Web Bytes Xilnex Framework

Security Target

Common Criteria: EAL1

Version 1.1

21-NOV-11

Document management

Document identification

Document ID	WEB_EAL1_ASE
Document title	Web Bytes Xilnex Framework Security Target
Product version	Version 3.0

Document history

Version	Date	Description
0.1	20-08-2010	Ready for review
0.2	02-12-2010	Updated to address EOR001-EOR005
0.3	06-12-2010	Updated TOE name to Xilnex Framework
0.4	08-12-2010	Updated to address EOR004.
1.0	19-JAN-2011	Submission with final ETR.
1.1	21-NOV-2011	Addressing the inconsistencies from MyCB

Table of Contents

1 Security Target introduction (ASE_INT) 4

1.1 ST and TOE identification 4

1.2 Document organization 4

1.3 TOE Overview 5

1.4 TOE Description 6

2 Conformance Claim (ASE_CCL) 9

3 Security objectives (ASE_OBJ) 10

3.1 Overview 10

3.2 Security objectives for the environment 10

4 Security requirements (ASE_REQ) 11

4.1 Overview 11

4.2 SFR conventions 11

4.3 Security functional requirements 12

4.4 Dependency analysis 20

4.5 TOE security assurance requirements 22

4.6 Assurance measures 23

5 TOE summary specification (ASE_TSS) 25

5.1 Overview 25

5.2 Secure Transmission 25

5.3 Access Control 25

5.4 Identification and Authentication 26

5.5 Encryption 26

5.6 Management 26

6 Glossary 28

1 Security Target introduction (ASE_INT)

1.1 ST and TOE identification

ST Title	Web Bytes Xilnex Framework Security Target
ST Version	1.1, 21-NOV-11
TOE Reference	Web Bytes Xilnex Framework
TOE Version	3.0
Assurance Level	EAL1
CC Identification	Common Criteria for Information Technology (IT) Security Evaluation, Version 3.1, July 2009, incorporating: • Part One – Introduction and General Model, Revision Three, July 2009; • Part Two – Security Functional Components, Revision Three, July 2009; and • Part Three – Security Assurance Components, Revision Three, July 2009.

1.2 Document organization

This document is organized into the following sections:

- Section 1 provides the introductory material for the ST as well as the TOE description including the physical and logical scope of the TOE.
- Section 2 provides the conformance claims for the evaluation.
- Section 3 defines the security objectives for the environment.
- Section 4 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively that must be satisfied by the TOE.
- Section 5 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE
- Section 6 provides the glossary for the ST.

1.3 TOE Overview

1.3.1 TOE type and usage

The TOE is ***Web Bytes Xilnex Framework***. The TOE is a distribution and synchronization platform which distributes subscribed applications to multiple clients as well performs data synchronization between all the clients in the same group. It can be installed on machines with Microsoft Windows XP, Vista or 7 (32-bit version). For Windows XP users, Microsoft .NET Framework 4.0 needs to be installed before installing the TOE.

The TOE consists of two primary components: the client software that installs directly on each user's PC, and the server software that extends client software with secure communication, identification and authentication, and data synchronization.

The communication between the client and server is secured using SSL. All applications can be downloaded through the client but they can only be launched by the client if the user has been successfully authenticated and have the subscription to the applications.

The TOE also synchronized 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.

The TOE also encrypts the local instance of the database and it is only decrypted and access after the user has been successfully authenticated. In offline mode, users will need to present their credentials (user ID, user password and user organization ID) to retrieve the key to decrypt the local instance of the database without authenticating to the server.

1.3.2 TOE security functions

The following table highlights the range of security functions and features implemented by the TOE.

Security function	Description
Secure transmission	Secure transmission of data sent over network from the client to the server. (SSL)
Access Control	Controls the access to software binaries and user data to users.

Security function	Description
Identification and authentication	Provides identification and authentication mechanism for users.
Encryption	The local cache database is encrypted using RC4 and all passwords are hashed using SHA512.
Management	The TOE provides security management through the use of the Administration Interface at the client and provides the capability to manage the security functionality of the TOE.

1.4 TOE Description

1.4.1 Physical scope of the TOE

The TOE consists of two primary components: the client software that installs directly on each user's PC, and the server software. A typical installation of the TOE can be found in Figure 1 below and identifies the various components of the Xilnex Framework.

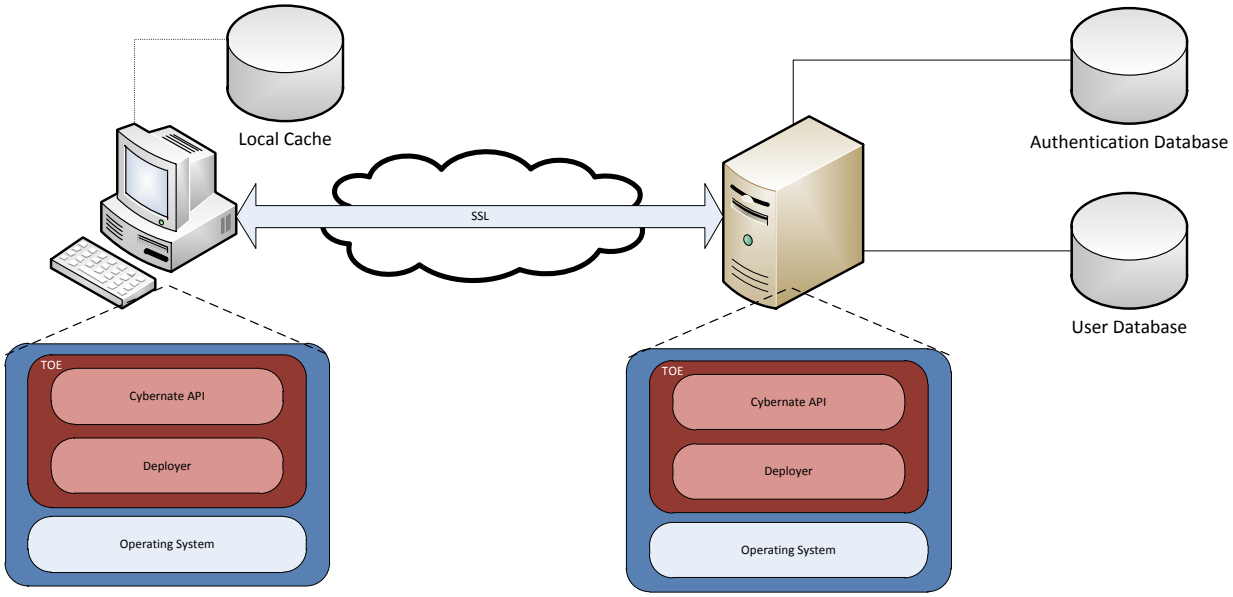

Figure 1 – Xilnex Framework architecture

The Deployer module 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.

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 create, 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.

Cybernate API also establish the secure communication between the server and the client.

Before the installation of the TOE, the operating system has to be installed on the machine.

The supported operating systems are Microsoft Windows XP, Windows 2003, Windows Vista and Windows 7. The following software must also be installed on all machines:

- Microsoft .NET Framework Version 4.0
  http://www.microsoft.com/downloads/details.aspx?FamilyID=9cfb2d51-5ff4-4491-b0e5-b386f32c0992&displaylang=en

1.4.2 Logical scope of the TOE

The logical boundary consists of the security functionality of TOE is summarized below.

- **Identification & 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.

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

- **Encryption.** Passwords are always hashed when they are being stored into the database and during authentication. The local cache is encrypted and can only be access when users successfully identified and authenticate themselves. They key will be read from the server.

- **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, user password and user 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.

- **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 within the TOE 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.

2 Conformance Claim (ASE_CCL)

The ST and TOE are conformant to version 3.1 (Revision 3) of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the TOE and ST:

- Part 2 conformant. Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1, Revision 3, July 2009.

- Part 3 conformant, EAL1 Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, Revision 3, July 2009.

3 Security objectives (ASE_OBJ)

3.1 Overview

The security objectives at an EAL1 level of assurance include concise statements of the objectives to be achieved by the supporting environment.

3.2 Security objectives for the environment

Identifier	Objective statements
OE.DATABASE	Those responsible for the TOE must ensure that the databases for the user data and the authentication data are configured to protect against unauthorized modification as well as confidentiality
OE.ADMIN	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.ENVIRONMENT	Those responsible for the administration of the underlying operating systems that support the TOE must ensure that the operating systems are installed, configured and patched appropriately.
OE.NETWORK	There is appropriate network layer protection, there is a firewall in place that only permits access through essential ports for external users to access the web-server.
OE.CERTIFICATES	SSL certificates are valid (not revoked or expired), are sourced from a trusted entity.

4 Security requirements (ASE_REQ)

4.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

4.2 SFR conventions

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

4.3 Security functional requirements

The security functional requirements are expressed using the notation stated in Section 4.2 and summarized in the table below.

Identifier	Title
FCS_COP.1a	Cryptographic operation (Hashing)
FCS_COP.1b	Cryptographic operation (Encryption and Decryption)
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_ITT.1	Basic internal TSF data transfer protection

4.3.1 FCS_COP.1a Cryptographic Operation (Hashing)

Hierarchical to:	No other components.
FCS_COP.1a.1	The TSF shall perform [**hashing**] in accordance with a specified cryptographic algorithm [**SHA512**] and cryptographic key sizes [**none**] that meet the following: [**FIPS 180-2**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	This cryptographic operation does not use key. The username and password of the users are hashed and compare with the values stored in the authentication database.

4.3.2 FCS_COP.1b Cryptographic Operation (Encryption and Decryption)

Hierarchical to:	No other components.
FCS_COP.1b .1	The TSF shall perform [**encryption & decryption**] in accordance with a specified cryptographic algorithm [**RC4**] and cryptographic key sizes [**128 bit**] that meet the following: [**RFC 4345**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	A local instance of the database (local cache) is created on the client side and it is encrypted using a random key generated by the TOE. The encryption keys will be stored in the authentication database at the server side.

4.3.3 FCS_CKM.1 Cryptographic Key Generation

Hierarchical to:	No other components.
FCS_CKM.1 .1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RC4**] and specified cryptographic key sizes [**128 bit**] that meet the following: [**RFC 4345**].
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Notes:	A local instance of the database (local cache) is created on the client side and it is encrypted using a random key generated by the TOE. The encryption/decryption key will be stored in the authentication database at the server side.

4.3.4 FCS_CKM.4 Cryptographic Key Destruction

Hierarchical to:	No other components.
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zeroization of keys**] that meets the following: [**FIPS140-1**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Notes:	A local instance of the database (local cache) is created on the client side and it is encrypted using a random key generated by the TOE. The encryption keys will be stored in the authentication database at the server side.

4.3.5 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [**Access Control SFP**] on [

	Subjects: **a) Users** **Objects:** **a) Applications and user data** **Operations:** **a) Launching of applications** **b) Accessing local cache** **c) Accessing user data database at server side**].
Dependencies:	FDP_ACF.1 - Security attribute based access control
Notes:	None.

4.3.6 FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**Access Control SFP**] to objects based on the following: [**Subject attribute:** **a) ID of the user** **b) Company Unique ID** **Object attributes:** **a) Access Control List**].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**a) The operation is allowed, if:** **b) The Access Control List for an object permits the user ID to access that object; OR** c) **The Access Control List for an object permits the company ID to access that Object.**]

FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**None**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**None**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Notes:	None.

4.3.7 FIA_AFL.1 Authentication failure handling

Hierarchical to:	No other components.
FIA_AFL.1.1	The TSF shall detect when [***3***] unsuccessful authentication attempts occur related to [**user entering their passwords for authentication**].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**block the user usage of the TOE for a pre-defined time of 10 seconds**].
Dependencies:	FIA_UID.1 Timing of identification
Notes:	The aim is to prevent continuous brute force of password guessing. The default time is 10 seconds. A longer time will result in legitimate user not getting access to the applications and this can be crucial in Point-of-Sales system.

4.3.8 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**user organization ID**].
Dependencies:	No dependencies.
Notes:	None.

4.3.9 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification

4.3.10 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies.
Notes:	None.

4.3.11 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [**Access Control SFP**] to restrict the 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**].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

4.3.12 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [**Access Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow ~~the~~ [**none**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

4.3.13 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	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**].
Dependencies:	No dependencies.
Notes:	None.

4.3.14 FMT_SMR.1 Security Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**User and Administrator**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

4.3.15 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to:	No other components.
FPT_ITT.1.1	The TSF shall protect TSF data from [***disclosure and modification***] when it is transmitted between separate parts of the TOE.
Dependencies:	None
Notes:	None.

4.4 Dependency analysis

SFR	Dependency	Inclusion
FCS_COP.1a	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	None. No keys are needed for hashing
FCS_COP.1b	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 FCS_CKM.4
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1b FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UID.2
FIA_ATD.1	No dependencies	N/A
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UID.2	No dependencies	N/A

SFR	Dependency	Inclusion
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 FDP_ACF.1 FMT_SMF.1 FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FPT_ITT.1	No dependencies	N/A

4.5 TOE security assurance requirements

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 1 (EAL1).

EAL1 provides a basic level of assurance by a limited security target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behavior.

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

EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents. This EAL provides a meaningful increase in assurance over unevaluated IT.

Assurance class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.1 TOE CM coverage
	ALC_CMC.1 Labelling of the TOE
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

4.6 Assurance measures

Assurance requirement	Assurance measures	Demonstration
ADV_FSP.1 Basic functional specification	Development	The development assurance measure provides all the necessary design documentation to support the analysis of the TOE for an evaluation at EAL1. The functional specification provides a detailed description of the security functions of the TOE.
AGD_OPE.1 Operational user guidance	Guidance documents	The operational user guidance documentation provides the guidance for end users, administrators and other parties who will utilise the TOE. These documents provide all the necessary instructions and direction for ensuring that the TOE is installed, configured, used and administered in a secure manner.
AGD_PRE.1 Preparative procedures		
ALC_CMC.1 Labelling of the TOE	Life cycle support	Configuration management measures provide the assurance that the TOE and supporting evidence can be uniquely identified.
ALC_CMS.1 TOE CM coverage		
ASE_CCL.1 Conformance claims	Security Target evaluation	Security Target evaluation assurance measures ensure that the claim to EAL1 can be accurately appraised.
ASE_ECD.1 Extended components definition		
ASE_INT.1 ST Introduction		
ASE_OBJ.1 Security objectives for the operational environment		

Assurance requirement	Assurance measures	Demonstration
ASE_REQ.1 Stated security requirements		
ASE_TSS.1 TOE summary specification		
ATE_IND.1 Independent testing - conformance	Tests	The tests assurance measure ensures that the TOE has been appropriately tested for the claimed set of security functions. The test plans for the TOE identifies the set of security functions that are to be tested, the procedures for establishing the test environment and also for conducting the test cases. The results of the tests are also recorded to provide evidence of test results.
AVA_VAN.1 Vulnerability survey	Vulnerability assessment	The TOE will be made available for vulnerability analysis and penetration testing.

5 TOE summary specification (ASE_TSS)

5.1 Overview

This section provides the TOE summary specification, a high-level definition of the security functions claimed to meet the functional and assurance requirements.

The TOE security functions include the following:

- **Secure Transmission**
- **Access Control**
- **Identification and Authentication**
- **Encryption**
- **Management**

5.2 Secure Transmission

The TOE establishes a trusted channel (**FPT_ITT.1**) using the SSL protocol for the transfer of user data from the TOE to a remote instance of the TOE. The SSL session is based on mutual authentication of the TOE, and the remote instance, using installed digital certificates. If the TOE is unable to transfer user data to a remote instance of the TOE (offline), it will continue to cache the data until it is able to do so (online).

5.3 Access Control

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 (**FDP_ACC.1, FDP_ACF.1, FIA_ATD.1**). The TOE maintains access control lists for each object within an organisation. Each ACL maps users and roles to the operations that they are permitted to perform on the object.

The access control lists are stored at the server side as well as in the local cache on the client side. This enable users to work in offline mode without being connected to the server.

5.4 Identification and Authentication

Users and administrator login through interface at the client side of the TOE. The TOE requires that the user (being a User or Administrator) identify and authenticate them before performing any TSF mediated action on behalf of the user (**FIA_UID.2, FIA_UAU.2**).

Users will be locked out for 10 seconds if they failed their authentication 3 times (**FIA_AFL.1**).

All users presented username and passwords are hashed before being used to authenticate the user or when users change their passwords and is being written to the database. This is all done by the TOE (**FCS_COP.1a**).

5.5 Encryption

For the local cache generated at the client side, it is encrypted using RC4 (**FCS_COP.1b**). The key for encryption is generated using the random number functionality of .NET framework (**FCS_CKM.1**). The key will be stored at the server side and can only be accessed when a user has successfully identified and authenticated himself/herself. No copy of the key is stored at the client side. The key is zeroized at the client side when it has been used for encryption or decryption (**FCS_CKM.4**).

For users who are not connected to the server, they can access the local cache. 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 credentials (user ID, User password and User 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.

5.6 Management

The TOE contains various management functions to ensure efficient and secure management of the TOE (**FMT_SMF.1**):

a) **User Management**

   The TOE only Administrator to query, create, delete, and modify users into the respective organization. For administrator, the default password is given when they subscribed to the xilnex service on xilnex website. This password is communicated to him/her through email. Administrator will be promoted to change their password upon first logon.

b) **Changing of passwords**

All users can change their passwords through the client interface. All changing of password is allowed only in online mode where the client and the server are connected.

c) Permission Management for Functions and Data

Administrator role can modify the access control list, mapping of users to applications and database that they are allowed to access (**FMT_MSA.1**).

The TOE maintains 2 roles (**FMT_SMR.1**) 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 1 administrator for each organization.

The TOE allows no one to change the default values of the TSF data and security attributes of the TOE (**FMT_MSA.3**).

6 Glossary

Term	Description
Authentication Data	It is information used to verify the claimed identity of a user.
FIPS 140-1	It is a Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology for cryptographic modules.
FIPS 180-2	It is a Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology for SHA.
Local Cache	À local instance of the database at the client's machine.
RC4	RC4 (also known as ARC4 or ARCFOUR meaning Alleged RC4, see below) is the most widely-used software stream cipher.
RFC 4345	This document specifies methods of using the RC4 cipher.
SHA512	The Secure Hash Algorithm is one of a number of cryptographic hash functions published by the National Institute of Standards and Technology as a U.S. Federal Information Processing Standard
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, that might affect the operation of the TOE
Users	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.