ST Version Date – November 19, 2010

Version 1-6

eWorkshop

Version 1.0

SECURITY TARGET

Prepared for

Triangle Sphere Sdn Bhd

Suite 8.09, Level 8, Wisma Zelan,
No 1, Jalan Tasik Permaisuri 2,
Bandar Tun Razak,
56000 Kuala Lumpur
Malaysia

By

Teknimuda (M) Sdn Bhd

Table of Contents

FIGURES

TABLES

ST Version Change History

Version	Pages Affected	Date	Comments
1-1		6 July 2010	First Issue
1-2		22 July 2010	Second Issue
1-3		16 August 2010	Third Issue. This includes addition and corrections as follows; a. Addition of TOE diagram b. Addition of FAU_GEN, FAU_SAR and FPT_STM security functions c. Correction of attributes in SFRs d. Removed Security Objectives for TOE. e. Removed Security Problem Definition.
1-4		12 October 2010	Fourth Issue. Updated as per comments in EOR1-D1 as follows: a. Clarity of the terms Administrator and User b. Audit trail records access aligned in whole document to allow only Administrator access in Table 1. c. Minor corrections..
1-5		29 October 2010	Fifth Issue. Updated as follows: a. Reset boundary of TOE in Figure 1 b. Audit trail records accessible to Administrator only in Table 1. c. Included Application Notes for FAU_GEN.1.1 and FPT_STM.1.1. d. Minor corrections..
1.6		19 November 2010	Comply with EOR#5 as follows: a. Change 500Gb to 100Gb

b. Amend OE.AUTH

1 SECURITY TARGET INTRODUCTION

1.1 ST Reference

This section provides ST control and identification information.

ST Title:	eWorkshop Version 1.0 Security Target
ST Version:	1-5
ST Date:	October 29, 2010
ST Authors:	A Fattah Yatim, Mohd Zahari Zakaria
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009
Assurance Level:	Evaluation Assurance Level 1 (EAL1)

1.2 TOE Reference

This section provides TOE control and identification information.

TOE Identification: **eWorkshop Version 1.0**

Development Tools: **ASP.net**
Visual Studio 2005
mySQL

Developer: Triangle Sphere Sdn Bhd

Suite 8.09, Level 8, Wisma Zelan,
No 1, Jalan Tasik Permaisuri 2,
Bandar Tun Razak,
56000 Kuala Lumpur

Malaysia

1.3 TOE Overview

eWorkshop Version 1.0 is an application for managing a vehicle maintenance workshop, suitable for an entity that has a fleet of vehicles to maintain or is contracted to maintain vehicles. It is a web based application for the Intranet environment.

eWorkshop Version 1.0 is targeted for use in workshops for vehicle maintenance that have a complete cycle of planned maintenance, emergency maintenance or repair, parts procurement and inventory storage, billing and claims and basic financial management.

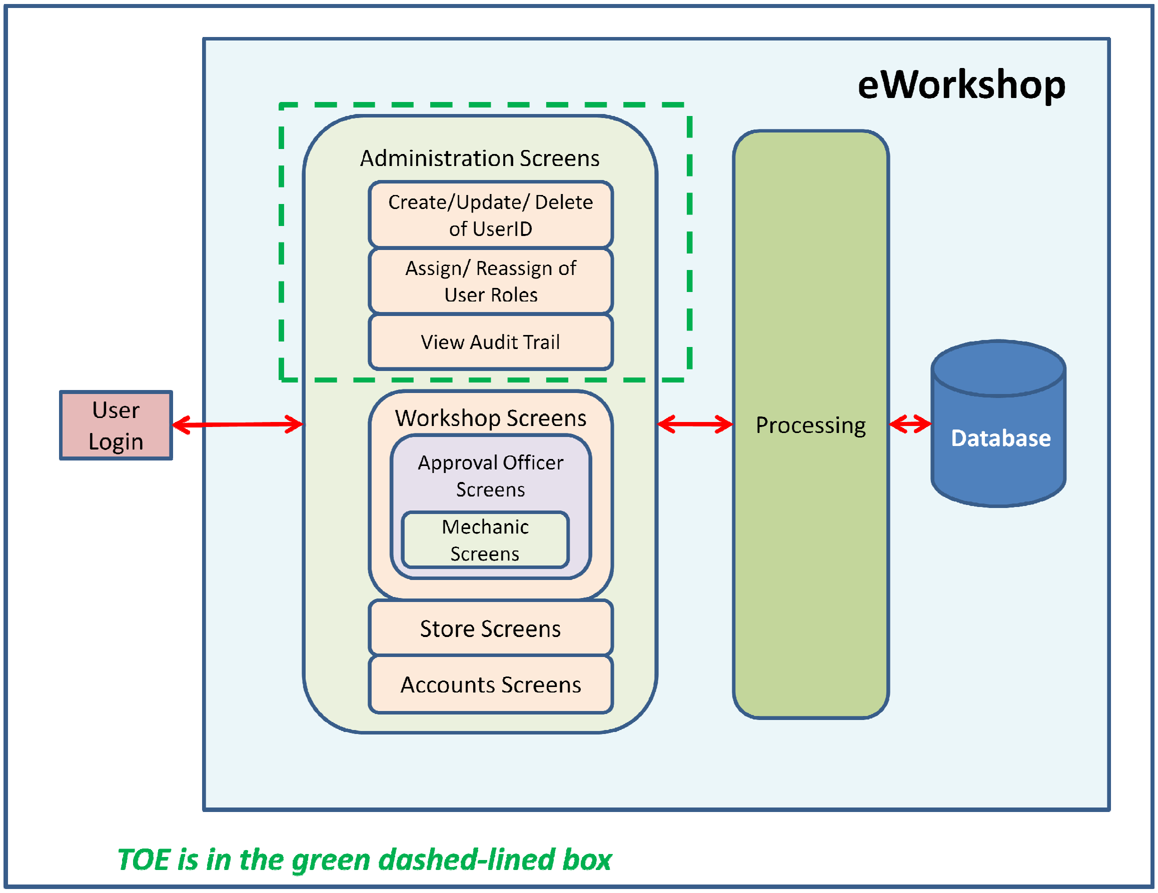
The TOE however is the **Access Control Administration** part of eWorkshop Version 1.0 which covers:

a. the creation and deletion of logon ids and

b. the assignment (and reassignment) of user privileges through user roles pre-defined by the client organisation during application set up.

The TOE is depicted in the following diagram:

Figure 1 : TOE for eWorkshop Version 1.0



1.3.1 Usage and Major Security Features of TOE

The application manages the creation of work orders, confirmation of work done and ultimately involves finances which covers purchasing of parts, payment for work done and the billing of customers all of which needs to be controlled in order to avoid leakages, duplicate claims, unauthorised expenditures or expenditures for work that have not been actually carried out.

A key aspect of proper control and management is the segregation of responsibilities and authorities and the application supports these controls structure to ensure accountability and traceability.

The TOE enables the security enforcement and management of accesses to the eWorkshop Version 1.0 application and information stored and processed by the application. The accesses are managed at two levels:

a. Creation of Logon Ids for authorised users and deletion of Logon Ids for users who have left the organisation.

b. Assignment of user roles to authorised users so that the users can access the screens and functions to perform their designated responsibilities (and nothing else).

Other security functions that are performed by the TOE are Security Audit that logs records pertaining to creation, update/ delete of IDs, protection of data by authorising the access by role, Session locking after 15 minutes of idle, and time stamp from underlying OS to protect the TSF.

1.3.2 TOE Type

eWorkshop Version 1.0 provides the following: Web Access Control for the Intranet environment.

1.3.3 Non-TOE hardware/software/firmware

1.3.3.1 Hardware

Servers – Intel based or equivalent 2GHz or faster, 4GB of RAM, 100GB disk space, running on Windows Server 2003

Client – Intel based workstation, 1GHz or faster, 1GB of RAM, 10GB disk space with Windows XP Professional Edition, Windows 7 Home Premium, Windows 7 Professional and Windows 7 Ultimate

1.3.3.2 Software

Server - mySQL Database 3.51, 4.1 and 5.1

Microsoft .NET Framework Version 2.0

1.4 TOE Description

This section and subsections provide the TOE description, starting with an overview of the eWorkshop Version 1.0 application features overall, defining the TOE which covers only a part of the eWorkshop Version 1.0 application and followed by further details on the TOE.

1.4.1 General overview

eWorkshop Version 1.0 is an application for managing a vehicle maintenance workshop, suitable for an entity that has a fleet of vehicles to maintain or is contracted to maintain vehicles. It is a web based application for the Intranet environment.

eWorkshop Version 1.0 is targeted for use in workshops for vehicle maintenance that have a complete cycle of planned maintenance, emergency maintenance or repair, parts procurement and inventory storage, billing and claims and basic financial management.

The application manages the creation of work orders, confirmation of work done and ultimately involves finances which cover purchasing of parts, payment for work done and the billing of customers all of which needs to be controlled.

In each stage of these activities, there is a possibility of leakage, whether inadvertent or deliberate and the structure of the application ensures system integrity and minimises the possibility of such leakages.

A key aspect of proper control and management is the segregation of responsibilities and authorities, and the application supports these controls structure to ensure accountability and traceability. The designation of roles to segregate responsibilities is outside of the application (procedural with approvals) but once approved, the designated roles will be assigned to the respective authorised users by the Administrator in the application.

From within the application, authorised users will be able to perform their functions and roles as pre-defined or pre-configured in the application.

The main features of eWorkshop Version 1.0 cover the registration, transaction recording and reporting of the following:

1. Vehicle particulars - Registration of vehicle details including licence number, chasis number, engine number, mileage.
2. Client particulars - Registration of client and panel information.
3. Cost and service particulars:
    a. Provides service and cost information quickly and accurately.
    b. Produce cash bill and allocated warrants.

    c. Produces invoices for credit and check payments.
    d. Information on debtors on screen.
    e. Inclusion of applicable service tax and other charges.

4. Parts and stock particulars:
    a. Registration of external supplies of parts.
    b. Inventory and stock control.
    c. Provides details on parts purchased and purchase price, parts used and parts in storage.
    d. Use of unique part numbers.
5. Consolidation and reporting:
    a. Multiple data entry locations and central consolidation.
    b. Scheduled year end reports.
    c. Detailed service and repair report for each job.
    d. Detailed service and repair history for each vehicle.

Some of the the benefits of the use of the application are:

1. Avoidance of duplication or double payment to suppliers.
2. All transactions are recorded and all client payment history are properly managed and controlled.
3. Optimal use and control of spare parts as all maintenance and repairs and its use of parts are recorded and closely monitored.
4. With proper record keeping and control, waste is eliminated.
5. With up to date and accurate information, sound management and business decisions can be made.

The TOE however is the **Access Control Administration** part of eWorkshop Version 1.0 which includes the creation and deletion of logon ids and the assignment and reassignment of user privileges through user roles pre-defined by the client organisation. With the user role defined, users will be allowed access to screens for the respective user roles only. This is further defined in the following sub sections.

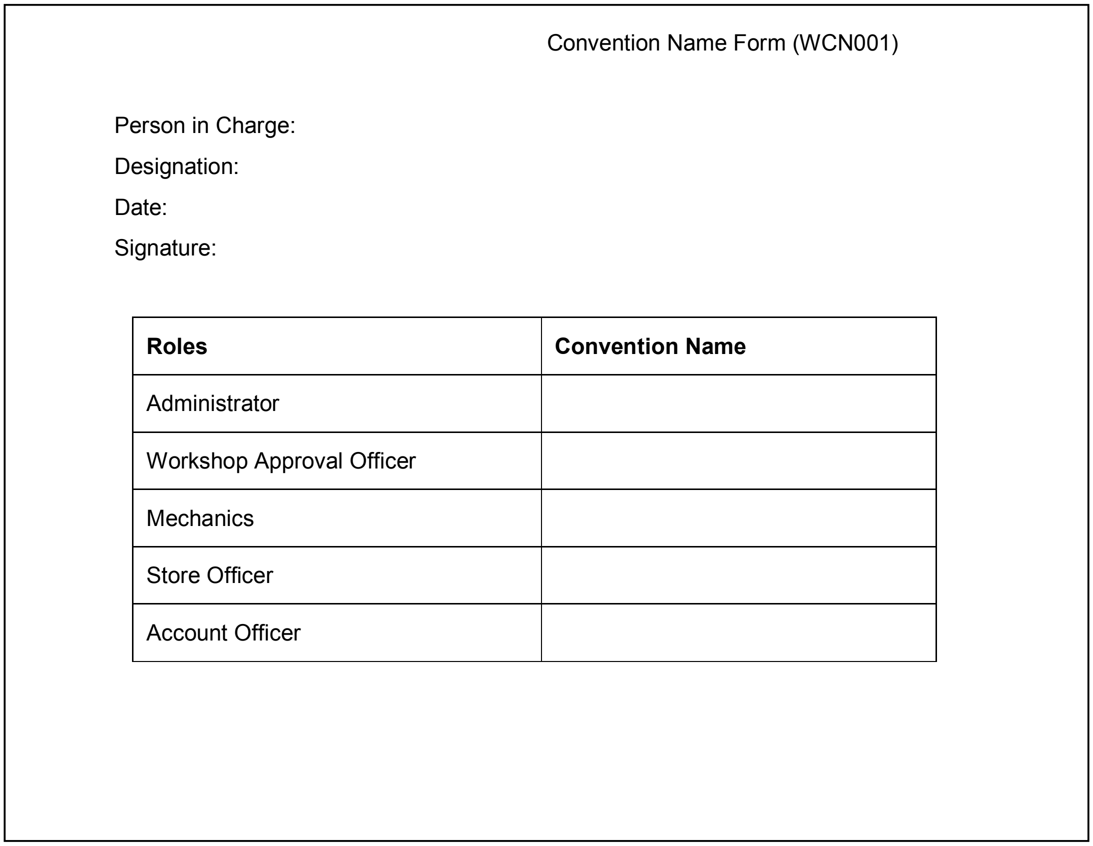
1.4.2 TOE Details

The TOE comprises:

1. Creation and deletion of logon Ids and the default passwords
2. The assignment of user roles (or privileges or access rights) to access appropriate sections of the application for the user to perform his user role and responsibilities. The user roles implemented in an existing system are:
    a. Administrator,
    b. Workshop Approval Officer,
    c. Mechanics,
    d. Store Officer,
    e. Account Officer.

The above are the role names in an actual system used by a client. Should another client wish to use other names for the above user roles, this can be configured during installation of the application by the application supplier, following the specification and sign off of a naming convention form as follows:

Figure 2 : Convention Name Form



Convention Name Form (WCN001)

Person in Charge:

Designation:

Date:

Signature:

Roles	**Convention Name**
Administrator	
Workshop Approval Officer	
Mechanics	
Store Officer	
Account Officer	

Throughout this document, the term ‘user’ or ‘user role(s)’ are applicable to ALL users including ‘Administrator’ or ‘Administrator role’ respectively, whereas the term ‘Administrator’ or ‘Administrator role’ refers to only that, i.e. the respective Administrator or Administrator roles. The eWorkshop system allows as many of EACH role to be created by anybody assigned the Administrator role. Hence the Administrator role can create another ID AND assign Administrator role to that ID.

The Administrator role needs special mention and is often separately identified throughout this document as the Administrator role can perform all functions that are normally carried out by the other four roles. Though this feature (i.e. that the Administrator role can perform all other role functions) is not a usual feature, it is a necessary feature for the application as specified by the current user (as of 2010) of the eWorkshop application.

All ‘user roles’ except the Administrator role, are NOT part of the TOE but is mentioned in this document to enable the easy verification or proof of the Administrator functions in the creation, update and delete of user Ids and assignment of user roles.

The screens and report displays that a particular role can use or view is also pre-specified. The lists of screens follow a screen naming code as follows:

Table 1 : Screen Code for Role ID

Role ID or Second Tier Role ID	Screen Code Accessible Begins with
Administrator	WMM – Workshop Management Management (Administration), WMW – Workshop Management Workshop, WMS – Workshop Management Store, WMA – Workshop Management Account, WMT – Workshop Management Trails (Audit Trails)
Workshop Approval Officer	WMW
Mechanics	WMW (except for several WMW screens specified in Table 2),
Store Officer	WMS
Account Officer	WMA

The screens list accessible by user roles are shown in the table below and the legend on the access mode is at the bottom of the table:

Table 2 : User Roles and Screens Accessible

No	Screen Accessible	Administrator	Workshop Approval Officer	Mechanics	Store Officer	Account Officer
1	**Administration (WMM 1)**					
1.1	Registration **(WMM 1.1)**					
	- Create System User **(WMM 1.1.1)**	V/C/E/D				
	- Create Employee Profile **(WMM 1.1.2)**	V/C/E/D				
	- Workshop Profile **(WMM 1.1.3)**	V/C/E				
1.2	Utilities **(WMM 1.2)**					
	- Change Password **(WMM 1.2.1)**	E				
1.3	Listing **(WMM 1.3)**					
	-System User Listing **(WMM 1.3.1)**	V				
	-Employee Listing **(WMM 1.3.2)**	V				
1.4	Master Menu **(WMM 1.4)**					
	-Job Repair **(WMM 1.4.1)**	V/E				
	-Job In Progress Editing **(WMM 1.4.2)**	V/E				
	-Job Close Editing **(WMM 1.4.3)**	V/E				

No	Screen Accessible	Administrator	Workshop Approval Officer	Mechanics	Store Officer	Account Officer
	-Inventory **(WMM 1.4.4)**	V/E				
	-JKR 38 Table **(WMM 1.4.5)**	V/E				
	-LPO & Indent Liability **(WMM 1.4.6)**	V/E				
	-Indent Cleared **(WMM 1.4.7)**	V/E				
	-LPO Stock Cleared **(WMM 1.4.8)**	V/E				
	-LPO Job Cleared **(WMM 1.4.9)**	V/E				
	-Allowance **(WMM 1.4.10)**	V/E				
	-Servicing **(WMM 1.4.11)**	V/E				
	-Transport **(WMM 1.4.12)**	V/E				
	-Labour Chargers **(WMM 1.4.13)**	V/E				
	-Sundries **(WMM 1.4.14)**	V/E				
	-Direct Order **(WMM 1.4.15)**	V/E				
	-Customer **(WMM 1.4.16)**	V/E				
	-Supplier **(WMM 1.4.17)**	V/E				
	-Warrant **(WMM 1.4.18)**	V/E				
	-Service Rate Editing **(WMM 1.4.19)**	V/E				
	-Voucher Edit **(WMM 1.4.20)**	V/E				
	-Inventory Edit **(WMM 1.4.21)**	V/E				
	-Year End Process **(WMM 1.4.22)**	V				
1.5	Other Role **(WMM 1.5)**					
	-Workshop **(WMM 1.5.1)**	V				
	-Store **(WMM 1.5.2)**	V				
	-Account **(WMM 1.5.3)**	V				
	-Building **(WMM 1.5.4)**	V				
1.6	Management Board **(WMM 1.6)**					
	-Workshop **(WMM 1.6.1)**	V				
	-Report **(WMM 1.6.2)**	V				
2	**Workshop (WMW 2**					
2.1	Create **(WMW 2.1)**					
	-Repair ('O' Order) **(WMW 2.1.1)**	V/C	V/C	V/C		
	-Service ('P' Order) **(WMW 2.1.2)**	V/C	V/C	V/C		
	-Booking (PK Order) **(WMW 2.1.3)**	V/C	V/C	V/C		
2.2	Vehicle **(WMW 2.2)**					
	-Vehicle Profile **(WMW 2.2.1)**	C	C	C		
	-Edit Vehicle **(WMW 2.2.2)**	V/E	V/E	V/E		
2.3	Job Proceeding **(WMW 2.3)**					
	-Approval **(WMW 2.3.1)**	V/E	V/E			
	-Job Edit (KIV) **(WMW 2.3.2)**	V/E	V/E			
	-Indent Noting **(WMW 2.3.3)**	V/E	V/E	V/E		
	-Close Job **(WMW 2.3.4)**	V/E	V/E	V/E		
2.4	Utilities **(WMW 2.4)**					
	-Change Password **(WMW 2.4.1)**	E	E	E		
	-Back to Admin **(WMW 2.4.2)**	V				
2.5	Listing **(WMW 2.5)**					
	-Indent List **(WMW 2.5.1)**	V	V	V		
	-Inventory Listing **(WMW 2.5.2)**	V	V	V		
	-Vehicle Listing **(WMW 2.5.3)**	V	V	V		
	-Job Listing **(WMW 2.5.4)**	V	V	V		
	-Workshop Report **(WMW 2.5.5)**	V	V	V		
3	**Store (WMS 3)**					
3.1	Job Proceeding **(WMS 3.1)**					
	-LPO Noting **(WMS 3.1.1)**	E			E	
	-Stock Issue (JKR 38) **(WMS 3.1.2)**	V/C			V/C	
3.2	Utilities **(WMS 3.2)**					
	-Change Password **(WMS 3.2.1)**	E			E	
	-Back to Admin **(WMS 3.2.2)**	V				

No	Screen Accessible	Administrator	Workshop Approval Officer	Mechanics	Store Officer	Account Officer
3.3	Listings and Report **(WMS 3.3)**					
	-Inventory Listing **(WMS 3.3.1)**	V			V	
	-JKR 38 List **(WMS 3.3.2)**	V			V	
	-JKR 38 List All **(WMS 3.3.3)**	V			V	
	-LPO Listing **(WMS 3.3.4)**	V			V	
	-Reports **(WMS 3.3.5)**	V			V	
	-Quarterly Reports **(WMS 3.3.6)**	V			V	
	-Stock Verify **(WMS 3.3.7)**	V			V	
	-Kad Kawalan Stok (KEW.PS-3) **(WMS 3.3.8)**	V			V	
4	**Account (WMA 4)**					
4.1	Create **(WMA 4.1)**					
	-Repair 'O' Job **(WMA 4.1.1)**	C				C
4.2	Job Update **(WMA 4.2)**					
	-Workshop : Repair 'O' Job **(WMA 4.2.1)**	V/E				V/E
	-Workshop : Service 'P' Job **(WMA 4.2.2)**	V/E				V/E
	-Workshop : Booking PK Job **(WMA 4.2.3)**	V/E				V/E
	-Building : Repair 'O' Job **(WMA 4.2.4)**	V/E				V/E
4.3	Expenses **(WMA 4.3)**					
	-Allowance / Transport **(WMA 4.3.1)**	V/C				V/C
	-Overhead and Labour **(WMA 4.3.2)**	V/C				V/C
	-Service Charge **(WMA 4.3.3)**	V/C				V/C
	-Transport Charge **(WMA 4.3.4)**	V/C				V/C
4.4	Job Proceeding **(WMA 4.4)**					
	-LPO Noting **(WMA 4.4.1)**	V/E				V/E
	-Indent Noting **(WMA 4.4.2)**	V/E				V/E
	-Job Close **(WMA 4.4.3)**	V/E				V/E
4.5	Clearing **(WMA 4.5)**					
	-LPO **(WMA 4.5.1)**	V/E				V/E
	-Indent **(WMA 4.5.2)**	V/E				V/E
4.6	Finance Matter **(WMA 4.6)**					
	-Payment (Allowance) **(WMA 4.6.1)**	V/E				V/E
	-Payment (Supplier) **(WMA 4.6.2)**	V/E				V/E
	-Payment(Sundries) **(WMA 4.6.3)**	V/E				V/E
	-Payment (Direct Order) **(WMA 4.6.4)**	V/E				V/E
	-Journal Job **(WMA 4.6.5)**	V/E				V/E
	-Payment Receipt **(WMA 4.6.6)**	V/E				V/E
	-Warrant **(WMA 4.6.7)**	V/E				V/E
	-Billing of Completed Job **(WMA 4.6.8)**	V/E				V/E
4.7	Utilities **(WMA 4.7)**					
	-Change Password **(WMA 4.7.1)**	E				E
	-Back to Admin **(WMA 4.7.2)**	V				
4.8	Listings **(WMA 4.8)**					V
	-LPO Noting List **(WMA 4.8.1)**	V				V
	-Indent Noting List **(WMA 4.8.2)**	V				V
	-Job Listing **(WMA 4.8.3)**	V				V
4.9	Printing **(WMA 4.9)**					
	-General Report **(WMA 4.9.1)**	V				V
	-Job Report **(WMA 4.9.2)**	V				V

No	Screen Accessible	Administrat or	Workshop Approval Officer	Mechanics	Store Officer	Account Officer
	-Vote Book Summary **(WMA 4.9.3)**	V				V
	-Vote Book Details **(WMA 4.9.4)**	V				V
	-Print Bill Customer **(WMA 4.9.5)**	V				V
5.0	Audit Trails **(WMT 5.0)**	V				
V – View C – Create E – Edit D – Delete						

1.4.3 Scope and Boundaries of the TOE

This section describes both physical and logical boundaries of the TOE.

1.4.3.1 Physical Boundaries

The physical boundary of the eWorkshop Application is the operating environment itself where any authorised person can access the application.

The application server is to be located in a secure area that is free from physical access to unauthorised parties. This would restrict access to the application through only logical access.

1.4.3.2 Logical scope

The TOE comprises:

1. Creation and deletion of logon Ids and the default passwords
2. The assignment of user roles (or privileges or access rights) to access appropriate sections of the application for the user to perform his user role and responsibilities. The user roles implemented in an existing system are:
    a. Administrator,
    b. Workshop Approval Officer,
    c. Mechanics,
    d. Store Officer,
    e. Account Officer

The logical scope of the TOE is defined as follows:

1. Security Audit

   The security audit function ensures that all administrator activity pertaining to creation/update/delete of logon IDs as well as the assignment of user roles is logged. Additionally all failed logon attempts by all user IDs are being logged as well as the resetting of passwords by Administrator roles. This audit trail logs can be viewed by users with Administrator roles and will be kept for six months. Audit trail records beyond six months will be automatically deleted by the application.

2. User Data Protection

   User data is protected by ensuring that specific user roles assigned by the administrator can only access specific screens and hence the data associated with the screens. Roles not authorized to access certain screens not within their role will therefore will not even be able to see those screens. The access is governed by the Administrator Policy and the User Policy. The Administrator Policy allows the administrator to perform the dual function of logon ID and user role administration, as well as the correction of erroneous data or misaligned data entries entered by the other users. The User Policy enables the user to access their authorised functions via the screens associated with the user role.

3. Identification , authentication and authorization

   All users must have a valid logon ID and user role to access the application. The user role would have been preassigned by the Administor when the ID was created. Users must logon on to identify themselves to the application together with their user role in order for them to use the application screens authorized by their user role.

4. Security Management

   All users must have a valid logon ID and user role to access the application. The user role would have been preassigned by the Administor when the ID was created. Users must logon on to identify themselves to the application together with their user role in order for them to use the application screens authorized by their user role.

5. TOE Access

   If a login session has remained idle for 15 mins, the application will automatically log the user off from the application. The user will have to re-login to access the application again.

6. Protection of the TSF

   To protect the integrity of the TOE, a reliable time stamp is required to be used in association with audit trail activities. The time stamp is provided by the operating system.

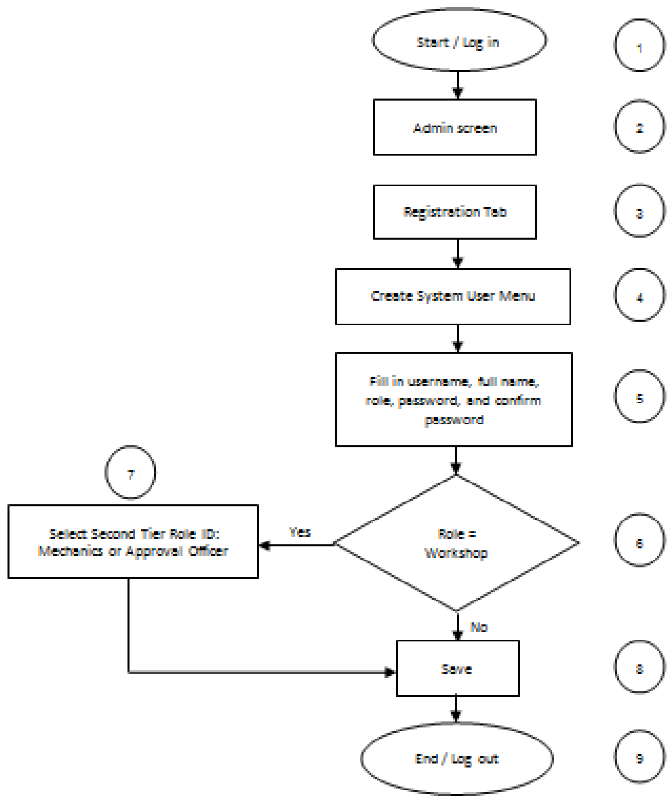
TOE - eWorkshop Access Control Administration

The logon ID creation and user roles for logical access to screens, reports and functions via user role assignment are administered by an Administrator appointed by the client organisation and pre-configured by the application supplier during the installation and setting up of the application.

The creation of logon ID and user roles assignment flow is shown in the following chart:

Figure 3 : Flow for Creation of ID and Role Assignment

Figure 3 : Flow for Creation of ID and Role Assignment


Start / Log in
1
Admin screen
2
Registration Tab
3
Create System User Menu
4
Fill in username, full name, role, password, and confirm password
5
7
Select Second Tier Role ID: Mechanics or Approval Officer
Yes
Role = Workshop
6
No
Save
8
End / Log out
9

The description of the actions in each step in the above diagram is described below:

1) User start program and logon as administrator.
2) User sees administrator screen to enable performance of administrator operations..
3) To create a system user, go to registration tab.
4) From registration tab, click the create system user menu button.
5) The user must key in the details of new system user i.e. the username, full name, role, password, and confirm password.
6) If the workshop role is selected, the user will get a submenu to select second tier role ID which is either Mechanics or Approval Officer.
7) The user will select either Mechanic or Approval Officer, if the workshop role is selected in step 6.
8) The user saves the selection.
9) To end the session, the user logs off.

There are many screens for the operation of the eWorkshop application and as these are user role specific, these screens are not shown here but the mapping between the user role and the screens accessible with that user role are tabulated in an actual implemented example for a client in Table 2. The actual function of the screens or processing of data entered into the screens is not part of the TOE, except those mentioned in the TOE details in the beginning of section 1.4.2.

1.4.4 Acronyms

The following abbreviations from the Common Criteria are used in this Security Target:

CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFR	Security Functional Requirement
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

2 Conformance Claim

2.1 CC Conformance Claim

This TOE conforms to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, Version 3.1 Revision 3, July 2009.
- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 3, July 2009.
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 3.1 Revision 3, July 2009.
- Evaluation Assurance Level 1 (EAL1)

2.2 PP Claim

There is no PP Claim related to this ST.

2.3 Package Claim

This ST claims a package for EAL1.

2.4 Conformance Rationale

As there is no PP Claim, the Conformance Rationale is not applicable.

3 SECURITY OBJECTIVES

3.1 Security Objectives for the Operational Environment

The security objectives countering security threats using the security policies enforced and the assumptions for the operational environment are described in Table 3.

Table 3 : Security Objectives for the Operational Environment

Name	Description
OE.AUTH	Users must be authorized by management before and ID and user role is being assigned for them to access and use the application in a secure manner.
OE.TRAIN	The operational environment shall ensure that all TOE users receive appropriate training before allowing them to work with the TOE;
OE.ENV	The operational environment will be secure and the use of the application will be confined to the Intranet.

4 EXTENDED COMPONENTS DEFINITION

There is no extended component in this ST.

5 SECURITY REQUIREMENTS

5.1 Security Functional Requirements

The SFRs for the TOE are listed in Table 4. These requirements were derived from the CC Part 2 Security Functional Requirements.

Table 4 : TOE Security Functional Requirements

Security Functional Class	Security Functional Components	Dependency and Hierarchical Relationship
Security Audit FAU	FAU_GEN.1 Audit Data Generation.	Dependent on FTP_STM.1
	FAU_GEN.2 User Identity Association	Dependent on FAU_GEN.1 and FIA_UID.1
	FAU_SAR.1 Audit review	Dependent on FAU_GEN.1
	FAU_SAR.2 Restricted audit review	Dependent on FAU_SAR.1
	FAU_SAR.3 Selectable audit review	Dependent on FAU_SAR.1
User Data Protection FDP	FDP_ACF.1 Security attribute based access control	Dependent on FDP_ACC.1 and FMT_MSA.3
	FDP_ACC.1 Subset access control	Dependent on FDP_ACF.1
Identification and Authentication FIA	FIA_UAU.1 Timing of authentication	Dependent on FIA_UID.1
	FIA_UID.2 User identification before any action	Hierarchical to FIA_UID.1 – Timing of identification
Security Management FMT	FMT_MSA.1 Management of security attributes	Dependent on FDP_ACC.1 Dependent on FMT_SMR.1 and FMT_SMF.1
	FMT_MSA.3 Static attribute initialization	Dependent on FMT_MSA.1 and FMT_SMR.1
	FMT_SMF.1 Specification of Management Functions	No dependency
	FMT_SMR.1 Security roles	Dependency on FIA_UID.1 is covered by FIA_UID.2
TOE Access FTA	FTA_SSL.1 TSF-initiated session locking	Dependency on FIA_UAU.1
Protection of the TSF FPT	FPT_STM.1 Reliable time stamps	No dependency

Note 1:

FIA_UID.2 is hierarchical to FIA_UID.1. FIA_UID.2 requires that a user be successfully authenticated via a valid logon ID and password before being able to do anything else. Hence FIA_UID.2 supersedes the need and covers the functions of FIA_UID,1.

Note 2:

The following conventions have been applied in this document:

Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: assignment, selection, and iteration.

1. The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold underline text** in red color font for additions and a strike thru for deletions.

2. The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized text* in square brackets, [*selection value*] in red color font.

3. The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment value] in red color font.

4. The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration number) in red color font.

5.1.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) ~~Start-up and shutdown of the audit functions;~~

b) All auditable events for the [*not specified*] level of audit; and

c) **[**Creation/update/delete or user Ids, assignment of user role and resetting of passwords for users by the Administrator, and failed login attempts by all user IDs**].**

Application Note : Audit functions will always be on and records beyond 6 months will be automatically deleted by the system periodically.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [Audit Trail ID,Role ID, Transaction Type, Status, Username, Transaction Date, Transaction Time].

FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

This component will provide authorised users the capability to obtain and interpret the information. In case of human users this information needs to be in a human understandable presentation. In case of external IT entities the information needs to be unambiguously represented in an electronic fashion.

FAU_SAR.1.1 The TSF shall provide **[**users with Administrator role**]** with the capability to read **[**audit trail of creation/update/delete of user Ids, assignment of user roles and resetting of password and failed login attempts by all user IDs**]** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply **[**selection criteria for display of audit trail data**]** of audit data based on **[**date range and/or ID specified**].**

5.1.2 Class FDP: User Data Protection

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [Administrator Policy and User Policy] to objects based on the following: [user roles in Table 1].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [user must have a valid userid and a defined or assigned role].

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 [none].

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [Administrator Policy and User Policy] on [user roles in Table 1].

5.1.3 Class FIA: Identification and Authentication

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [access only to the logon screen] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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.

5.1.4 Class FMT: Security Management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [Administrator Policy] to restrict the ability to [*create, modify, delete*] the security attributes [username, password, role] to [the authorised identified user roles in Table 1].

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [Administrator Policy and User Policy] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [the authorised identified user roles in Table 1] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [create user Ids and assign user roles in Table 1].

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [the authorised identified user roles in Table 1].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.5 Class FTA: TOE Access

FTA_SSL.1 TSF-initiated session locking

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL.1.1 The TSF shall lock an interactive session after [15 mins of user inactivity] by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [re-login].

5.1.6 Class FPT: Protection of the TSF

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 ~~The TSF shall be able to provide reliable time stamps.~~

Application Note : The time stamps will be taken by the TSF from the operating system.

5.2 Security Assurance Requirements

The security assurance components drawn from CC Part 3 Security Assurance Requirements EAL 1 are identified in Table 5.

Table 5 : TOE Security Assurance Requirements: EAL1

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_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
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

6 TOE SUMMARY SPECIFICATION

This Chapter presents a functional overview of the TOE; the security functions implemented by the TOE; and the Assurance Measures applied to ensure their correct implementation.

6.1 Summary Specification Rationale

The TOE Summary Specification chapter describes every Security Function of the TOE, meeting the requirements of every SFR. Within the description of the SF, a rationale is provided. All the SFs are presented in Table 6; this table maps SFRs to SFs. This demonstrates that the Security Functions fulfil every SFR.

Table 6 : Mapping Security Functional Requirements to Security Functions

SECURITY FUNCTIONS SFR	SECURITY AUDIT	USER DATA PROTECTION	IDENTIFICATION AND AUTHENTICATION	SECURITY MANAGEMENT	TOE ACCESS	PROTECTION OF THE TSF
FAU_GEN.1	X					
FAU_GEN.2	X					
FAU_SAR.1	X					
FAU_SAR.2	X					
FAU_SAR.3	X					
FDP_ACF.1		X				
FDP_ACC.1		X				
FIA_UAU.1			X			
FIA_UID.2			X			
FMT_MSA.1				X		
FMT_MSA.3				X		
FMT_SMF.1				X		
FMT_SMR.1				X		
FTA_SSL.1					X	
FPT_STM.1						X

6.2 TOE Summary Specification

This Section presents the security functions performed by the TOE to satisfy the identified SFRs in Section 5.1.

6.2.1 Security Audit

FAU_GEN.1 Audit Data Generation

Audit records on creation/update/delete of logon ID, the assignment of user role and failed logon attempts generated by the TOE, resetting of passwords by Administrator role, to ensure accountability and tracing of important activities.

FAU_GEN.2 User Identity Association

Each of the audit records generated through FAU_GEN.1 will be associated by the TOE with the actual identity of the user whose action generated the audit record to ensure accountability and traceability of activities.

FAU_SAR.1 Audit Review

The TOE enables the audit trail records generated from FAU_GEN.1 and FAU_GEN.2 to be reviewed by all users with Administrator role in read only mode.

FAU_SAR.2 Restricted Audit Review

The TOE restricts the view of audit trail records generated from FAU_GEN.1 and FAU_GEN.2 to only authorised users in read only mode.

FAU_SAR.3 Selectable Audit Review

The TOE allows the authorised user to specify or select the date range and/or the ID of interest to narrow down the audit trail records generated from FAU_GEN.1 and FAU_GEN.2 for easy review.

6.2.2 User Data Protection

FDP_ACF.1 Security Attribute Based Access Control

Access to the application functions is controlled by the user role assigned to the user . The user role must be assigned by the authorized Administrator upon approval through procedures outside of the application.

FDP_ACC.1 Subset Access Control

Access to the application functions is controlled by the user role assigned to the user. The user role must be assigned by the authorized administrator upon approval through procedures outside of the application. The access is governed by the Administrator Policy and the User Policy. The Administrator Policy allows the administrator to perform the dual function of logon ID and user role administration, as well as the correction of erroneous data or misaligned data entries entered by the other users. The User Policy enables the user to access their authorised functions via the screens associated with the user role.

The user data protection function addresses this requirement.

6.2.3 Identification and Authentication

FIA_UAU.1 Timing of Authentication

To prevent unauthorized access to the TOE functions as well as reliable accountability for authorized administrator use of security functions, the TOE require authorized administrators to perform authentication before they may access any of the TOE functions or data.

The authentication policy required to meet the assurance requirements of AVA_VAN.1 is described below. Passwords for authentication through the appliance console or the administration consoles must be 6 to 15 characters.

This policy ensures a sufficiently low probability of guessing the password.

The security identification and authentication function addresses this requirement.

FIA_UID.2 User Identification before any Action

To prevent unauthorized access to the TOE functions as well as reliable accountability for user and authorized administrator use of security functions, a user or authorized administrator has to identify and authenticate through a login interface before any action on the TOE. When accessing the TOE, the user or authorised administrator will be prompted for his/her login and password before any other action on the console.

6.2.4 Security Management

FMT_MSA.1Management of security attributes

Through the assignment of user roles by the authorized administrator, the user is authorised and restricted to perform the appropriate functions of creation, update and delete of information within the appropriate role boundary.

FMT_MSA.3 – Static attribute initialisation

Through the assignment of user roles by the authorized administrator, the user is authorised and restricted to perform the appropriate functions of creation, update and delete of information within the appropriate user role boundary.

FMT_SMF.1 – Specification of Management Functions

The authorized administrator is able to create user Ids and assign user roles as appropriate. A user can have only one user role.

FMT_SMR.1 – Security roles

The authorized administrator is able to assign user roles as appropriate. A user can have only one user role.

6.2.5 TOE Access

FTA_SSL.1 Session locking

When there is inactivity of a user terminal for up to 15 mins, the TOE will automatically initiate session locking. User must re-login to access the application again.

6.2.6 Protection of the TSF

FPT_STM.1 Reliable Time Stamps

The TOE will use the time from the operating system to generate time stamps of the activities within the application.