Employee Express Security Module (EmplX Security Module) Security Target

Common Criteria: EAL2

Version 1.0

09-AUG-11

Document management

Document identification

Document ID	EPX_EAL2_ST
Document title	Employee Express Security Module (EmplX Security Module) Security Target
Document date/version	1.0, 09-AUG-11

Document history

Version	Date	Description
0.1	16-JUL-10	Released for internal review
0.2	19-JUL-10	Updated to address internal comments
0.3	06-AUG-10	Updated to reflect the scope of the TOE..
0.4	15-DEC-10	Updated to address EORs.
0.5	13-MAY-11	Updated from draft ETR
0.6	24-MAY-11	Updated to address EORs
0.7	10-JUNE-11	Updated to address changes for Product Version
1.0	09-AUG-11	Initial release

Table of Contents

1 Security Target introduction (ASE_INT.1)

1.1 ST reference

ST Title	Employee Express Security Module (EmplX Security Module) of Security Target
ST Identifier	EPX_EAL2_ST
ST Version/Date	1.0 (09-AUG-11)

1.2 TOE reference

TOE Title	EmplX Security Module
TOE Version	1.0 (Build SVR V2.0)

1.3 Document organisation

This document is organized into the following major sections:

- Section 1 provides the introductory material for the ST as well as the TOE description (ASE_INT.1).
- Section 2 provides the conformance claims for the evaluation (ASE_CCL.1).
- Section 3 provides the definition of the security problem that the TOE has been designed to address (ASE_SPD.1).
- Section 4 defines the security objectives for the TOE and the environment (ASE_OBJ.2).
- Section 5 contains the security functional and assurance requirements derived from the Common Criteria, Part 2 and 3 respectively, which are in turn satisfied by the TOE and the development lifecycle (ASE_REQ.2).
- Section 6 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE (ASE_TSS.1).

1.4 TOE overview

1.4.1 TOE usage and major security functions

The Target of Evaluation (TOE) is the Employee Express Security Module (EmplX Security Module). EmplX is an online Human Resource Management Systems (HRMS), a web application written on PHP. The EmplX HRMS simplifies an organisation's administration functions, by providing a platform (either as a managed service or a standalone installation) that enables:

- employees to update personal information and allow supervisor or HR managers to view the information.
- employees to complete leave applications online through a web browser.
- employees to complete Expense Claims online through a web browser.
- employees to log in their work hours effectively through a web browser.
- employees to access and print their pay slip or pay stub the moment they require it.
- generation of customizable reports.
- Employees and supervisors access the application through any browser on any workstation.

The security module is part of EmplX HRMS. The TOE is a PHP module on the web server. All http requests to the web server will be meditated by the TOE before allowing access to the rest of the EmplX application.

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

Security function	Description
Access control	The TOE manages access control within each organisation based on user IDs, user roles and access control lists. 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.
Organisation Management	The TOE provides strict controls on organisation management. The TOE ensures that only Super Administrators can manage the creation, modification and destruction of an organisation. Users and Supervisors can only operate within their organisation.

Security function	Description
Identification and authentication	The TOE requires that each user is successfully identified (user ID) and authenticated (password) before any interaction with protected resources is permitted.
Security Management	The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.
Secure communications	The TOE is able to protect the user data from disclosure and modification when it is sent from users' browser to the TOE.

1.4.2 TOE type

The TOE is a specialist 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.

1.4.3 Supporting hardware, software and/or firmware

The TOE operates in a web server environment. In addition to requiring services from the environment to achieve its primary aim, the TOE also relies on the environment to maintain a secure posture so that the application cannot be compromised by factors out of the TSC.

The TOE requires the following from the environment to function:

Type	Description
Operating System	CentOS 5
Web Server	Apache
Database (RDBMS)	Postgresql 8

The TOE requires, specifically, that the underlying environment provide appropriate authentication and authorisation controls for all users and administrators in the underlying environment (including the Operating System, RDBMS, and Web Server). The TOE also requires that the underlying environment, primarily the Client browser and Web Server, provide protection for authentication details traversing

the network. In addition, the TOE requires that the underlying environment is free of vulnerabilities that allow an attacker to bypass the TOE security functions.

1.5 TOE description

1.5.1 Physical scope of the TOE

The TOE is a PHP module which is part of the EmplX Human Resource Management System (HRMS) web application hosted on a web server. A typical installation of the TOE can be found in Figure 1 below and identifies the various components of the EmplX architecture.

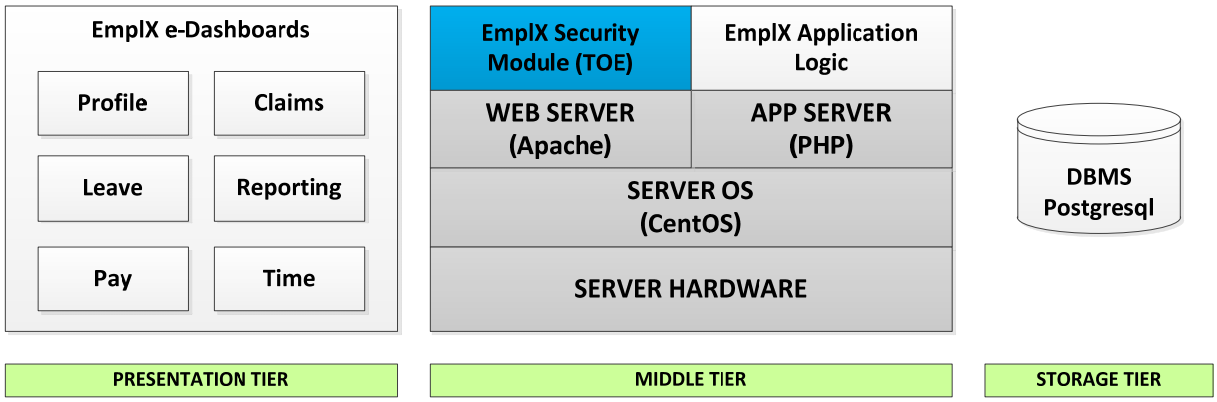

Figure 1 – EmplX architecture

The web application, EmplX is hosted on a Apache web server with all the PHP modules and pages. The TOE (EmplX Security Module) is a PHP module running on the web server.

1.5.2 Logical scope of the TOE

The logical scope of the TOE is described through the security functionality that the EmplX Security Module provides for the EmplX HRMS, this functionality is as follows:

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 (being an Employee, Supervisor, Administrator and Super Administrator) identify and authenticate themselves before performing any TSF 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. Access rules are stored in Access Control Lists associated with each object in the TSC.

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 organization 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. The roles maintained by the TOE are: Employee, Supervisor, and Administrator and Super Administrator. The functions above, and indeed, aspects of these functions, are restricted based on these roles.

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 the 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 users in different organisations. Each organisation is maintained and managed in its own database.

2 Conformance Claim (ASE_CCL.1)

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:

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

b) Part 3 conformant, EAL2. Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, Revision 3. Evaluation is EAL2.

3 Security Problem Definition (ASE_SPD.1)

3.1 Overview

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through:

a) a series of ***threats*** that the TOE has been designed to mitigate,

b) specific ***assumptions*** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and

c) any relevant ***organisational security policies*** are any statements made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

Threats	Statements
T.ACCESS	An unauthorized user obtains or modifies stored user data that they are not authorised to access resulting in a loss of confidentiality or integrity of the data.
T.MANAGEMENT	An unauthorized user modifies management data that they are not authorised to access resulting in a loss of integrity of the data that the TOE uses to enforce the security functions.
T.PASSWORD	An unauthorized user gains access to the passwords in the database and use them to authenticate to the TOE resulting in a loss of confidentiality or integrity of user or management data.
T-COMM	An unauthorized user gains access to the user data when it is traversing across the internet from to the EmplX HRMS application resulting in a loss of confidentiality and integrity of user data.
T.ORGANISATION	A valid user in one organisation uses valid credentials valid for their organisation to obtain or modify stored user or management data in another organisation resulting in a loss of confidentiality or integrity of the data.

3.3 Assumptions

Assumption	Statements
A.ENVIRONMENT	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)
A.ADMIN	It is assumed that the administrator who manages the TOE is not hostile and is competent.
A.PHYSICAL	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.
A.DATABASE	It is assumed that the databases in the TOE environment have been correctly configured according to the principle of least privilege.
A.NETWORK	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.
A.PATCH	It is assumed that the underlying operating system, web-server, application server and DBMSs and are patched and hardened to protect against known vulnerabilities and security configuration issues.
A.SSL_CONFIG	It is assumed that the web-server has SSL certificates installed and are valid (not revoked or expired), are sourced from a trusted entity.
A.MANAGEMENT	All management of the TOE will be performed through the management interfaces of the TOE and not through the underlying environment.

4 Security objectives (ASE_OBJ.2)

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in Section 3. There are security objectives for the TOE to address and additional objectives that provide specific direction for the intended in environment in which the TOE is to operate.

4.2 Security objectives for the TOE

Identifier	Objective statements
O.ACCESS	The TOE must ensure that only authorised users are able to access protected resources or functions.
O.USER	The TOE must ensure that all users are identified and authenticated before they access a protected resources or functions.
O.MANAGE	The TOE must allow administrators to effectively manage the TOE, while ensuring that appropriate control is maintained over those functions. .
O.PASSWORD	The TOE must ensure that passwords stored in the database are not in clear plaintext.
O.ORGANISATION	The TOE must ensure that users from one organisation can only access resources and functions in their own organisation.
O.COMM	The TOE must ensure that user data traversing across the network to the web server is protected from disclosure and loss of integrity.

4.3 Security objectives for the environment

Identifier	Objective statements
OE.ENVIRONMENT	Those responsible for the TOE must ensure that appropriate authentication and authorisation controls for all users and administrators in the underlying environment (including the Operating System, RDBMS, and Web Server)

Identifier	Objective statements
OE.ADMIN	The owners of the TOE must ensure that the administrator who manages the TOE is not hostile and is competent.
OE.PHYSICAL	Those responsible for the TOE must ensure 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.
OE.DATABASE	Those responsible for the TOE must ensure that the databases in the TOE environment have been correctly configured according to the principle of least privilege.
OE.MANAGEMENT	Those responsible for the TOE must ensure that all management of the TOE is performed through the management interfaces of the TOE and not through the underlying environment.
OE.NETWORK	Those responsible for the TOE must ensure that 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.
OE.PATCH	Those responsible for the TOE must ensure that the underlying operating system, web-server, application server and DBMSs and are patched and hardened to protect against known vulnerabilities and security configuration issues.
OE.SSL_CONFIG	Those responsible for the TOE must ensure that the web-server has SSL certificates installed and are valid (not revoked or expired), are sourced from a trusted entity.

4.4 TOE security objectives rationale

The following table demonstrates that all security objectives for the TOE trace back to the threats and OSPs in the security problem definition.

Threats/OSPs	Objectives	Rationale
T.ACCESS	O.ACCESS	The objective ensures that the TOE restricts access to the TOE objects to the authorized users.
	O.USER	The objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions.
T.MANAGEMENT	O.USER	The objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions.
	O.MANAGE	This objective ensures that the TOE provides the tools necessary for the authorized administrator to manage the security-related functions and that those tools are usable only by users with appropriate authorizations.
	O.ACCESS	The objective ensures that the TOE restricts access to the TOE objects to the authorized users
T.PASSWORD	O.PASSWORD	The objective ensures that all passwords stored in the database are hashed using SHA-2 before written to the database. No one can see the password in plaintext and will not be able to use the password to authenticate to the TOE.
T.COMM	O.COMM	The objective ensures that all user data from the user to the web server will be secured using SSL protecting the user data from unauthorized disclosure and loss of integrity.
T.ORGANISATION	O.USER	The objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions.

Threats/OSPs	Objectives	Rationale
T.ORGANISATION	O.ORGANISATION	The TOE must ensure that users from one organisation can only access resources and functions in their own organisation.

4.5 Environment security objectives rationale

The following table demonstrates that all security objectives for the operational environment all trace back to assumptions or OSPs in the security problem definition.

Assumptions	Objective	Rationale
A.ENVIRONMENT	OE.ENVIRONMENT	This objective ensures that those responsible for the TOE ensure that appropriate authentication and authorisation controls for all users and administrators in the underlying environment (including the Operating System, RDBMS, and Web Server)
A.ADMIN	OE.ADMIN	This objective ensures that those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
A.PHYSICAL	OE.PHYSICAL	This objective ensures that those responsible for the TOE ensure 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.
A.DATABASE	OE.DATABASE	This objective ensures that those responsible for the TOE ensure that the databases in the TOE environment have been correctly configured according to the principle of least privilege.
A.MANAGEMENT	OE.MANAGEMENT	This objective ensures that those responsible for the TOE ensure that all management of the TOE is performed through the management interfaces of the TOE and not through the underlying environment.
A.NETWORK	OE.NETWORK	This objective ensures that those responsible for the TOE ensure that 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.

Assumptions	Objective	Rationale
APATCH	OE.PATCH	This objective ensures that those responsible for the TOE ensure that the underlying operating system, web-server, application server and DBMSs and are patched and hardened to protect against known vulnerabilities and security configuration issues.
A.SSL_CONFIG	OE.SSL_CONFIG	This objective ensures that those responsible for the TOE ensure that the web-server has SSL certificates installed and are valid (not revoked or expired), are sourced from a trusted entity.

5 Security requirements (ASE_REQ.2)

5.1 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.

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.

5.2 Security functional requirements

5.2.1 Overview

The security functional requirements are expressed using the notation stated in Section 5.1 above and itemised in the table below.

Identifier	Title
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
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_MTD.1a	Management of security functions behaviour (Default)
FMT_MTD.1b	Management of security functions behaviour (Configuration)
FMT_MTD.1c	Management of security functions behaviour (Password)
FMT_MTD.1d	Management of security functions behaviour (Organisation)
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FTP_TRP.1	Trusted path

5.2.2 FCS_COP.1 Cryptographic Operation

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [**secure hashing**] in accordance with a specified cryptographic algorithm [**SHA-2**] 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 password of the users is hashed and compare with the values stored in the authentication data database.

5.2.3 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) HTTP request on behalf of users** **Objects:** **a) Protected resources (methods and HTML pages)** **Operations:** **a) Methods execution** **b) Serving of HTML pages**]
Dependencies:	FDP_ACF.1 – Security attribute based access control
Notes:	None.

5.2.4 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) corresponding user role** **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 User Role to access that Object**].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**the Administrator role can access all records and functions**].
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.

5.2.5 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
Notes:	User Credentials for Employees and Supervisors only exist within a specific organisation.

5.2.6 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.

5.2.7 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 roles 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.

5.2.8 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.

5.2.9 FMT_MTD.1a Management of security functions behaviour (Default)

Hierarchical to:	No other components
FMT_MTD.1a.1	The TSF shall restrict the ability to [***change_default***] the [**all TSF data**] to [**None**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.10 FMT_MTD.1b Management of security functions behaviour (Configuration)

Hierarchical to:	No other components
FMT_MTD.1b.1	The TSF shall restrict the ability to [***query, modify, delete, clear*** [**Create**] the [**Access Control Lists, Mapping of users to Roles, User accounts**] to [**Supervisor, Administrator**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.11 FMT_MTD.1c Management of security functions behaviour (Password)

Hierarchical to:	No other components
FMT_MTD.1c.	The TSF shall 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)**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.12 FMT_MTD.1d Management of security functions behaviour (Organisation)

Hierarchical to:	No other components.
FMT_MTD.1d	The TSF shall restrict the ability to [***query, modify, delete, clear*** [**Create**] the [**Organisation**] to [**Super Administrator**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.13 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 Ids to roles** **b) creation of users with default passwords** **c) deletion of users** **d) changing of passwords** **e) management of Access Control lists**

	f) Management of organization]
Dependencies:	No dependencies.
Notes:	None.

5.2.14 FMT_SMR.1 Security Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**Employee, Supervisor, Administrator and Super Administrator**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.15 FTP_TRP.1 Trusted path

Hierarchical to:	No other components.
FTP_TRP.1.1	The TSF shall provide a communication path between itself and [***remote***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***modification, disclosure***]].
FTP_TRP.1.2	The TSF shall permit [***remote users***] to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [***initial authentication***]].
Dependencies:	No dependencies
Notes:	None.

5.3 TOE security assurance requirements

EAL2 requires evidence relating to the design information and test results, but does not demand more effort on the part of the developer than is consistent with good commercial practice.

EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behavior.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

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

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_CMC.2 Use of a CM system
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction

Assurance class	Assurance components
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.2 Independent testing - sample
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

5.4 Defined terms

The following table defines all subjects, objects, operations, security attributes, external entities and other key terms that are used within the statements of security functional and assurance requirements.

Term/Acronym	Definition
Authentication Data	It is information used to verify the claimed identity of a user.
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
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.
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 uses 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.

5.5 Security requirements rationale

5.5.1 SFR dependency rationale

Below demonstrates the mutual supportiveness of the SFR's for the TOE by demonstrating how the SFR dependencies are fulfilled by the TOE, and by justifying those dependencies that are not fulfilled.

The SARs relevant to the TOE constitute an evaluation assurance level EAL2 as defined in Common Criteria and include no extensions or augmentations. Therefore, as a complete evaluation assurance level, they are a mutually supportive set and require no further justification.

SFR	Dependency	Inclusion
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_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UID.2	No dependencies	N/A
FMT_SMF.1	No dependencies	N/A
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_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2

SFR	Dependency	Inclusion
FCS_COP.1	[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	SHA-2 is a hashing algorithm and is a one-way function. Therefore it does not use any key for hashing and there is no FCS_CKM.1 and FCS_CKM.4 involved for the function. Therefore the dependencies are not applicable.
FMT_MTD.1a	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FMT_MTD.1b	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FMT_MTD.1c	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FMT_MTD.1d	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FTP_TRP.1	No dependencies	N/A

5.5.2 Mapping of SFRs to security objectives for the TOE

Objective	SFR and Demonstration
O.ACCESS	**FDP_ACC.1**: The requirement helps meets the objective by identifying the objects and users subjected to the access control policy. **FDP_ACF.1**: The requirement meets this objective by ensuring the TOE only allows access to objects based on the defined access control policy.
O.USER	**FIA_UID.2**: The requirement helps meets the objective by identifying the users before any TSF mediated actions. **FIA_UAU.2**: The requirement helps meets the objective by authenticating the users before any TSF mediated actions. **FMT_SMR.1**: The TOE manages 4 roles: Supervisor, Employee, Administrator and Super Administrator.
O.PASSWORD	**FCS_COP.1:** The requirement helps to meet the objective by hashing all the passwords using SHA-2 before they are written into the database.
O.MANAGE	**FMT_MSA.1**: The TOE allows the super administrator to determine who will have access to the folder and the folder's contents and what actions the user can be perform. **FMT_MSA.3**: The TOE enforces a restrictive access when a new object is created. The TOE has a default ACL which is assigned to all newly-created objects. This default ACL cannot be altered by any user. **FMT_MTD.1a:** This requirements helps meet the objective by allowing no one to change the default values of the TSF data. **FMT_MTD.1c:** This requirement helps meet the objective by allowing users of all roles to change their passwords. **FMT_MTD.1b:** This requirements helps meet the objective by allowing only the Super Administrators and Supervisor roles to create, delete, modify access control list, mapping of users to roles and user accounts to the respective organisation database. **FMT_MTD.1d:** This requirements helps meet the objective by allowing only the Super Administrators to create, delete, modify Organization to the database. **FMT_SMF.1**: The TOE allows the mapping of user to roles, creation of users,

Objective	SFR and Demonstration
	deletion of users, changing of passwords, management of ACL and managing organisation.. **FMT_SMR.1**: The TOE manages 4 roles: Supervisor, Employee, Administrator and Super Administrator.
O.COMM	**FTP_TRP.1.** This requirement helps meet the objective by establishing a SSL secure channel from the user's browser to the EmplX HRMS web application protecting the user data from disclosure and modification.
O.ORGANISATION	**FIA_UID.2**: The requirement helps meets the objective by identifying the users before any TSF mediated actions. User credentials of employees and supervisors can only exist within a specific organization. **FIA_UAU.2**: The requirement helps meets the objective by authenticating the users before any TSF mediated actions. User credentials of employees and supervisors can only exist within a specific organization. **FDP_ACC.1**: The requirement helps meets the objective by identifying the objects and users subjected to the access control policy. **FDP_ACF.1**: The requirement meets this objective by ensuring the TOE only allows access to objects based on the defined access control policy.

5.5.3 Explanation for selecting the SARs

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 2 (EAL2).

The TOE is intended to protect confidential information related to a business's employees. This information, while sensitive within an organization, the value to an attacker is relatively low. As such, it is considered that the average motivation of attackers will be low, which implies that the overall attack potential for this TOE will be LOW. EAL2 is sufficient to demonstrate that the TOE is resistant to attackers with a LOW attack potential.

6 TOE summary specification (ASE_TSS.1)

6.1 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:

- Access Control
- Identification and Authentication
- Security Management
- Secure communications
- Organisation Management

6.2 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 (**FDP_ACC.1, FDP_ACF.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.

There are 4 users maintained by the TOE. They are Employee, Supervisor, Administrator and Super Administrator (**FMT_SMR.1**). Each type of user will have different access rights to a protected resource. All users will have a unique user ID.

6.3 Identification and Authentication

When a user issues a request to the TOE to access a protected resource (methods or HTML pages), the TOE requires that the user (being an Employee, Supervisor, Administrator or Super Administrator) identify and authenticate themselves before performing any TSF mediated action on behalf of the user (**FIA_UID.2, FIA_UAU.2**). 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.

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

6.4 Security 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 in organization. (FMT_MTD.1b).

b) 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 in the organisation that he/she is modifying (FMT_MTD.1b, FMT_MSA.1).

c) **Organization Management**

The TOE maintains four 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: Employee, Supervisor, Administrator and Super Administrator. The functions above, and indeed, aspects of these functions, are restricted based on these roles.

The TOE allows no one to change the default values of the TSF data and security attributes of the TOE (**FMT_MTD.1a, FMT_MSA.3**).

6.5 Secure communications

When a user access the EmplX HRMS web application on their browser by typing in the web address of the site, the TOE will initiate a SSL secure channel establishment with the user's browser (**FTP_TRP.1**).

The TOE implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols. It provides a rich API which provides functionality for:

a) dealing with protocol methods,

b) implementing ciphers,

c) managing keys,

d) implementing sessions and context, and

e) establishing and managing connections.

6.6 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 (**FDP_ACC.1, FDP_ACF.1**). Only Super Administrators have the privilege required to create users in different organisations (**FMT_MTD.1d**). Each organisation is maintained and managed in its own database.