Access Control SFP on HTTP request on behalf of users. **Objects**: Protected resources (methods and HTML pages). **Operations**: Methods execution Serving of	FDP_ACC.1	ACCESS_API	**PASS**. The result shows that the TOE functions as per claims.

DESCRIPTION	SECURITY FUNCTION	TSFI	STATUS
HTML pages			
1. To test that the TOE enforce the Access Control SFP to objects based on the following: a. Subject attribute (ID of the user, corresponding user role) b. Object attribute (Access control list) 2. The Access Control List for an object permits the user ID to access that object; OR the Access Control List for an object permits the User Role to access that Object. 3. To test the TOE explicitly authorise access of subjects to objects based on the following additional rules: [the Super Administrator role can access all records and functions]. 4. To test that the TOE explicitly deny access of subjects to objects	FDP_ACF.1.1 FDP_ACF.1.2 FDP_ACF.1.3 FDP_ACF.1.4	ACCESS_API	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE authenticate each user before allowing any other TSF-mediated actions on behalf of that user	FIA_UAU.2	AUTH_API	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE identified each user before allowing any other TSF-mediated actions on behalf of that user	FIA_UID.2	AUTH_API	**PASS**. The result shows that the TOE functions as per claims.

DESCRIPTION	SECURITY FUNCTION	TSFI	STATUS
To test that the TOE enforce the Access Control SFP to restrict the ability to *write* or *delete* the security attributes that map user IDs to roles to only the users that are mapped to the Super Administrator role	FMT_MSA.1	SECMAN_API	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE enforce the Access Control SFP to provide *restrictive* default values for security attributes that are used to enforce the SFP.	FMT_MSA.3 .1	SECMAN_API	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE restrict the ability to change *default* for all TSF data	FMT_MTD.1a	SECMAN_API	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE restrict the ability to *query, modify, delete, create* the Access Control Lists, Mapping of users to Roles, User accounts to Supervisor, Super Administrator	FMT_MTD.1b	SECMAN_API	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE restrict the ability to [*modify*] the [User Password] to [Employee (that is related to the password), Supervisor (all users within the Organisation), Super Administrator (all users)].	FMT_MTD.1c	SECMAN_API	**PASS**. The result shows that the TOE functions as per claims.
The TSF shall restrict the ability to [*query, modify, delete, clear* [Create] the [Organisation] to [Super Administrator].	FMT_MTD.1d	SECMAN_API	**PASS**. The result shows that the TOE functions as per claims.
To test that the TOE is	FMT_SMF.1	SECMAN_API	**PASS.** Result

DESCRIPTION	SECURITY FUNCTION	TSFI	STATUS
capable of performing the following management functions: a) mapping user IDs to roles b) creation of users with default passwords c) deletion of users d) changing of passwords e) management of Access Control lists			as expected.
1. The TSF shall maintain the roles [Employee, Supervisor and Super Administrator]. 2. To test that the TOE able to associate users with the roles	FMT_SMR.1 FMT_SMR.1.2	SECMAN_API	**PASS.** Result as expected.
a) To test that the TOE maintain a communication path between itself and remote users that is logically distinct from other communication paths and provide assured identification of its end points and protection of the communicated data from modification or disclosure. b) To test that the TOE permit the remote users to initiate communication via trusted path c) To test that TOE maintain the trusted path for initial authentication	FTP_TRP.1.1 FTP_TRP.1.2 FTP_TRP.1.3	SECMAN_API	**PASS.** Result as expected.

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

2.1.4.3 Penetration Testing

42 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.

43 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.

44 The penetration tests focused on :

a) Injection attacks;

b) Cross-Site scripting;

c) Malicious file execution;

d) Information disclosure.

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

2.1.4.4 Testing Results

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

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

3 Results of the Evaluation

48 After due consideration during the oversight of the evaluation execution by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of EmplX Security Module performed by the stratsec Security Evaluation Facility which known as STRATSEF.

49 STRATSEF found that EmplX Security Module upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance level EAL2.

50 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

51 EAL2 provides a basic level of assurance by a limited Security Target and an analysis of the security functions in that Security Target, using a design document, architectural document, functional and interface specification and guidance documentation, to understand the security behaviour.

52 The analysis is supported by a search for potential vulnerabilities in the public domain, developer's test cases and independent testing (functional and penetration) of the TOE security functions.

53 EAL2 also provides assurance through unique identification of the TOE and implementation of a configuration management system so that there is no ambiguity in terms of which instance of the TOE is being evaluated.

3.2 Recommendation

54 In addition to ensure secure usage of the product, below are additional recommendations for EmplX Security Module users:

a) Developers and users of the TOE should review the intended operational environment and ensure that all elements are suitably maintained and addressed. It is important the following be continually maintained:

   i) The servers that host the web and database servers are hosted in a secure operating facility with restricted physical access with non-shared hardware.

   ii) The databases in the TOE environment have been correctly configured according to the principle of least privilege.

   iii) There is appropriate network layer protection in place that only permits access through required ports for external users to access the web server.

iv) The underlying operating system, web server, application server and DBMSS and are patched and hardened to protect against known vulnerabilities and security configuration issues.

v) That the web server has suitable transport layer encryption enabled for all authentications and sensitive data transfer and that this is supported by a certificate this is valid and generated by a trusted source.

vi) That secure coding principles are always followed so that injection and scripting vulnerabilities are not introduced into the operational environment.

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

c) The Super Administrator implements a regular external and independent testing programme to constantly monitor the security posture of the EmplX HRMS system.

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] Employee Express Security Module (EmplX Security Module) Security Target, version 1.0, 9 August 2011.

[7] Evaluation Technical Report EAL2 Evaluation of the EmplX Security Module, version 1.1, 25 October 2011.

[8] MYwave Application Security User Guide, v 2.00, 6 August 2010.

[9] MYwave Application Installation Guide, v 1.00, 5 October 2010.

[10] MYwave Application Developer's Guidance, v 1.00, 5 October 2010.

[11] MYwave Application Create New HRMS Company, v 1.00, 1 October 2010.

[12] EmplX Security Module EAL2 Guidance Documentation, v 0.5, 10 June 2011.

A.2 Terminology

A.2.1 Acronyms

Table 3: List of Acronyms

Acronym	Expanded Term
ACL	Access control list
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology (ISO/IEC 18045)
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body

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
PP	Protection Profile
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
Authentication Data	It is information used to verify the claimed identity of a user.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA.
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS ISO/IEC Guide 65.
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
FIPS 180-2	It is a Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology for Secure Hash Standard
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.

Term	Definition and Source
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy.
SHA-2	SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512) designed by the National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard. For the evaluation, SHA-256 is implemented only.
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE
Unauthorized users	Unauthorized users can mean a legitimate user with access rights to certain web resource, an external entity that has no rights to any protected web resource/data.
Users	It means any entity (human user or external IT entity) outside the TOE that interacts with the TOE. In this case, there are end users (Administrator, Supervisor and Employee, Super Administrator) of the TOE access the TOE through a web browser as well as Super Administrators who are also developers of PHP modules that use the TOE underlying functions.
User data	Data created by and for the user, that does not affect the operation of the TSF
TSC	TOE Scope of Control, the set of interactions that can occur with or within a TOE and are subject to the rules of the TSP
TSP	TOE Security Policy, a set of rules that regulate how assets are managed, protected and distributed.

--- END OF DOCUMENT ---