C030 Certification Report

Web Bytes Xilnex Framework version 3.0

File name: ISCB-5-RPT-C030-CR-v1a
Version: v1a
Date of document: 16 February 2012
Document classification: PUBLIC

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

C030 Certification Report

Web Bytes Xilnex Framework version 3.0

16 February 2012

ISCB Department

CyberSecurity Malaysia

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

Document Authorisation

DOCUMENT TITLE:	C030 Certification Report - Web Bytes Xilnex Framework version 3.0
DOCUMENT REFERENCE:	ISCB-5-RPT-C030-CR-v1a
ISSUE:	v1a
DATE:	16 February 2012

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

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

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

Printed in Malaysia

Foreward

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

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

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

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

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 3 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 3 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
v1	3 February 2012	All	Final Released.
v1a	16 February 2012	Page iv	Add the date of the certificate.

Executive Summary

Web Bytes Xilnex Framework Version 3.0 (hereafter referred as Xilnex Framework) from Web Bytes Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 1 evaluation.

The TOE is a distribution and synchronization platform which distributes subscribed applications to multiple clients as well performs data synchronisation between all the clients in the same group. The TOE comprises of two primary components as follows:

- **Client Software**. The client software that installs directly on each user's PC which operates the daily process and update based on the user activities.
- **Server Software**. The server software that extends client software with secure communication, identification and authentication, and data synchronization.

The security functions that the TOE provides include the following:

- **Secure Transmission** – All communications between the server and the client is through an SSL channel. It protects the user data from disclosure and modification. Note: In offline mode where the users have no connection to the server, users will still need to present their credentials (user ID, password and organization ID) to get the key for decrypting the local cache. The TOE will use the credentials to get the key back through a complementary function.
- **Access control** – The TOE allows users to launch only the applications they subscribed to as well as accessing the database. The TOE will check the user ID and their organization ID to ensure the applications that the user is allowed to run.
- **Identification and Authentication** – Users will have to present their credentials to the server for identification and authentication. Only after a successful identification and authentication will the user is allowed to launch the applications and access the user data at the backend and at the local cache. For this online identification and authentication, the user will need to be connected to the server.
- **Encryption** – Username and passwords are always hashed when they are being stored into the database and during authentication. The local cache is also encrypted and can only be accessed when users are successfully identified and authenticated.
- **Management –** The TOE contains various management functions to ensure efficient and secure management of the TOE:
    - User management;
    - Changing passwords; and
    - Configuration of Access Control list.

  The TOE maintains two roles to ensure that the functions are restricted to only the TOE administrator. The roles maintained by the TOE are users and administrator. The functions above, and indeed, aspects of these functions, are restricted based on these roles.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for Xilnex Framework, the security requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

This report describes the findings of the security evaluation of Xilnex Framework, to the Common Criteria (CC) evaluation assurance level EAL1 and the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]). The evaluation was performed by the STRATSEC.NET SDN BHD (stratsec) Security Evaluation Facility (STRATSEF) and was completed on 18 January 2012.

Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the Xilnex Framework evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificate. The product will be listed on the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement at www.commoncriteriaportal.org).

It is the responsibility of the user to ensure that the Xilnex Framework meets their requirement and security needs. It is recommended that prospective users of the Xilnex Framework 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), Web Bytes Xilnex Framework version 3.0 (hereafter referred as Xilnex Framework), is a distribution and synchronization platform which distributes subscribed applications to multiple clients as well performs data synchronisation between all the clients in the same group.

2 The TOE comprises of two major components that need to be installed at client and server side respectively as follows:

- **Client Software**. (Deployer and Cybernate API) The client software that installs directly on each user's PC which operates the daily process and update based on the user activities.
- **Server Software**. (Deployer and Cybernate API) The server software that extends client software with secure communication, identification and authentication, and data synchronization.

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

a) **Secure Transmission** – All communications between the server and the client is through an SSL channel. It protects the user data from disclosure and modification. Note: In offline mode where the users have no connection to the server, users will still need to present their credentials (user ID, password and organization ID) to get the key for decrypting the local cache. The TOE will use the credentials to get the key back through a complementary function.

b) **Access control** – The TOE allows users to launch only the applications they subscribed to as well as accessing the database. The TOE will check the user ID and their organization ID to ensure the applications that the user is allowed to run.

c) **Identification and Authentication** – Users will have to present their credentials to the server for identification and authentication. Only after a successful identification and authentication will the user is allowed to launch the applications and access the user data at the backend and at the local cache. For this online identification and authentication, the user will need to be connected to the server.

d) **Encryption** – Username and passwords are always hashed when they are being stored into the database and during authentication. The local cache is also encrypted and can only be accessed when users are successfully identified and authenticated.

e) **Management –** The TOE contains various management functions to ensure efficient and secure management of the TOE:

- User management;
- Changing passwords; and

- o Configuration of Access Control list.

The TOE maintains two roles to ensure that the functions are restricted to only the TOE administrator. The roles maintained by the TOE are users and administrator. The functions above, and indeed, aspects of these functions, are restricted based on these roles.

1.2 TOE Identification

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

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C030
TOE Name	Web Bytes Xilnex Framework
TOE Version	3.0
Security Target Title	Web Bytes Xilnex Framework Security Target
Security Target Version	1.1
Security Target Date	21 November 2011
Assurance Level	Evaluation Assurance Level 1 (EAL 1)
Criteria	Common Criteria for Information Technology Security Evaluation, July 2009, Version 3.1, Revision 3 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, July 2009, version 3.1 revision 3 (Ref [3])
Protection Profile Conformance	None.
Common Criteria Conformance	CC Part 2 Conformant. CC Part 3 Conformant. Package conformant to EAL1.
Sponsor and Developer	Web Bytes Sdn Bhd, Unit 1-2-33, Kompleks Mayang Mall, Jalan Mayang Pasir 1, 11950 Bayan Baru, Pulau Pinang MALAYSIA
Evaluation Facility	STRATSEC.NET SDN BHD also known as STRATSEF

1.3 Security Policy

5 In order to provide user data protection, the TOE enforces an access control policy on applications and user database. After a user identifies and authenticates to the TOE, the TOE will check the user ID and organization ID for the applications and database the user is allowed to access. The TOE maintains access control lists (ACLs) for each object within an organization. Each ACL maps users and roles to the operations that they are permitted to perform on the object.

6 The detail of the security policy of the TOE is expressed by the set of security functional requirements which includes cryptographic support, user data protection, identification and authentication, security management, and trusted path/channels. Further details on these security policies may be found in Section 4 of the ST (Ref [6]).

1.4 TOE Architecture

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

8 Physically, the TOE consists of the client software, and the server software.

9 A typical installation of the TOE can be found in Figure 1 below and identifies the various supporting components that combine to deliver the system. The TOE is an application that requires a server machine, operating system, database, and other supporting software as described in Section 1.4.1 of the ST (Ref [6]).

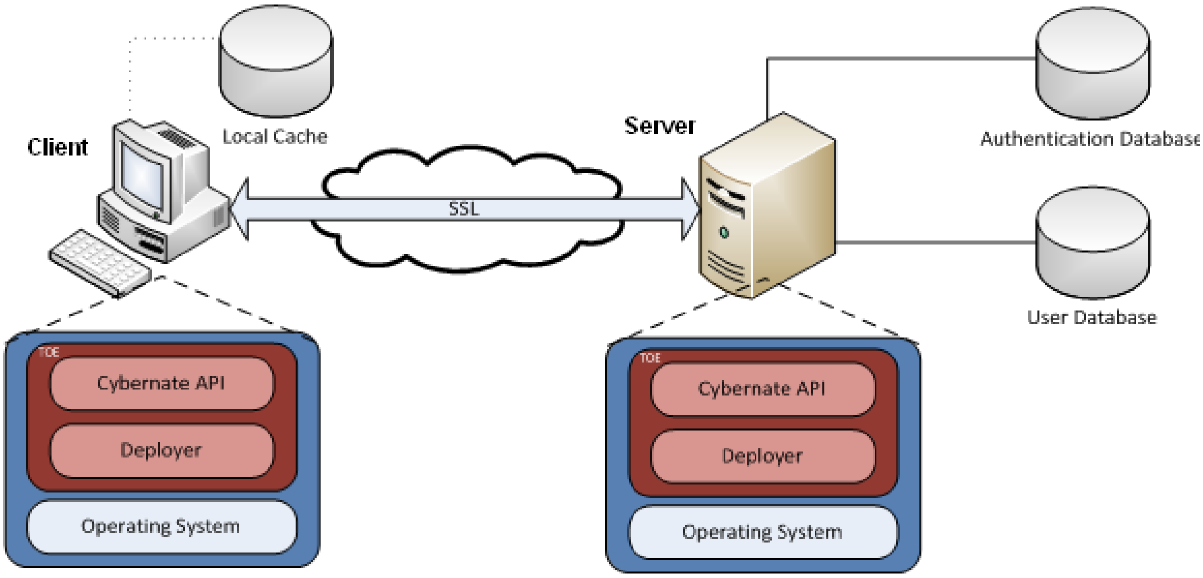

Figure 1: Xilnex Framework Architecture

10 The TOE consist of 2 modules as follows:

a) The Deployer module that handles the setup of the required folders, fonts and required libraries at the client side. The module detects the machine configuration and performs the necessary setup to enable applications to run. The Deployer module will download the Cybernate API from the server.

b) The Cybernate API provides the identification and authentication feature of the TOE. It also controls what applications can the user runs at the client side. Administrator can also creates, and delete users through this interface. Cybernate API will create a complete instance of the organization database at the client side (local cache). This local cache will be encrypted by Cybernate API using a random generated key. It also establishes the secure communication between the server and the client.

1.5 Clarification of Scope

11 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) **Secure Transmission** - the TOE established a trusted channel using the SSL protocol for the transfer of user data from the TOE to a remote instance of the TOE to ensure it protects the user data from disclosure and modification. The SSL session is based on mutual authentication of the TOE, and the remote instance, using installed digital certificates.

   The TOE will synchronize the user databases between all users within an organization. All clients will have a local instance of the database from the server. This enables users to work in offline mode when they do not have a connection to the server. Once connected to the server, the client will update the server with the latest data.

b) **Access Control** - The TOE enforces an access control policy on applications and user data. The TOE allows users to launch only the applications they subscribed as well as accessing the database at server side. The TOE will check the user ID and their organization ID for the applications and database the user is allowed to access. The TOE maintains access control lists (ACLs) for each object within an organization. Each ACL maps users and roles to the operations that they are permitted to perform on the object. The ACLs are stored at the server as well as in the client local cache to enable users to work offline without being connected to the server.

c) **Identification & Authentication** - The TOE requires the users (User or Administrator) to identify and authenticate themselves before performing any TOE security function mediated actions on behalf of the user. Users and administrator will login through an interface at the client side of the TOE. Only after a successful identification and authentication will the user is allowed to launch the applications and access the user data at the server and at the client local cache.

   Users will be locked out for 10 seconds if they failed their authentication 3 times.

d) **Encryption** – Username and password are always hashed when they are being stored into the database and during authentication. The local cache (local instance of the database), which is generated at the client side, is encrypted and can only be accessed when users successfully identify and authenticate themselves. The key for encryption is generated using random number functionality of .NET framework and will be stored at the server side. The key is zeroized at the client side when it has been used for encryption or decryption.

For users who are not connected to the server, upon the first logon by the user, a code is generated by the TOE. This code is generated from the local cache encryption key and the user credential (user ID, password and Organization ID). The code is stored at the client side in the Windows registry. Only with the correct credentials can the encryption key be generated back for decrypting the local cache. 1 code is generated for 1 user.

e) **Management** - The TOE contains various management functions to ensure efficient and secure management of the TOE:

- User management – only Administrator can query, create, delete, and modify users into the respective organization. Default password will be given to the users via email and need to be changed upon first logon.
- Changing password – all users can change their password through the client interface. All changing of password is allowed only in online mode where the client and the server are connected.
- Configuration of Access Control List (ACL) – Administrator can modify the ACL, mapping users to applications and database that they are allowed to access.

The TOE maintains 2 roles within the TOE to ensure that the functions are restricted to only those users that need to have access to privileged functions. The roles maintained by the TOE are: User and Administrator. The functions above, and indeed, aspects of these functions, are restricted based on these roles. There is only one administrator for each organization.

12 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.

13 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) An Operating System (Microsoft Windows XP, Windows Vista and Windows 7);

b) Microsoft .NET Framework Version 4.0;

c) Xilnex Framework Backend consist of:

- Web Server running on Windows Server 2003 with Microsoft IIS.
- Database – MySQL version 5.1.

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

1.6 Assumptions

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

1.7 Evaluated Configuration

16 This section describes the configuration of the TOE that is included within the scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the documented delivery and installation procedures and only by trustworthy staff.

17 The secure setup, installation and configuration of the TOE are based on Section 4 of the Web Bytes Xilnex Framework Guidance Documentation (Ref [8]). Basically it covers:

a) Installing and configuring the Deployer module – an executable at the client side for user to access the subscribed applications and communicating with the Deployer module at the server.

b) Installing and configuring the Cybernate API – a DLL file that provides a set of functions that enables developers to take advantage of the Cybernate Platform's synchronization ability without the needs to understand or reprogram any related synchronization mechanism. It provides necessary data manipulation functions that can be use by developers as if they are writing a simple database program. Cybernate API also provides necessary authentication functions in accessing the local database cache and also authentication for server synchronization.

c) Installing and configuring Xilnex Framework Backend – a system running by Web Bytes super administrator to configure the TOE and running on IIS as web services.

1.8 Delivery Procedures

18 There are 2 parts to the TOE. The first part is Cybernate API Version 3.0 (cybernate.dll) which is a DLL file for developers to use to build custom application on top of it.

19 The second part is the Deployer module (xilnex.exe (version 1.0.18.0)) which is an executable at the client side for users to access the subscribed applications and communicating with the Deployer module at Web Bytes (server). It can be downloaded from http://xilnex.com/Download.aspx.

20 For the Cybernate API, the DLL file and the user guide for developer (Xilnex Framework SDK - CybernateAPI version 3.0) will be sent to the developers of custom applications on a CD. The CD is sent via a trusted courier (DHL, Fedex, etc) or in person by the administrators of Web Bytes.

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

1.9 Documentation

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

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

a) Web Bytes Xilnex Framework Guidance Documentation (Ref [8])

2 Evaluation

24 The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 1 (EAL1). The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [5]).

2.1 Evaluation Analysis Activities

25 The evaluation activities involved a structured evaluation of Xilnex Framework Version 3.0, including the following components:

2.1.1 Life-cycle support

26 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators confirmed that the configuration list which includes the TOE and the evaluation evidence were clearly and uniquely labelled.

2.1.2 Development

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

2.1.3 Guidance documents

28 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

29 Testing at EAL1 consists of performing independent function test, and performing penetration tests. The formal testing was conducted by evaluators from stratsec at Web Bytes office in Bayan Baru, Pulau Pinang since due to time constraint, stratsec lab was not able to replicate the TOE development server to stratsec environment. This approach was taken due to the need to gain access to the development server of the TOE which is required to conduct the testing. In addition, initial stage for remote penetration testing was performed from the stratsec test environment 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 Independent Functional Testing

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

31 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The result of the independent tests developed and performed by the evaluators to verify the TOE functionality are as follows:

Table 2: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
To test that TOE performing hashing for user password using SHA512 algorithm and performing encryption and decryption for user local cache using RC4 algorithm with 128 key size.	FCS_COP.1 Cryptographic Operation (SHA512 and RC4)	User Interface Database Interface	**PASS.** Result as expected.
To test that TOE generate cryptographic key for user local cache using RC4 algorithm with 128 key size.	FCS_CKM.1 Cryptographic Key Generation (RC4)	User Interface	**PASS.** Result as expected.
To test that TOE performing appropriate action in destroying the cryptographic key using zeroization of keys method.	FCS_CKM.4 Cryptographic Key Destruction	User Interface	**PASS.** Result as expected.
To test that the TSF shall enforce the Access Control Policy.	FDP_ACC.1 Subset access control	User Interface Database Interface Device Interface	**PASS.** Result as expected.
To test that the TSF shall	FDP_ACF.1 Security	User Interface	**PASS.** Result as

enforce the Access Control Policy to objects based on the following: a) ID of the user b) Company Unique ID c) Access Control List	attribute based access control	Database Interface	expected.
To test that the TSF shall detect when 3 unsuccessful authentication attempts occur and block the user usage of the TOE for a pre-defined time of 10 seconds.	FIA_AFL.1 Authentication failure handling	User Interface Database Interface	**PASS.** Result as expected.
To test that the TSF shall maintain the following list of security attributes belonging to individual users: [**user password and user organization ID**].	FIA_ATD.1 User attribute definition	User Interface Database Interface	**PASS.** Result as expected.
To test that the TSF shall require each **user** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.	FIA_UAU.2 User authentication before any action	User Interface Database Interface	**PASS.** Result as expected.
The TSF shall require each **user** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.	FIA_UID.2 User identification before any action	User Interface Database Interface	**PASS.** Result as expected.
To test that the TSF shall enforce the [**Access Control SFP**] to restrict the	FMT_MSA.1 Management of security attributes	User Interface	**PASS.** Result as expected.

ability to [***write or delete***] the security attributes [**that map user IDs to user organization ID and applications to only the users that are mapped**] to [**the Administrator role**].			
To test that the TSF shall enforce the [**Access Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP and shall allow ~~the~~ [**none**] to specify alternative initial values to override the default values when an object or information is created.	FMT_MSA.3 Static attribute initialisation	User Interface	**PASS.** Result as expected.
To test that the TSF shall be capable of performing the following management functions: [**a) mapping user to user organization ID.** **b) creation of users with default passwords** **c) deletion of users** **d) changing of passwords** **e) management of Access Control list**]	FMT_SMF.1 Specification of Management Function	User Interface	**PASS.** Result as expected.
The TSF shall maintain the roles [**User and Administrator**] and shall be able to associate users with roles.	FMT_SMR.1 Security Roles	User Interface	**PASS.** Result as expected.
To test that the TSF shall protect TSF data from	FMT_ITT.1 Basic Internal TSF Data	User Interface OS Interface	**PASS.** Result as expected.

[*disclosure and modification*] when it is transmitted between separate parts of the TOE.	Transfer Protection		

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

2.1.4.2 Penetration Testing

33 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, and functional specification.

34 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.

35 The penetration tests focused on :

a) SQL Injection Attack.

b) Information Disclosure.

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

2.1.4.3 Testing Results

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

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

3 Result of the Evaluation

39 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 Xilnex Framework performed by the stratsec Security Evaluation Facility which known as STRATSEF.

40 The STRATSEF found that Xilnex Framework upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance level EAL1.

41 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

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

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

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

3.2 Recommendation

45 In addition to ensure secure usage of the product, below are additional recommendations for Xilnex Framework users:

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

b) Those responsible for administrating the Xilnex Framework Backend must ensure that the following is maintained for the TOE:

   - There is appropriate network layer protection, such as a firewall, that only permits access through essential ports for external users to access the web-server.
   - The underlying operating system for the database and web-servers are patched and hardened to protect against known vulnerabilities and security configuration issues.
   - SSL certificates are valid (not revoked or expired), are sourced from a trusted entity.

- That algorithm selected for SSL encryption and key lengths are appropriate for protecting the level of information being transmitted between the client and the server.
- The servers that host the web and database servers are hosted in a secure operating facility with restricted physical access and are not installed in shared hardware.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

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

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

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

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

[6] Web Bytes Xilnex Framework Security Target, Version 1.1, 21 November 2011.

[7] Evaluation Technical Report EAL1 Evaluation of Xilnex Framework, Version 1.4, 18 January 2012.

[8] Web Bytes Xilnex Framework Guidance Documentation, version 1.0, 19 January 2011.

A.2 Terminology

A.2.1 Acronyms

Table 3: List of Acronyms

Acronym	Expanded Term
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
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile

Acronym	Expanded Term
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Certifier	The certifier responsible for managing a specific certification task.
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS ISO/IEC Guide 65.
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.
Local Cache	A local instance of the database at the client’s machine.

Term	Definition and Source
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
MyCB 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.
SSL	Secure Sockets Layer (SSL), a protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message.
TSF data	Data created by and for the TOE, which might affect the operation of the TOE.
TSP	TOE Security Policy, a set of rules that regulate how assets are managed, protected and distributed.
User	It means any entity (human user or external IT entity) outside the TOE that interacts with the TOE. In this case, users of the TOE are developers who will build custom application to run over the TOE and users of the custom applications.

--- END OF DOCUMENT ---